CHAPTER 5

Connectivity Technologies for IoT

Internet of Things (IoT) is a set of technologies that are enabling new use cases and delivering services across a wide variety of markets and applications. When people think of IoT, they often think of home or personal IoT. However, IoT will play a role in many commercial applications such as smart manufacturing, smart cities, autonomous cars, building automation, and healthcare. How will an IoT-enabled device communicate what it knows to the Internet? Suitable connectivity solutions range from a multitude of wired connectivity technologies such as Ethernet to wireless technologies like Wi-Fi and even 5G cellular. Many solutions need a combination of multiple communication technologies. For example, a smart car system playing video or using GPS navigation might need 4G LTE in order to communicate with the outside world and Wi-Fi and Bluetooth to communicate with devices like phones and rear seat entertainment (RSE) used by the passengers. In this chapter, we will take a look at a selected set of connectivity technologies that enable these applications.

S. Cheruvu et al., *Demystifying Internet of Things Security*,
https://doi.org/10.1007/978-1-4842-2896-8_5

Ethernet Time-Sensitive Networking

Ethernet Time-Sensitive Networking (TSN) is reshaping the industrial communication landscape and laying the foundation for the convergence of Information Technology (IT) and Industrial Operations Technology (OT). TSN essentially is a set of features that have been added to standard Ethernet. By bringing industrial-grade robustness and reliability to Ethernet, TSN offers an IEEE standard communication technology that can be used to enable deterministic communications for industrial applications. Being an IEEE standard, it enables interoperability between standard compliant industrial devices from different suppliers. TSN removes the need for physical separation of critical and noncritical communication networks, reducing the cost of the infrastructure needed to allow open data exchange between operations technology network and enterprise/information technology network – a concept that is at the heart of the Industrial Internet of Things (IIoT). At the network system level, TSN supports deterministic communication based on network schedules that are distributed to devices via standard configuration interfaces.

TSN standards address a wide range of functions, and their implementation can be similarly broad, encompassing various hardware elements such as endpoints and switches, embedded software, standard interfaces, routing algorithms, and configuration tools. To ensure the highest levels of TSN performance, a system-level solution is required that takes each element into account and provides a seamless interface between them. Seamless fault-tolerant communication and enhanced cybersecurity with robust network planning, configuration, and monitoring will be a necessity in the networks of the future.

Legacy Ethernet-Based Connectivity in Industrial Applications

Today, there are multiple variants of Industrial Ethernet protocols available on the market. In most cases, the Industrial Ethernet protocol selected for use in industrial devices differs from vendor to vendor or from Industry Alliance to Industry Alliance, which means that devices are only compatible with other equipment from the same vendor or an Industry Alliance using the same protocol. This is known as manufacturer lock-in. It forces customers to either buy all industrial equipment from one vendor or a limited set of vendors who are part of the same Alliance. This approach may not be the most cost- and performance-optimized way to implement the required solution. If a customer chooses not to do this, there is considerable challenge of integrating equipment from multiple vendors into a single network system or there needs to be a set of protocol conversion gateways implemented between the various Industrial Ethernet protocols. Both options will lead to unnecessary expense and limit innovation on the factory floor over many years. Thus industrial automation architectures become hierarchical, purpose-built, and inflexible.

This approach is currently undergoing a dramatic change with the advent of the IIoT and Industry 4.0, which demands for full automation and greater insights in manufacturing. These demands are pushing industrial automation architectures to become more flexible and seamless to interoperate. In these types of increasingly converged architectures, real-time connectivity is essential for controlling critical processes, as well as for collecting and analyzing data from machines, in a timely manner. TSN offers the real-time connectivity capabilities that match and sometimes exceed what current Industrial Ethernet protocols can provide, with the added flexibility of being based on IEEE standards. Similar to what is the norm in the enterprise world, TSN Ethernet can therefore be the common communication protocol that connects industrial equipment from different vendors, simultaneously delivering the very challenging functional requirements demanded by mission-critical embedded and industrial applications.

Key Benefits of TSN

The primary strength of TSN is its status as an open standard–based technology, unaffiliated to any Industry Alliance or company. For an industrial automation market that has struggled for many years with multiple incompatible proprietary communication protocols, TSN brings several key benefits.

TSN guarantees compatibility at the network level between devices from multiple suppliers. This gives customers much greater choice of devices for building their system, avoiding manufacturer lock-in and enabling seamless connectivity across various subsystems and systems.

As TSN is part of the Ethernet standard family, it naturally scales with Ethernet, which means that the technology will not be limited in terms of bandwidth/speeds, thus allowing more and more sensors and actuators that are needed for implementing complex automation applications to be connected to a network system.

TSN supports standards-based network configuration capabilities. This means that new nodes can be added to the network and discovered without the need for costly downtimes and manual configuration. New data streams can be added to the network without the risk of disturbing existing traffic and without the need to reconfigure the entire network.

TSN can be used for communication between machines as well as from machines to enterprise systems. Communication between mission-critical TSN-based systems and existing noncritical Ethernet-based systems can be achieved over the same infrastructure. In other words, non-TSN Ethernet nodes can work over a TSN network, without modification.

Overall system costs are significantly reduced when we adopt standards-based technology. Consumer choice and competition will result in lower device prices. Research, development, and maintenance costs are all driven down when solution providers and customers can focus on one standard technology rather than a number of different proprietary protocols and solutions.

Breaking down communication barriers between critical and noncritical systems is a foundational concept of the IIoT and Industry 4.0. TSN enables the convergence of networks and systems that were previously kept separate for reasons of operational integrity, real-time performance, safety, and security.

TSN allows time-critical messages to be sent over the same communication line as all other Ethernet traffic, without disturbance or increase in delay and with controlled delay variation. Different traffic classes can coexist on the network with no impact on higher criticality level traffic from traffic with lower priority.

End-to-end latency is guaranteed even under heavy traffic load, and standard mechanisms can be used to accelerate message transport for high-priority communications. Thus, the most challenging motion control and safety-critical applications can be converged with other Ethernet traffic on Ethernet networks using TSN.

Convergence makes accessing data from industrial systems easier. With more systems on the same network, the task of gathering data from a wide variety of sources is simplified. Data from industrial systems can be sent to enterprise systems over standard Ethernet without the need for protocol conversion gateways. Overall system costs are significantly reduced by the convergence of different traffic classes on a single network infrastructure. Hardware and maintenance costs are lower because we need fewer devices and cables to build the network infrastructure.

Higher layer protocols can be combined with TSN, as the technology is implemented primarily at the data link layer (OSI model layer 2).[1] One example is the Open Platform Communications-Unified Architecture (OPC-UA) protocol.[2]

[1] ISO/IEC 7498-1:1994 - Information technology - Open Systems Interconnection - Basic Reference Model: The Basic Model.

[2] More details on OPC-UA can be found at https://opcfoundation.org/about/opc-technologies/opc-ua/

TSN Standards

Table 5-1 lists the TSN set of features that have been added to standard Ethernet. The features are defined and published in a number of IEEE 802.1 standards that address topics such as timing, synchronization, forwarding, queuing, seamless redundancy, and stream reservation. These individual features extend the functionality and Quality of Service (QoS) of Ethernet to enable guaranteed message transmission through switched networks, providing the fundamental capabilities such as robustness, reliability, and determinism required for an industrial communication technology.

Table 5-1. *List of Published IEEE Standards for TSN (March 2019)*

Function	Standard
Time Synchronization	• IEEE Std. 802.1AS^{TM}-2011: generalized Precision Time Protocol (gPTP)
Bounded Low Latency	• IEEE Std. 802.1Qav^{TM}-2009: Credit-based shaper • IEEE Std. 802.1Qbv^{TM}-2015: Transmission gate scheduling • IEEE Std. 802.1Qbu^{TM}-2016 & IEEE Std. 802.3br^{TM}-2016 : Frame Preemption • IEEE Std. 802.1Qch^{TM}-2017 : Cyclic Queuing and Forwarding
Reliability	• IEEE Std. 802.1Qca^{TM}-2015 : Path Control and Reservation • IEEE Std. 802.1CB^{TM}-2017 : Frame Replication & Elimination • IEEE Std. 802.1Qci^{TM}-2017 : Per-stream Filtering & Policing
Resource Management	• IEEE Std. 802.1Qat^{TM}-2010 : Stream Reservation Protocol • IEEE Std. 802.1Qcc^{TM}-2018 : SRP Enhancements and Performance Improvements • IEEE Std. 802.1Qcp^{TM}-2018 : YANG model

To address new use cases and make performance improvements, many more IEEE standards are being defined, as listed in Table 5-2.

***Table 5-2.** List of Upcoming IEEE Standards for TSN (March 2019)*

Time Synchronization	• P802.1AS-Rev (Draft v8.0): Time Synchronization improvement
Bounded Low Latency	• P802.1Qcr (Draft v0.5): Asynchronous Traffic Shaping • P802.1Qcz (PAR approved): Congestion Isolation
Reliability	• P802.1Qcx (Draft v1.0): YANG Data Model for Connectivity Fault Management
Resource Management	• P802.1CS (Draft v2.1): Link-local Registration Protocol • P802.1Qcj (Draft v0.4): Automatic Attachment to Provider Backbone Bridging (PBB) services • P802.1Qcw (Draft v0.2): YANG Data Models for Qbv, Qbu, and Qci • P802.1Qdd (PAR approved): Resource Allocation Protocol • P802.1ABcu (Draft v0.6): LLDP YANG Data Model • P802.1CBcv (PAR approved): Frame Replication & Elimination YANG Model and MIB Module • P802.1CBdb (PAR approved): FRER Extended Stream Identification Functions

For latest Update, check `https://1.ieee802.org/tsn/`

The key TSN features that provide guaranteed message delivery timing are time synchronization and traffic scheduling. They are addressed by the 802.1AS and 802.1Qbv standards, respectively. All devices participating in the TSN network are synchronized to a global time and are aware of a network schedule that dictates when prioritized messages will be forwarded from each switch. TSN makes use of multiple queues per port at the egress of the switch, where messages are held until a gate opens (at a time slot specified by the schedule) to release queued messages for transmission. The timed release of messages ensures that delays in the network can be deterministically predicted and managed. This allows for the convergence of critical traffic and noncritical traffic on the same network.

The preemption feature defined in the TSN 802.1Qbu standard can be used to increase the efficiency of bandwidth use for noncritical messages. In highly converged networks, it could be the case that large low-priority frames are delayed by higher-priority traffic on the network and dropped. Preemption enables the transmission of large frames to be interrupted, sent in smaller fragments and reassembled at the next link. This maximizes bandwidth utilization for all traffic types on the TSN network. Another important benefit of message preemption is the reduction of transmission latency for so-called Express traffic, which can preempt regular (lower-priority) Ethernet packets. Especially on lower-speed networks (e.g., 10 or 100 megabits per second (Mbps)) carrying large regular Ethernet packets up to 1,500 bytes and more, the latency reduction for Express traffic can be useful for building converged networks.

TSN provides a standard method for achieving seamless redundancy for industrial communication over Ethernet. The feature allows for the simultaneous transmission of duplicate message copies across different paths in the network. The first message copy to be received in time without error is processed, while the other copies are discarded. This adds another layer of determinism to the delivery of critical messages in converged networks.

A crucial feature of TSN is the support for open, vendor-independent network configuration. This is achieved through the standardization in IEEE of YANG models for various TSN standards. These can be configured over the NETCONF protocol using encoding formats such as XML or JSON. YANG models for bridging, traffic scheduling, frame preemption, seamless redundancy, and policing ensure that configuration of key TSN features is done according to standard methods. This allows TSN networks to be composed of any standard compliant device from any vendor and can be configured by any standard compliant network configuration software.

TSN Profiles

TSN is essentially a toolbox of features that address various needs such as reliability, bounded low latency, time synchronization, and resource management. These capabilities are realized through various TSN specifications (e.g., IEEE 802.1AS-Rev, IEEE 802.1Qbv, etc.), and customers can choose the relevant standards to implement based on their specific application needs. Profile standards are being specified for some of them to describe which TSN standards to use and how. A TSN profile selects features, options, configurations, and protocols to build a bridged network for the given TSN application. Table 5-3 shows a list of select TSN profiles that are currently being defined.

Table 5-3. *List of TSN Profiles (March 2019)*

Industry	TSN Profile
Industrial Automation	• IEC/IEEE 60802 (Draft v0.3):TSN Profile for Industrial Automation
Automotive In-Vehicle Networks	• IEEE Std. 802.1BA™ -2011 : Audio Video Bridging system [AVB Profile] • IEEE Std. 1722™ -2016: Transport Protocol for Time-Sensitive Applications [+AVTP Control format message types: FlexRay, LIN, CAN, MOST, Sensor, etc] • IEEE Std. 1722.1™ -2013: Audio Video Discovery, Enumeration, Connection management and Control (AVDECC) • P802.1DG (PAR approved): TSN Profile for Automotive In-Vehicle Ethernet Communications
Service Provider Networks	• P802.1DF (PAR approved): TSN Profile for Service Provider Networks

(*continued*)

Table 5-3. (*continued*)

Industry	TSN Profile
Mobile Fronthaul	• IEEE Std. 802.1CM™ -2018: TSN for Fronthaul [Mobile Fronthaul Profile] • P802.1CMde (PAR approved): Enhancements to Fronthaul Profiles to Support New Fronthaul Interface, Synchronization, and Syntonization Standards

The following sections provide an overview of the major TSN standards.

802.1AS/AS-Rev

Enhanced Generic Precise Timing Protocol: Timing and synchronization are vital mechanisms for achieving deterministic communication. 802.1AS is a profile of the IEEE 1588 PTP (Precision Time Protocol) synchronization protocol that enables synchronization compatibility between different TSN devices (Figure 5-1). This lays the foundation for the scheduling of traffic through each participating network device. 802.1AS-Rev is being defined to add support for fault tolerance and multiple active synchronization masters (Figure 5-2). Multiple clock-masters for redundancy enable high availability of TSN networks – in cases when a grandmaster becomes faulty, system elements such as end nodes and bridges are still able to remain synchronized by obtaining the timing information from the redundant grandmasters. 802.1AS-Rev is also a profile of the IEEE 1588 PTP synchronization protocol.

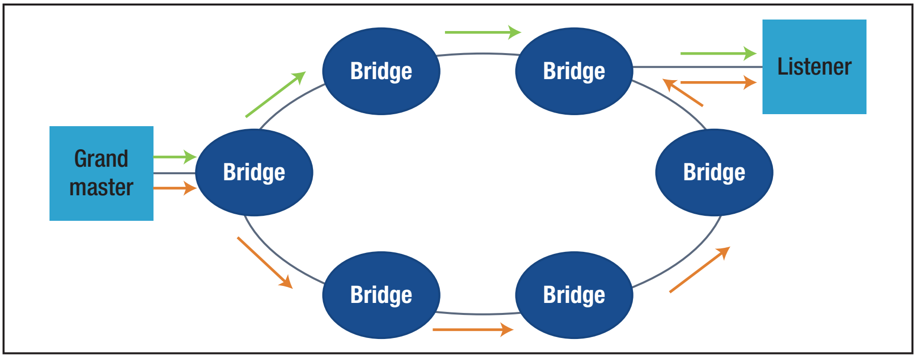

Figure 5-1. *802.1AS operation*[3]

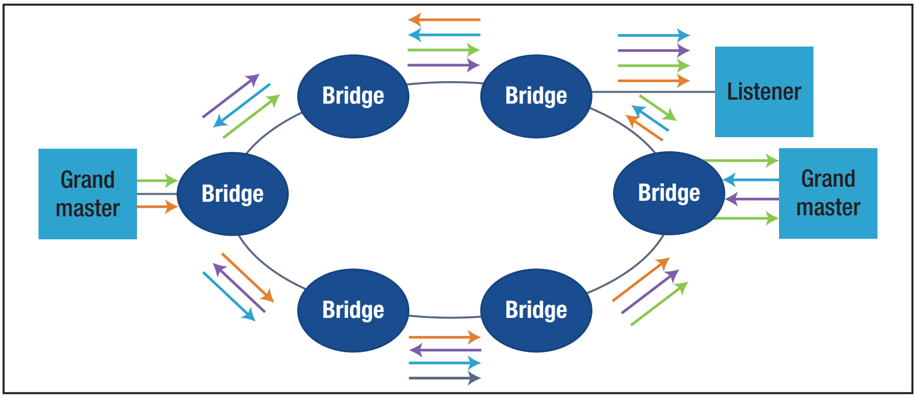

Figure 5-2. *802.1AS-Rev operation*[4]

[3] Figure 5a: Single grand master transmitting 2 copies using separate paths. https://www.synopsys.com/designware-ip/technical-bulletin/ether-time-sens-net-for-auto-adas-socs-2018q2.html

[4] Figure 5b: Multiple grand masters transmitting 2 copies using separate paths. https://www.synopsys.com/designware-ip/technical-bulletin/ether-time-sens-net-for-auto-adas-socs-2018q2.html

802.1Qbv

Time-Aware Shaper: Scheduling of traffic is a core concept in TSN. Based on the shared global time provided by 802.1AS, a schedule is created and distributed between participating network devices. 802.1Qbv defines the mechanisms for controlling the flow of queued traffic through gates at the egress of a TSN switch (Figure 5-3). Frames are assigned to queues based on Quality of Service (QoS) priority. The transmission of messages from these queues is executed during scheduled time windows. Other queues will typically be blocked from transmission during these time windows, therefore removing the chance of scheduled traffic being impeded by nonscheduled traffic. In other words, there is a gate in front of each queue which opens at a specific point of time which is reserved for that queue. This means that the delay through each switch is deterministic and that message latency through a network of TSN-enabled components can be guaranteed. The IEEE 802.1Qbv standard defines up to eight queues per port for forwarding traffic. The scheduler is designed to separate the communication on the Ethernet network into fixed length, repeating time cycles.

Figure 5-3 shows an example with four queues, with a cycle time of td and guard band of tg. At time t0, the time-critical data queue, Queue 3 is open. Once that frame is transmitted, the best effort Queues 0, 1, and 2 are opened. Before the end of the cycle, at time t0-tg, all the non-time-critical data is blocked, so that the port is free to transmit the time-critical data at the start of the next cycle. This is essentially a time-division multiple access (TDMA) scheme.

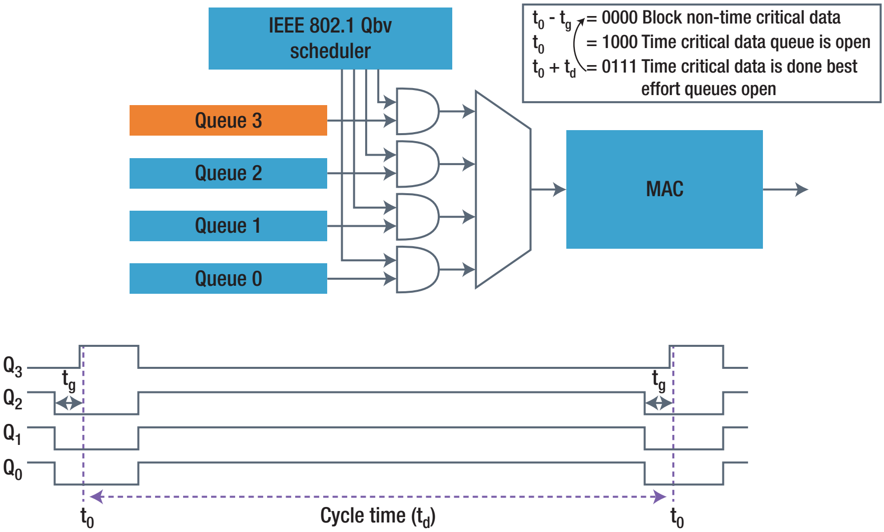
IEEE 802.1 Qbv scheduler
$t_0 - t_g$ = 0000 Block non-time critical data
t_0 = 1000 Time critical data queue is open
$t_0 + t_d$ = 0111 Time critical data is done best effort queues open
Queue 3
Queue 2
Queue 1
Queue 0
MAC
Q_3
Q_2
Q_1
Q_0
t_g
t_g
t_0
Cycle time (t_d)
t_0

Figure 5-3. *802.1Qbv operation*[5]

802.1Qbu

Frame Preemption: While the 802.1Qbv mechanisms protect critical messages against interference from other network traffic, it does not necessarily result in optimal bandwidth usage or minimal communication latency. Where these factors are important, the preemption mechanism defined in 802.1Qbu can be used (Figure 5-4). 802.1Qbu allows the transmission of standard Ethernet or jumbo frames to be interrupted in order to allow the transmission of high-priority frames, and then resumed afterward without discarding the previously transmitted piece of the interrupted message. Frame preemption always operates on a link-by-link basis. A frame is only fragmented from one Ethernet switch to the next Ethernet switch, where it is reassembled.

[5] Time-aware shaper allows scheduling. https://www.synopsys.com/designware-ip/technical-bulletin/ether-time-sens-net-for-auto-adas-socs-2018q2.html

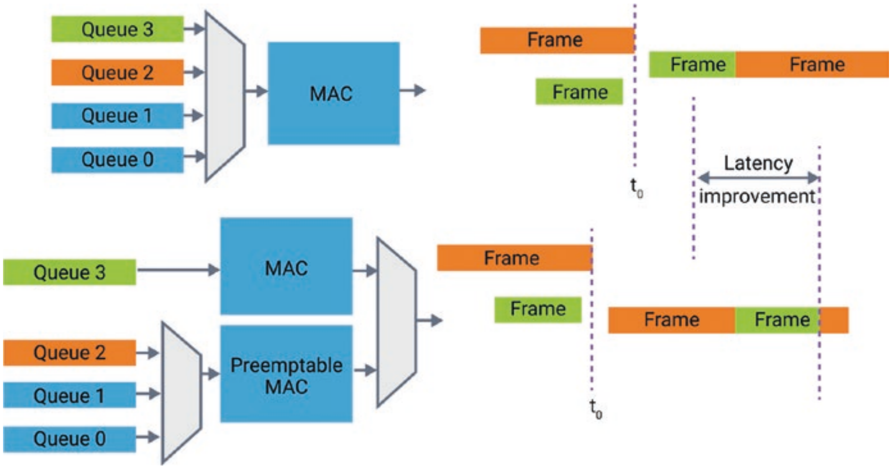

***Figure 5-4.** 802.1Qbu frame preemption*[6]

In Figure 5-4, without preemption as shown in the top, if a high-priority frame in Queue 3 arrives after a low-priority frame, the high-priority frame is delayed until the transmission of the low-priority frame is finished. In the case of an Ethernet port with preemption enabled, as shown in the bottom, the low-priority traffic passes through a preemptable MAC. The transmission of the low-priority frame is stopped, once a high-priority frame arrives and the high-priority frame from Queue 3 is allowed to go out. Once the transmission of the high-priority frame is completed, the rest of the low-priority frame is transmitted. Each partial frame is completed by a CRC32 for error detection. In contrast to the regular Ethernet CRC32, the last 16 bits are inverted to make a partial frame distinguishable from a standard Ethernet frame. Also the start frame delimiter (SFD) is changed.

[6] Preemption reduces latency of time-critical data streams. https://www.synopsys.com/designware-ip/technical-bulletin/ether-time-sens-net-for-auto-adas-socs-2018q2.html

802.1CB

Frame Replication and Elimination: Redundancy management implemented in 802.1CB follows similar approaches known from High-Availability Seamless Redundancy (HSR) (IEC 62439-3 Clause 5) and Parallel Redundancy Protocol (PRP) (IEC 62439-3 Clause 4). It supports zero switch over time when a link fails or frames are dropped. To increase availability, redundant copies of the same messages are communicated in parallel over disjoint paths through the network as shown in Figure 5-5. Time-critical frames are expanded to include a sequence number, and then they are replicated where each identical copy follows a separate path in the network. The redundancy management mechanism then combines these redundant messages to generate a single stream of information to the receiver(s). At any point in the network where the separate paths join again, duplicate frames can be eliminated from the stream as shown in Figure 5-5. The 802.1Qca standard for Path Control and Reservation defines how such paths can be set up. The standard also allows for auto configuration.

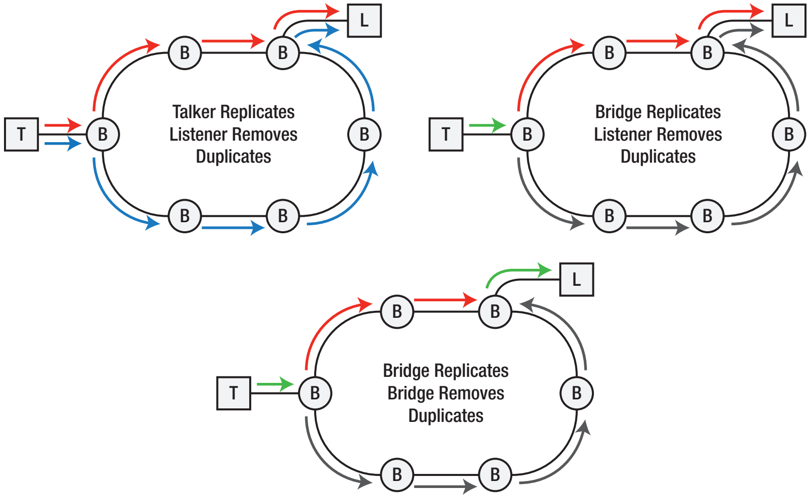

Figure 5-5. *802.1CB frame replication and elimination*[7]

802.1Qcc

Enhanced Stream Reservation Protocol: The enhancements to Stream Reservation Protocol (802.1Qat) include support for more streams, configurable stream reservation classes and streams, better description of stream characteristics, support for layer 3 streaming, deterministic stream reservation convergence, and User Network Interface (UNI) for routing and reservations. 802.1Qcc supports offline and/or online configuration of TSN network scheduling to provide network management for control plane. It supports a “Central Controller” or predefined “Engineered Configuration” of the network.

[7] Frame Replication & Elimination Page 16. https://bcourses.berkeley.edu/files/66071146/download?download_frd=1

The fully centralized configuration model is depicted in Figure 5-6. It is composed of Centralized User Configuration (CUC) entity and a Centralized Network Configuration (CNC). Computing the configuration setting and enforcing it (e.g., setting up gate schedules, reserving resources, etc.) in bridges are done by CNC. Thus CNC will be in charge of configuring TSN features such as credit-based shaper, frame preemption, scheduled traffic, per-stream filtering and policing, and frame replication and elimination for reliability. The CUC is responsible for building up the applications' requirements.

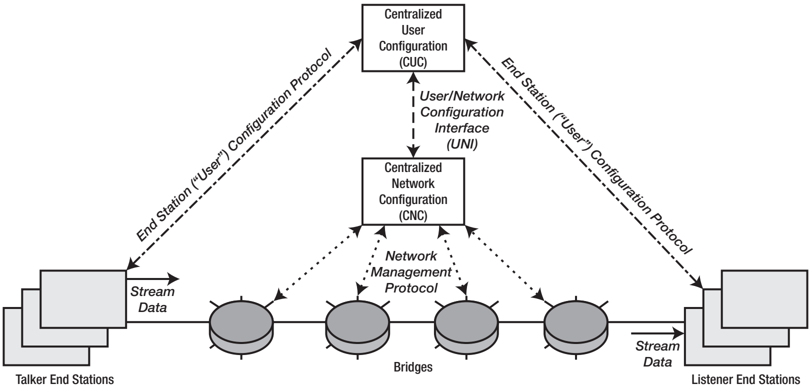
Centralized User Configuration (CUC)
User/Network Configuration Interface (UNI)
Centralized Network Configuration (CNC)
End Station ("User") Configuration Protocol
End Station ("User") Configuration Protocol
Network Management Protocol
Stream Data
Stream Data
Talker End Stations
Bridges
Listener End Stations

Figure 5-6. *802.1Qcc centralized network configuration*[8]

802.1Qci

Per-Stream Filtering and Policing: This protects against faulty and/or malicious endpoints and switches and isolates faults to specific regions in the network. It works at the ingress of the switch (forwarding engine) in order to protect the outgoing queues from being flooded with frames. In this process,

[8] Figure 3: Centralized Network Configuration. https://www.odva.org/Portals/0/Library/Conference/2017-ODVA-Conference_Zuponcic_Hantel_Klecka_Didier_TSN_Influences_on_ODVA_Technologies_FINAL.pdf

the data packets are checked to ensure that they fit to a reserved data stream at the network input. If this is not the case, the packet will be filtered out and rejected and won't be forwarded further. This can be leveraged to prevent attacks on level 2 of the OSI layer model. It utilizes well-known flow identifiers and policers used in the industry. Per-Stream Filtering and Policing (PSFP) allows filtering and policing decisions to be made on a per-stream basis. The various stages of data flow for one stream are depicted in Figure 5-7.

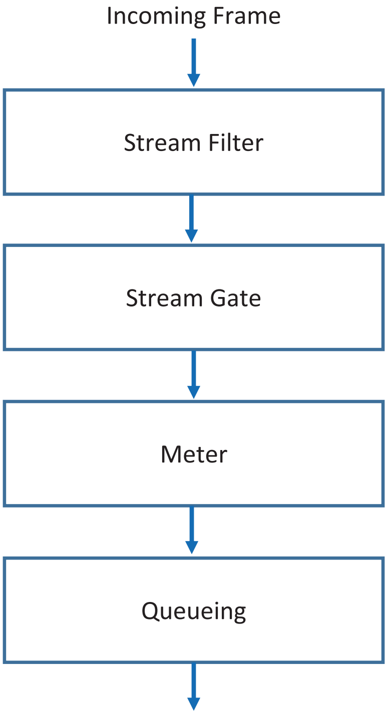

Figure 5-7. *802.1Qci per-stream filtering and policing*

802.1Qch

Cyclic Queuing and Forwarding: This defines cycles for forwarding traffic that is queued using 802.1Qci to assign buffers and 802.1Qbv to shape traffic. This cyclic enqueuing and queue draining procedure gives a defined (but not optimal) upper boundary for latency. Basically this is a simplified way to use TSN if controlled timing is desired, but reducing latency to absolute minimum is not highly important. The synchronized operations effectively allow bridges to synchronize their frame transmissions in a cyclic manner, achieving zero congestion loss and bounded latency, independently of the network topology.

In this scheme, time-sensitive streams are scheduled (enqueued and dequeued) at each time interval resulting in a worst-case deterministic delay of two times the cycle time between the sender (talker) and the next (intermediate) receiver (listener). As shown in Figure 5-8, each high-priority traffic frame scheduled on a cycle is scheduled to be received at the next bridge in the next cycle. A guard band before the start of the cycle prevents any interfering low-priority traffic from affecting the high-priority traffic. 802.1Qch can be combined with frame preemption, to reduce the cycle time from the transmission time of a full size frame to the transmission time of a minimum size frame fragment. Thus, preemption can improve the performance for high-priority traffic. For this to work correctly, all frames must be kept to their allotted cycles, that is, all transmitted frames must be received during the expected cycle at the receiving bridge.

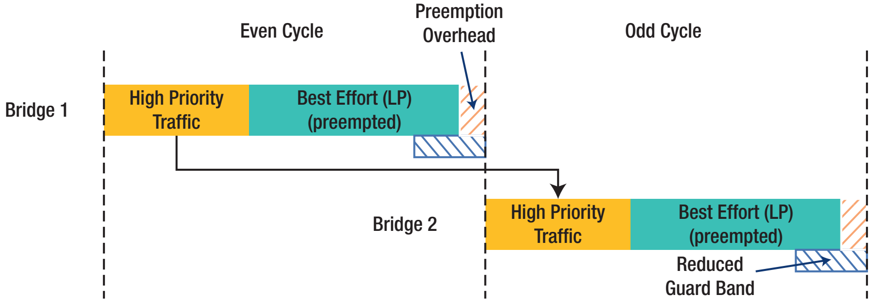

Figure 5-8. *802.1Qch operation with preemption (802.1Qbu)*[9]

To summarize, the network transit latency of a frame is completely characterized by the cycle time and the number of hops. Therefore, the frame latency is completely independent of the topology parameters and non-TSN traffic.

802.1Qcr

Asynchronous Traffic Shaping: This provides bounded latency and jitter (relatively lower performance levels) without the need for time synchronization. It aims to smoothen traffic patterns by reshaping streams per hop, implementing per flow queues and prioritizing urgent traffic over lower-priority traffic. Previously described TSN standards such as Time-Aware Shaper (802.1Qbv) and Cyclic Queuing and Forwarding (802.1Qch) depend on network-wide coordinated time and packet transmission at enforced periodic cycles, resulting in suboptimal utilization of available network bandwidth. 802.1Qcr operates asynchronously, without the need

[9] Illustration of CQF with preemption for a linear network. https://arxiv.org/pdf/1803.07673.pdf

for bridges and endpoints to synchronize in time. Therefore, it is expected that this technique can utilize available network bandwidth efficiently under heavy link utilization with mixed criticality traffic.

TSN and Security

Since TSN is Ethernet based, the security mechanisms that are state of the art today can be employed to secure the TSN network. Traditional security solutions such as firewalls will be the key to this. Since firewalls need to inspect packets, the resulting computational overhead in firewalls can create an additional transmission delay. This delay should be taken into account while configuring the TSN network schedules. If security mechanisms introduce longer delays than that are tolerable by the TSN application, they can be implemented at the border or periphery of the TSN network, such as an Industrial Demilitarized Zone that connects the TSN industrial control network to the rest of the IT system.

OPC-UA Over TSN

Of the many higher layer industrial communication protocols that could be combined with TSN, one of the prominent ones is OPC-UA. Much like TSN, OPC-UA is an open, standard technology that is vendor independent and useful for a wide range of industrial applications. The combination of OPC-UA and TSN therefore provides a complete open, standard, and interoperable solution that fulfills a plurality of industrial communication requirements.

By representing data in a uniform way, OPC-UA enables interoperability between devices that could not previously share data and gives you new insight into a wealth of information. For this reason, it has been adopted and integrated into products by all of the major industrial automation vendors. OPC-UA was originally limited to a client or server architecture; however the recently released publish/subscribe (PubSub) extension now enables multicast communication. In combination with TSN, OPC-UA

PubSub allows data to be sent with precise timing and thus be used for real-time industrial applications as illustrated in Figure 5-9. In the horizontal direction, OPC-UA-based controller-to-controller communication can be done over TSN. In the vertical direction, OPC-UA-based controller-to-cloud communication can be done directly, via a gateway or broker. This enables IT (Information Technology) systems having less stringent timing requirements to interwork with OT (Operations Technology) systems that need guaranteed data delivery with precise timing.

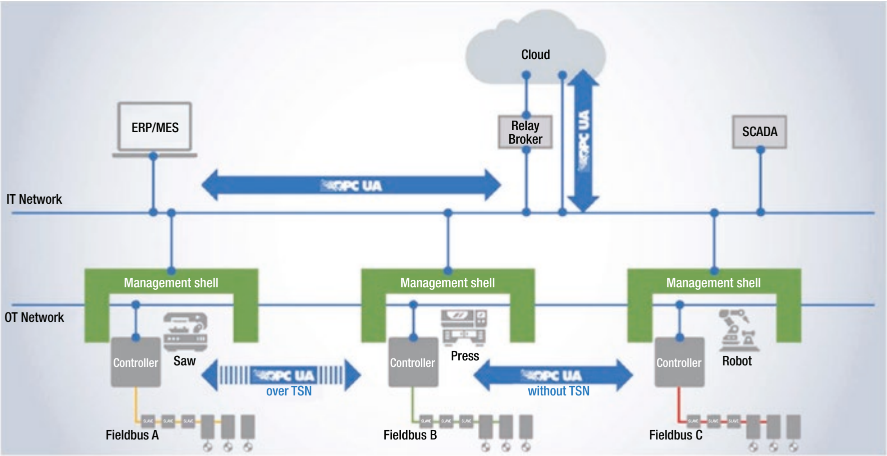

Figure 5-9. *Factory automation network with OPC-UA over TSN*

OPC-UA also enables a standard method for configuring TSN networks online and in a dynamic way. This does not require you to input any system parameters for the scheduler as these are all taken from the OPC-UA application parameters within each device. A broker mechanism as defined by the OPC Foundation provides an interface between OPC-UA applications and TSN scheduling software.

Overview of Wireless Connectivity Technologies

The IoT will require several wireless technologies if it's to meet its potential. For example, Bluetooth Low Energy and IEEE 802.15.4 are good choices for battery-powered sensors, but for devices that are constantly moving, or are not near a LAN (local area network), such relatively short-range wireless technologies are not suitable for connecting to the Internet.

Even if a LAN is present, manufacturers might prefer longer-range wireless technology for its convenience and autonomy. For example, a white goods manufacturer could select cellular technology over Wi-Fi because it enables a refrigerator or washing machine to connect to the Cloud automatically, eliminating the need for a consumer to enter a password to add the appliance to a home's LAN. In these situations, low-power wide area networks (LPWAN) or Narrowband IoT technologies could come to the rescue.

Considerations for Choosing Wireless Technologies for IoT

There are many wireless networking technologies that are deployed in IoT today, each with a different set of capabilities. Here are some of the key considerations when choosing these different solutions.

Spectrum

Wireless spectrum can be characterized as either licensed or unlicensed. Access to licensed spectrum is typically purchased from local government to provide an organization exclusive access to a particular channel in a particular location. Operation in that channel should be largely free of interference from competing radios. The drawback is that the spectrum of interest may be extremely scarce or expensive to access. In some other cases, radio connectivity bands allowed in one country may not be available in other geographical area for same usage. For instance, mobile networks in India use the 900 MHz and 1800 MHz frequency bands, while GSM (Global System for Mobile communications) carriers in the United States operate in 850 MHz and 1900 MHz frequency bands. To deploy an IoT device globally, then it may have to support multiple radio bands making the device costly as well as time-consuming to develop. Even when more easily accessible, it can take months to gain the approval to operate, so licensed bands are not well suited to rapid deployments. Unlicensed spectrum is generally open and available to anybody to use with no exclusive rights granted to any particular organization or individual. The downside is that competing systems may occupy the same channel at different power levels leading to interference. Manufacturers of radio systems operating in unlicensed bands include capabilities in these radios to adapt their operation for this potential interference. These techniques include adaptive modulation, automatic transmit power control and out-of-band filtering, and so on.

Range and Capacity

Several factors impact the amount of data capacity that can be delivered at a particular distance. Those factors include spectrum, channel bandwidth, transmitter power, terrain, noise immunity, and antenna size. In general, the longer the distance to be covered, the lower the data capacity. The longest propagation distance can be achieved by using a low-frequency narrowband channel with a high-gain antenna, while higher capacities could be achieved by selecting wider channels, with limited range. For optimal performance for each application, we need to choose the best combination of channel size, antenna, and radio power and modulation schemes to achieve the desired capacity.

A radio link can be described as being line of sight when there is a direct optical path between the two radios making up the link. A link is called non-line of sight when there is some obstruction between the two radios. Near line of sight is simply a partial obstruction rather than a complete obstruction. In general, lower-frequency solutions have better propagation characteristics than higher frequencies. Higher-frequency solutions that operate in multi-gigahertz range are typically line-of-sight or near line-of-sight systems. From 1 GHz to 6 GHz range, the propagation characteristics capabilities will vary depending on other factors, and typically below 1 GHz the propagation becomes much better, making those frequencies suitable for longer range. Figure 5-10 shows a landscape of data rates and ranges of common wireless technologies.

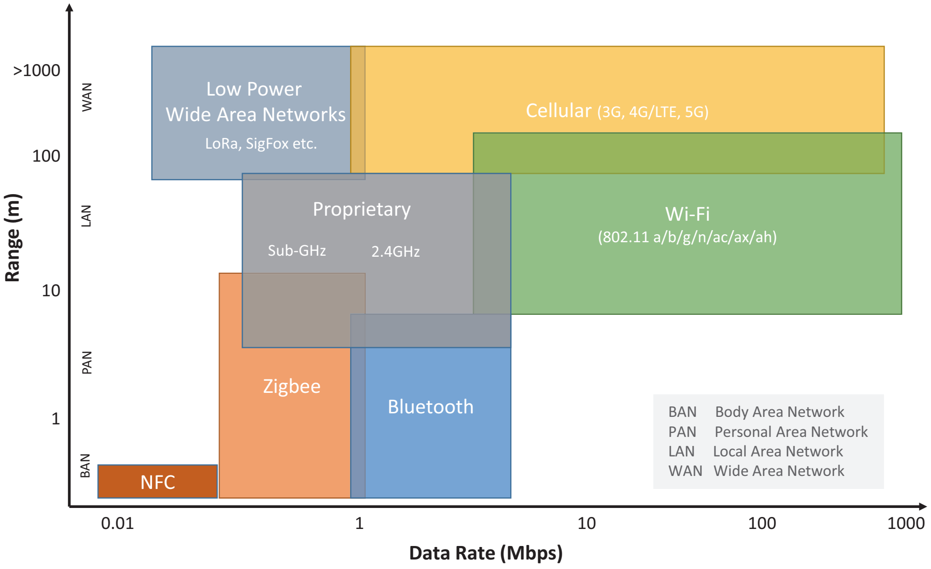

Figure 5-10. Range and data rate for various wireless technologies

Network Topology

Network topology is the arrangement of the elements in a network, including its nodes and connections between them. Common network topologies used for wireless connectivity are depicted in Figure 5-11.

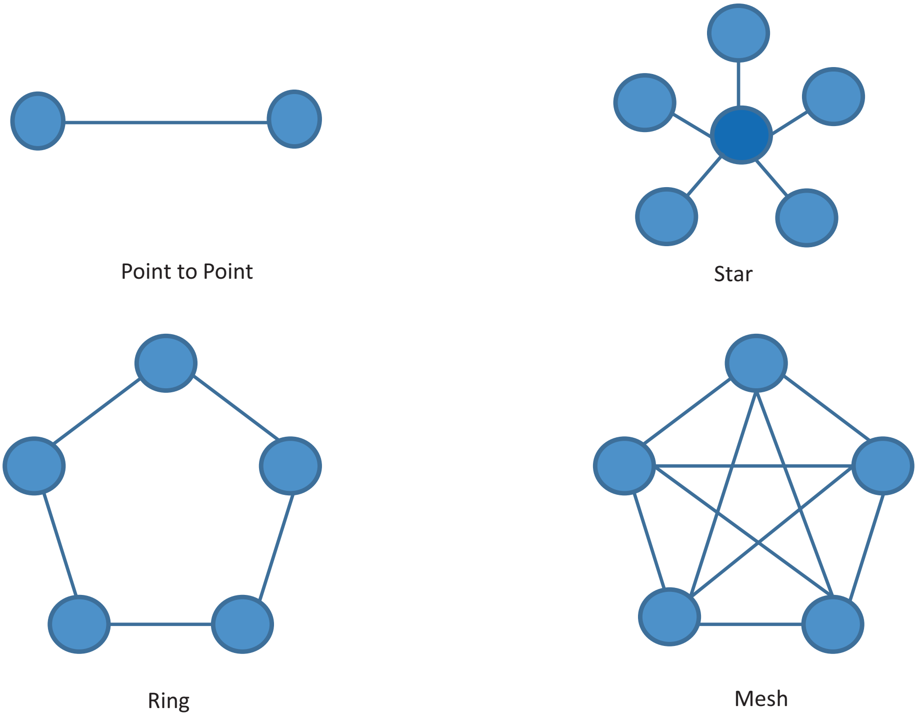

Figure 5-11. *Common network topologies*

Point-to-point topologies are best suited for delivering lots of capacity over long distances. Point-to-point connections cover longer distances that are less susceptible to interference as the antenna patterns are narrower so the energy can be focused in the direction of the desired transmission. PTP links are also used for short-range connections to the wireline backbone. Resiliency in a PTP link can be provided by deploying in 1+1 or other redundant configurations with parallel sets of radios.

Ring topologies are excellent for resilient operations of high-capacity links covering a large area. This configuration is typically used in the backhaul network.

Mesh networks can be built using multiple point-to-point links or with specialized meshing protocols to enable multiple paths from point A to point B. Mesh networks have the downside of each packet traversing multiple hops and so can lead to lower capacity and increased latency for a given infrastructure.

Point-to-multipoint (or star) networks provide scale and capacity over a geographic area. Point-to-multipoint networks are typically deployed to cover sectors or cells. The key differentiating capability to look for in point-to-point networks is their ability to scale in the number of nodes per cell but also the ability to place cells next to each other without interference.

Quality of Service

System builders and operators need to make the most efficient use of available spectrum by deploying multiple services on the same network and also making sure that mission-critical information is transmitted with highest priority. A network should support multiple Quality of Service (QoS) levels and the ability to sort traffic based on both layer 2 and layer 3 standard traffic classifiers. In this way, the transmitter of the data packet can mark the class of service or priority, and the end-to-end network will ensure that the packet is delivered with the desired level of low latency and availability.

Network Management

The capability to manage a network has a direct impact on the total cost of ownership of the IoT system. Networking systems that allow centralized management of configuration, fault detection, performance tuning and continuous monitoring, and security validation minimize the cost and effort. They also reduce unplanned outages and increase system availability and reliability.

Security

The security of wireless communications is growing in importance. Primary techniques to look for here is the ability to encrypt the over-the-air link, using a network, mesh, or link key. Besides this we need to secure management interfaces with HTTPS and SNMP. Systems should also provide the ability to create multiple user accounts with password complexity rules. Previously, many traditional automation and control solutions have not been exposed to security issues faced by the IT systems, but recently have become hacking targets as their solutions get connected to the Internet. Major security breaches could slow down the adoption of IoT.

As can be seen from Figure 5-12, several local area network (LAN) and wide area network (WAN) technologies with different levels of security and network management requirements need to work seamlessly to realize an end-to-end IoT system.

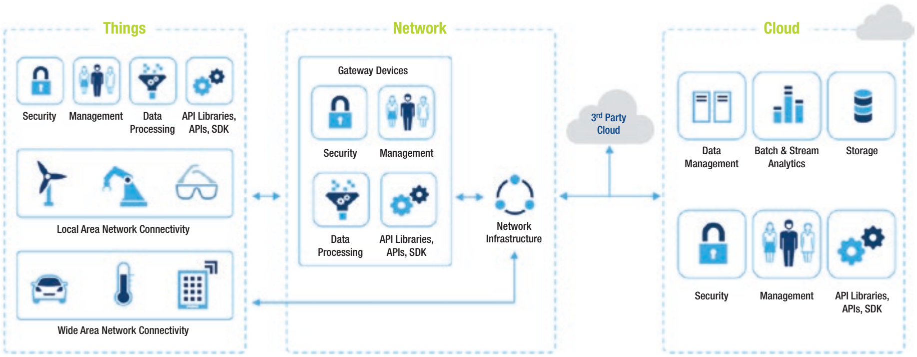

Figure 5-12. *End-to-end IoT systems need various connectivity technologies to work together*

Wi-Fi

Wi-Fi is a wireless connectivity technology based on the IEEE 802.11 standards. Initially created for wireless local area network (WLAN) applications, Wi-Fi is also increasingly used for peer-to-peer and wireless personal area network connections (WPAN). It provides secure, reliable, and fast wireless connectivity. A Wi-Fi network can be used to connect electronic devices to each other, to the Internet, and to wired networks that use Ethernet technology. It can provide real-world performance similar to that of basic wired networks. Wi-Fi networks operate in the 2.4 GHz and 5 GHz radio bands, with some products that contain both bands (dual-band). Wi-Fi is also pushing into a third band – the 60 GHz band – using ultra-wideband channels and the baseband solution originally developed by WiGig. The Wi-Fi Alliance is a wireless industry organization that promotes wireless technologies that are based on IEEE 802.11 and their interoperability. The Alliance also certifies products that comply with its specifications for Wi-Fi interoperability, security, and application-specific protocols.

Wi-Fi offers low power consumption and low cost relative to cellular. Unlike cellular, Wi-Fi operates in unlicensed spectrum, resulting also in lower data transmission costs. Range is limited by proximity to a wireless router or relays, and the quality of connection can be diminished by network congestion. There are several different Wi-Fi standards optimized for IoT applications. Next, we will take a brief look at them.

Wi-Fi Direct enables two or more devices to connect directly in the absence of a traditional Wi-Fi hotspot.

With the broad availability of the 802.11ac Wi-Fi standard, Wi-Fi operates in the 5 GHz band with wider channels (Note: 802.11n could also operate in 5 GHz but in smaller channels), thus enabling more capacity. Theoretical throughput of 11ac can exceed 1 Gbps.

Also known as Low-Power Wi-Fi, 802.11ah operates in the sub-1 GHz band. It is viewed as central to IoT, given support for extended range Wi-Fi and efficient power profile. 11ah extends Wi-Fi beyond 2.4 and 5 GHz, enabling coverage in challenging environments such as in building, basements, and so on. It also supports low-cost sensors without a power amplifier, and minimum data rates result in short-term data bursts.

802.11p is an approved standard for vehicle-to-vehicle communications. It uses dedicated short-range communications (DSRC) for applications such as toll collection, interaction between cars, and safety and roadside communications.

With the increased adoption of Wi-Fi networks for IoT applications arose the need for providing wireless network in places where connecting an access point (AP) to wired network infrastructure (e.g., a wired Ethernet switch) was not possible. A typical example would be the case of positioning an AP in the middle of a large warehouse, since the length of an Ethernet cable is limited to 100 meters. Some other use cases are the extension of an indoor wireless network to a parking lot or a campus, providing Wi-Fi coverage to outdoor industrial areas such as an oil refinery and others. Such a network can service applications like wireless security cameras, utility meters, flow and pressure sensors, vehicle tracking systems, and so on.

802.11s defines Wi-Fi mesh networking. As shown in Figure 5-13, mesh networks allow rapid deployment with lower-cost backhaul, and they make providing coverage in hard-to-wire areas easier. Inherently, mesh networks are self-healing, resilient, and extensible. Under the right conditions, they increase the range of the network due to multihop forwarding and provide higher bandwidth and better battery life due to the lower power transmissions caused by shorter hops between neighboring nodes.

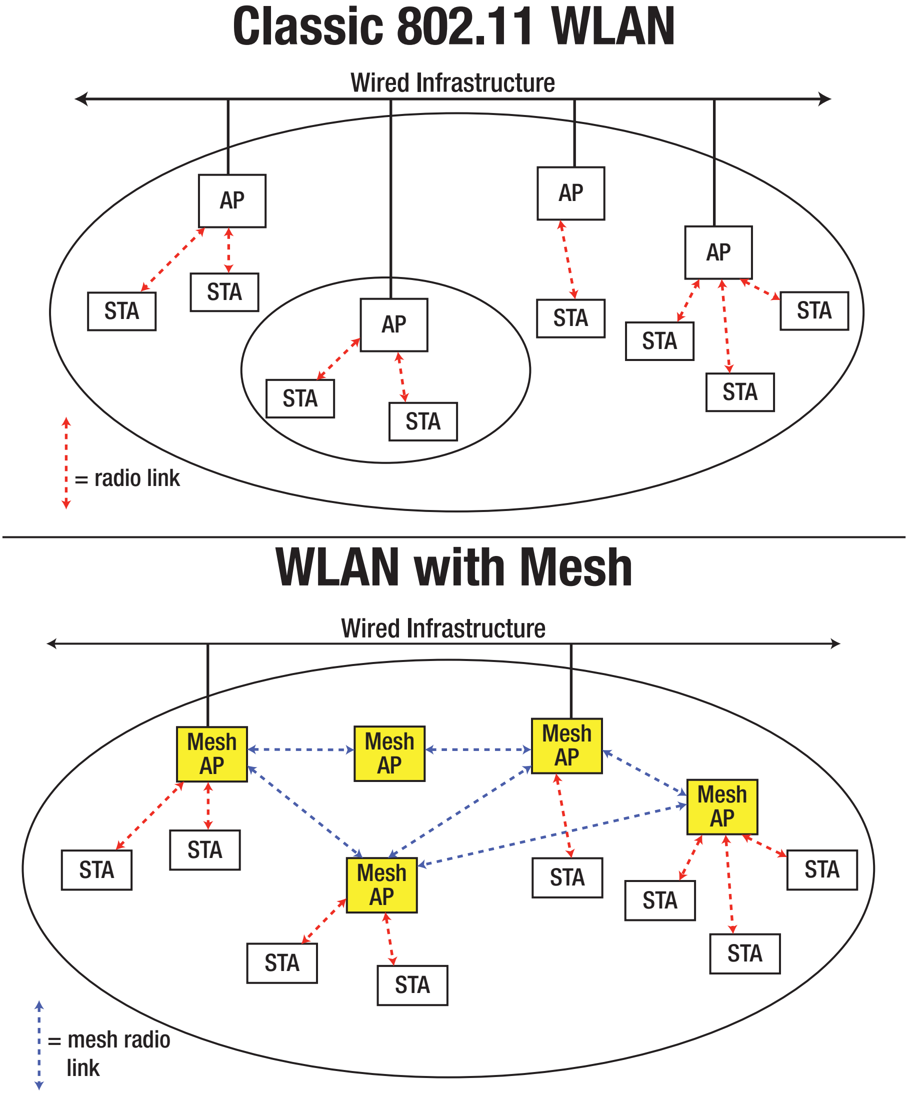

Figure 5-13. *Comparison of classic and mesh wireless local area network topologies*

Wi-Fi uses TCP/IP stack for Internet connectivity. Wi-Fi technology is hugely popular for consumer electronics and enterprise applications due to its ubiquitous presence in laptops, tablets, smartphones, and home entertainment devices. Wi-Fi access points are deployed today in many public spaces such as stadiums, airports, bus and railway stations, coffee shops, and schools. They are also present in most homes and offices. The increasing demand for cost-effective and easy Internet access along with the interoperability and ecosystem programs run by Wi-Fi Alliance has contributed to the wide adoption of this technology across the world. This worldwide availability makes Wi-Fi a natural choice for IoT connectivity, for applications that can leverage existing infrastructure without the need for custom protocol translators or gateways.

Today, most Wi-Fi networks operate in the 2.4 GHz and 5 GHz ISM (industrial, scientific, and medical) band. With more channels being available in the 5 GHz spectrum, higher data rates are possible. Wi-Fi networks have a start topology, with the access point acting as an Internet gateway. The transmit power permitted by Wi-Fi standards are high enough to enable in-home coverage in many cases. In large buildings, multiple access points and range extenders are often deployed at different locations to ensure adequate coverage and to avoid dead zones. Some Wi-Fi products support multiple antennae and transmitter and receiver chains for diversity. This helps in overcoming dead zones as well as increases data throughput.

Wi-Fi and TCP/IP software stacks are fairly complex and big in size. In traditional applications like laptops, smartphones, and tablets with adequate processing power and memory footprint, this was not a major issue. IoT devices – or things – often come with very low processing power and memory size and are typically battery powered. Till recently, adding Wi-Fi connectivity to those devices was neither practical nor cost-effective. Today, many wireless modules with embedded microcontrollers that run the TCP/IP stack and Wi-Fi software are available, thus offloading the task of networking from the main microprocessor unit. Wi-Fi devices targeted for low data rate IoT applications apply advanced sleep protocols and support fast on/off times to reduce the average power consumption dramatically. Since many IoT applications do not need the maximum data rates that Wi-Fi offers, intelligent power management techniques can efficiently draw bursts of current from the battery for very short intervals and keep products connected to the Internet for multiple years without battery replacement.

Wi-Fi modules for IoT applications typically integrate the RF frontend, thus eliminating the need for extensive radio design experience for the embedded system designer. They often come pre-certified for regulatory compliance such as FCC (Federal Communications Commission) in the United States, thus making the system certification process less time-consuming. Wi-Fi is the most ubiquitous wireless Internet connectivity technology today. Its high power and complexity has been a major barrier for IoT developers, but new silicon devices and modules reduce many of these barriers and enable Wi-Fi integration into emerging IoT applications and battery-operated devices. On the other hand, latest Wi-Fi standards offer very high bandwidth and capacity where needed, such as in video surveillance, retail, and sports arena applications. Thus Wi-Fi can support a wide variety of applications. Table 5-4 summarizes the Wi-Fi technologies currently available in the 2.4 GHz and 5 GHz spectrum.

Table 5-4. *Wi-Fi Protocol Summary*

Protocol	Frequency	Channel Width	MIMO	Maximum data rate(theoretical)
802.11ac wave2	5 GHz	80, 80+80, 160 MHz	Multi User (MU-MIMO)	1.73 Gbps[1]
802.11ac wave1	5 GHz	80 MHz	Single User (SU-MIMO)	866.7 Mbps[1]

(*continued*)

Table 5-4. (*continued*)

Protocol	Frequency	Channel Width	MIMO	Maximum data rate(theoretical)
802.11n	2.4 or 5 GHz	20, 40MHz	Single User (SU-MIMO)	450 Mbps[2]
802.11g	2.4 GHz	20 MHz	N/A	54 Mbps
802.11a	5 GHz	20 MHz	N/A	54 Mbps
802.11b	2.4 GHz	20 MHz	N/A	11 Mbps
Legacy 802.11	2.4 GHz	20 MHz	N/A	2 Mbps

[1] *2 Spatial streams with 256-QAM modulation.*

[2] *3 Spatial streams with 64-QAM modulation.*

To increase the relatively short range of Wi-Fi – specifically for IoT sensors that don't require high data rates – 802.11ah was introduced. It operates in the 900 MHz and uses target wake time to reduce the amount of energy a device needs to stay connected to the network. Devices wake up for very short times at defined intervals to accept messages. It penetrates through walls and obstructions better than high-frequency networks. It is well suited for smart building applications, like smart lighting, smart HVAC, and smart security systems. It would also work for smart city applications, like parking garages and parking meters. Since there is no global 900 MHz standard, the adoption rate of 802.11ah is currently very low. Table 5-5 summarizes the key characteristics of 802.11ah.

Table 5-5. *802.11ah Overview*

Name of Standard	IEEE P802.11ah (low power WiFi)
Frequency Band	License-exempt bands below 1 GHz, excluding the TV White Spaces
Channel Width	1/2/4/8/16 MHz
Range	Up to 1Km (outdoor)
End Node Transmit Power	Dependent on Regional Regulations (from 1mW to 1 W)
Packet Size	Up to 7,991 Bytes (w/o Aggregation), Up to 65,535 Bytes (with Aggregation)
Uplink Data Rate	150 Kbps ~ 346.666 Mbps
Downlink Data Rate	150 Kbps ~ 346.666 Mbps
Devices per Access Point	8191
Topology	Star, Tree
End node roaming allowed	Allowed by other IEEE 802.11 amendments (e.g., IEEE 802.11r)
Governing Body	IEEE 802.11 working group
Status	Targeting 2016 release

802.11ax represents the next phase of Wi-Fi. The Wi-Fi Alliance coined the term “Wi-Fi 6” when referring to the IEEE 802.11ax standard, indicating the sixth generation of Wi-Fi. Continued growth in the number of Wi-Fi-enabled devices, increased per-user traffic demand, greater number of users per access point (AP), higher-density Wi-Fi deployments, growing use of outdoor Wi-Fi, heterogeneous device and traffic types, and a desire for more power and spectral efficiency are all major driving forces behind 802.11ax. There are many 802.11ax enhancements in the 2.4 GHz band that will help increase the viability of Wi-Fi for Internet of Things

(IoT) applications. These include target wake time (TWT), orthogonal frequency-division multiple access (OFDMA), 2 MHz clients, and coexistence improvements with other IoT wireless technologies. With sub-1 GHz Wi-Fi HaLow (802.11ah) having gained very little traction to date, there is still considerable potential for 2.4 GHz Wi-Fi in the IoT. If certain 2.4 GHz 802.11ax implementations can offer comparable battery life to 802.11n, or other short-range wireless IoT connectivity solutions, it may open new opportunities for Wi-Fi across several IoT vertical applications. The standard builds on the strengths of 802.11ac while adding efficiency, flexibility, and scalability. Table 5-6 shows the major technical differences between 802.11ac and 802.11ax standards.

Table 5-6. *802.11ac and 802.11ax Comparison*

	802.11ac	**802.11ax**
Bands	5 GHz	2.4 GHz and 5 GHz
Channel Bandwith	20 MHz, 40 MHz, 80 MHz, 80+80 MHz, & 160 MHz	20 MHz, 40 MHz, 80 MHz, 80+80 MHz, &160 MHz
FFT Sizes	64, 128, 256, 512	256, 512, 1024, 2048
Subcarrier Spacing	312.5 kHz	78.125 kHz
OFDM Symbol Duration	3.2 us + 0.8/0.4 us CP	12.8 us + 0.8/1.6/3.2 us CP
Highest Modulation	256-QAM	1024-QAM
Data Rate: 1 Spatial Stream	433 Mbps (80 MHz, 1 SS)	600.4 Mbps (80 MHz, 1 SS)
Data Rate: 8 Spatial Streams	6933 Mbps (160 MHz, 8 SS)	9607.8 Mbps (160 MHz, 8 SS)

For Wi-Fi connectivity technology, security has two aspects. First is controlling who can connect to and configure the network and equipment. Second aspect deals with securing the data travelling wirelessly across your Wi-Fi network from unauthorized access by using encryption. For the overall network to be secure, one should also consider measures to protect the gateways and the connections across the Internet using virtual private network (VPN), firewalls, and so on.

Bluetooth

Bluetooth operates in the unlicensed industrial, scientific, and medical (ISM) band at 2.4 GHz using a spread spectrum, frequency hopping, and full-duplex signal at a nominal rate of 1600 hops/sec. The 2.4 GHz ISM band is available and unlicensed in most countries. Its range varies from 1 m to 100 m depending on which class of radio is used. Class 2 is the most commonly used radio. It has a range of around 10 m and uses 2.5 mW of power.

Bluetooth provides a short distance wireless connection with low power consumption, even compared to Wi-Fi. Bluetooth Low Energy (also known as Bluetooth Smart or BLE) further reduces the power consumption profile of traditional Bluetooth. For example, Bluetooth devices can sustain battery life for weeks or months, while Wi-Fi can be hours or days. Data transfer rates are somewhat limited at about 1 Mbps (though theoretical throughput is up to 24 Mbps), though the range extends up to about 100 meters (300+ feet). Similar to Wi-Fi, Bluetooth can be used for machine-to-machine connections and device pairing. Bluetooth 4.1 was introduced in December 2013, which enables devices to communicate with each other before feeding that data back to a host and interoperates with LTE.

The Bluetooth SIG controls the Bluetooth standard. Bluetooth technology was originally proposed as a standard for communications between phones and computers. The main use case that made Bluetooth initially popular was hands-free phone calls with headsets and in-vehicle infotainment systems in cars. With the advent of smartphones, high-fidelity music streaming and health and fitness accessories have also become more popular.

Bluetooth is a PAN (personal area network) technology primarily used today as a cable replacement for short-range communication. It can be used in a point-to-point or star network topology. It supports data throughputs up to 2 Mbps, with up to eight connected devices.

Original Bluetooth standard is today commonly referred to as Bluetooth Classic, to distinguish it from Bluetooth Low Energy. Bluetooth Low Energy, sometimes known as Bluetooth Smart, is an addition to the Bluetooth specification. Bluetooth SIG adopted it in the Bluetooth 4.0 standard in 2010 to enter the low-power IoT space.

Though Bluetooth Low Energy also uses the 2.4 GHz ISM band, it is not compatible with Bluetooth Classic. Bluetooth Low Energy uses 40 2 MHz-wide channels, whereas Bluetooth Classic uses 79 1 MHz-wide channels. Compared to Bluetooth Classic, Bluetooth Low Energy greatly reduces the power consumption of Bluetooth devices by supporting lower data throughput and enables lengthy lives for battery-operated devices. Bluetooth Low Energy also offers a beaconing capability and location-based services. Bluetooth Low Energy has proven to be very popular, triggering an explosion of new applications in spaces as diverse as fitness, toys, and automotive applications. It is now the main driving force behind many new Bluetooth standards.

Over the years, Bluetooth SIG has announced major revisions to the specifications to improve security, battery life, and easier interoperation with IP-based networks. For example, Bluetooth 4.2 specification added industrial strength security with elliptic curve cryptography (ECC)-based key management and Advanced Encryption Standard (AES) counter with cipher block chaining message authentication code (CCM) cryptography for message encryption.

Bluetooth 5 offers a choice of data rates and operating ranges – 2 Mbps, 1 Mbps, 500 Kbps, and 125 Kbps. The lower the data rates, the longer the ranges. The increases in range and data rate capabilities make Bluetooth Low Energy increasingly attractive in nonconsumer segments such as industrial data loggers or smart energy meters. Along with these, Bluetooth Low Energy's inherent advantage of built-in compatibility with mobile devices, it is an excellent choice for data display and retrieval, Internet connectivity, and initial provisioning and configuration of IoT devices in the field. Table 5-7 shows a comparison of Bluetooth Classic and Bluetooth Low Energy technologies.

In 2017, the Bluetooth SIG released the mesh profile and mesh model specifications. Mesh networking technology enables the use of Bluetooth Low Energy for many-to-many device communications in home automation applications such as smart lighting, low-power wireless sensor networks, and so on. It also enables extended range communication using intermediary nodes to relay the data across the network. These new mesh standards are compatible with both the Bluetooth 5 and Bluetooth 4.x standards.

Table 5-7. *Bluetooth Low Energy and Bluetooth Classic Comparison*

	Bluetooth Low Energy (LE)	**Bluetooth Classic [Basic Rate/Enhanced Data Rate (BR/EDR)]**
Optimized For…	Short burst data transmission	Continuous data streaming
Frequency Band	2.4 GHz ISM Band (2.402–2.480 GHz Utilized)	2.4GHz ISM Band (2.402–2.480 GHz Utilized)
Channels	40 channels with 2 MHz spacing (3 advertising channels/37 data channels)	79 channels with 1 MHz spacing

(*continued*)

Table 5-7. (*continued*)

	Bluetooth Low Energy (LE)	**Bluetooth Classic [Basic Rate/Enhanced Data Rate (BR/EDR)]**
Channel Usage	Frequency-Hopping Spread Spectrum (FHSS)	Frequency-Hopping Spread Spectrum (FHSS)
Modulation	GFSK	GFSK, π/4 DQPSK, 8DPSK
Power Consumption	~0.01x to 0.5x of reference (depending on use case)	1 (reference value)
Data Rate	LE 2M PHY: 2 Mb/s LE 1M PHY: 1 Mb/s LE Coded PHY (S=2): 500 Kb/s LE Coded PHY (S=8): 125 Kb/s	EDR PHY (8DPSK): 3 Mb/s EDR PHY (π/4 DQPSK): 2 Mb/s BR PHY (GFSK): 1 Mb/s
Max Tx Power*	Class 1: 100 mW (+20 dBm) Class 1.5: 10 mW (+10 dBm) Class 2: 2.5 mW (+4 dBm) Class 3: 1 mW (0 dBm)	Class 1: 100 mW (+20 dBm) Class 2: 2.5 mW (+4 dBm) Class 3: 1 mW (0 dBm)
Network Topologies	Point-to-point (including piconet) BroadcastMesh	Point-to-point (including piconet)

Security in Bluetooth mesh networking is concerned with the security of more than individual devices or connections between peer devices; it's concerned with the security of an entire network of devices and of various groupings of devices in the network. Consequently, security in Bluetooth mesh networking is mandatory. This is achieved by implementing the following fundamental security measures:

- Encryption and authentication: All Bluetooth mesh messages are encrypted and authenticated.

- Separation of concerns: Network security, application security, and device security are addressed independently.
- Area isolation: A Bluetooth mesh network can be divided into subnets, each cryptographically distinct and secure from the others.
- Key refresh: Security keys can be changed during the life of the Bluetooth mesh network via a key refresh procedure.
- Message obfuscation: Message obfuscation makes it difficult to track messages sent within the network and, as such, provides a privacy mechanism to make it difficult to track nodes.
- Replay attack protection: Bluetooth mesh security protects the network against replay attacks.
- Trashcan attack protection: Nodes can be removed from the network securely, in a way which prevents trashcan attacks.
- Secure device provisioning: The process by which devices are added to the Bluetooth mesh network to become nodes is a secure process.

Zigbee

Zigbee is based on the IEEE 802.15.4 link layer and typically operates in the 2.4 GHz ISM band. Its networking layer has been designed with mesh topology operations in mind from the ground up. This provides the ability to scale the network geographically through multihop operations (for applications such as smart meters), as well as increases fault tolerance and reliability as backup paths are created through the mesh between any two points.

Zigbee is designed, promoted, and maintained by the Zigbee Alliance. Zigbee 3.0, the latest specification, increases choice and flexibility for users and developers and delivers the confidence that products and services will all work together through standardization at all layers of the stack. Zigbee 3.0 is built on the Zigbee PRO, which enhances the IEEE 802.15.4 standard by adding mesh network and security layers along with an application framework and to become a full stack, low-power certifiable, interoperable Zigbee solution. Zigbee provides a complete solution that enables true device interoperability between different manufacturers. The Zigbee protocol suite incorporates the Zigbee cluster library: a standard library of device types, data models, and behaviors built by original equipment manufacturers (OEMs) operating in different vertical markets and proven in actual deployments for many years. A rigorous certification program managed by the Zigbee Alliance guarantees interoperability between Zigbee devices, verifying device type behavior and functionality from an end product perspective and ensuring that products from different manufacturers can operate together.

The Zigbee protocol suite includes standard commissioning, security, network, and device management procedures. Various device types can join and be authenticated in the network and be factory reset or decommissioned in an interoperable way, guaranteeing end-to-end device interoperability from the start of device operation and seamlessly integrating with data collectors or hubs.

Zigbee-based applications mostly target the smart home and smart building domains, with focus in lighting and home control and physical security segments. Many telecom, security, and Internet service providers have endorsed Zigbee as the protocol of choice when introducing their home automation services to consumers, and many lighting manufacturers have a series of smart bulbs supporting this protocol.

Zigbee takes full advantage of IEEE 802.15.4 physical radio standard and operation in unlicensed bands worldwide at 2.4 GHz (global), 915 MHz (Americas), and 868 MHz (Europe). Raw data throughput rates of 250 Kbps can be achieved at 2.4 GHz (16 channels), 10 Kbps at 915–921 MHz (27 channels), and 100 Kbps at 868 MHz (63 channels). Transmission distances range from 10 to 100 meters, depending on power output and environmental characteristics. Sub-1 GHz channel transmission ranges up to 1 km. Table 5-8 provides a quick overview of the Zigbee technology.

Zigbee effectively uses the allocated bandwidth to convey both application data to operate devices and network management procedures like mesh and routing management with a very small energy footprint. Zigbee's addressing scheme is capable of supporting hundreds of nodes per network (up to 64K), and multiple network coordinators can be linked together to support extremely large networks. The logical size of a Zigbee network ultimately depends on which frequency band is selected, how often each device on the network needs to communicate, and how much data loss or retransmissions can be tolerated by the application.

Table 5-8. *Overview of Zigbee Technical Specifications*

Solution	Description
Network Protocol	Zigbee PRO 2015 (or newer)
Network Topology	Self-Forming, Self-Healing MESH
Network Device Types	Coordinator (routing capable), Router, End Device, Zigbee Green Power Device
Network Size (# of nodes)	Up to 65,000
Radio Technology	IEEE 802.15.4-2011
Frequency Band/Channels	2.4 GHz (ISM band) 16 channels (2 MHz wide)

(*continued*)

Table 5-8. (*continued*)

Solution	Description
Data Rate	250 Kbits/sec
Security Models	Centralized (with Install Codes support) Distributed
Encryption Support	AES-128 at Network Layer AES-128 available at Application Layer
Communication Range (Average)	Up to 300+ meters (line of sight) Up to 75–100 meters indoor
Low Power Support	Sleeping End Devices Zigbee Green Power Devices (energy harvesting)

NFC

Near field communications (NFC) is a short-range wireless communication technology designed to build on existing high-frequency (HF) (13.56 MHz) contactless and RFID technology. Using 13.56 MHz on the ISM band and with a typical operating distance of up to 4 cm, today NFC enables an exchange rate of between 106 Kbps and 848 Kbps. NFC creates a short-range wireless connection able to operate in three different modes of operation: card emulation, read/write, and peer-to-peer. NFC technology enables a wide range of use cases from keyless access to e-wallet in smartphone and smart tags for medical applications. This is due to ease of implementation and the ability to embed tags into credit cards, smartphones, and other wearable devices.

GPS/GNSS

GPS is a satellite-based radio navigation system that provides users with location, velocity, and time information. A GPS receiver acquires each visible satellite's signal and measures the individual time delays. Applying these time delays to known radio wave propagation characteristics allows the distance to each satellite to be calculated. GPS accuracy correlates with the number of satellites successfully acquired by a GPS receiver. New systems are under development, such as Glonass, Galileo, and Compass, which, when used in conjunction with GPS, will improve global coverage, reduce time to fix location, and increase performance in challenging environments. Location data collected by onboard GPS trackers are vital to many applications in the transportation industry such as fleet management, asset tracking, and autonomous vehicles.

Cellular

Cellular technologies provide "always-on" connectivity to the backbone network – to the Cloud. Similar to mobile phones for consumer applications, cellular data for IoT can be connected over 2G, 3G, or 4G networks. Benefits include broad coverage leveraging existing base station infrastructure as well as mobility (e.g., cars). Potential drawbacks include power consumption, fees associated with data transfer over licensed spectrum owned by carriers, and potential gaps in coverage.

As demand for ubiquitous connectivity for IoT devices gets ever stronger, cellular networks can deliver reliable and secure IoT services using existing network infrastructure. Massive investments have been made in spectrum allocations and network deployments to ensure good coverage for the entire population in most countries. The same networks that are used to connect people can now be leveraged to connect things.

Traditional cellular options such as 2G, 3G, or higher category 4G modems consume a lot of power and don't fit well with applications where only a small amount of data is transmitted infrequently, such as smart meters, asset trackers, healthcare equipment, agriculture sensors, parking spaces, and street lights. Cellular IoT is designed to meet the requirements of such low-power, long-range applications. It takes existing technology that we already use every day for our smartphones and scales it back to meet the needs of low-power devices.

When it comes to analyzing cost of a communication solution, the total cost of ownership includes spectrum costs, infrastructure costs, and operational expenses. As cellular networks are already in place, very little new infrastructure needs to be installed. The base stations, cell towers, buildings, and power supply are already in place, all around the world. The technology also has the potential to cover hundreds of thousands of IoT devices per square kilometer – many more than other communication options.

No single technology or solution is ideally suited to all the different potential massive IoT applications, market situations, and spectrum availability. As a result, the mobile industry is standardizing several technologies, including Long-Term Evolution for Machines (LTE-M) and Narrowband IoT (NB-IoT). NB-IoT is ideally suited for low bandwidth, infrequent communication from a relatively stationary device, while LTE-M suits higher bandwidth or mobile and roaming applications.

A good application for NB-IoT is the use of remote environmental sensors to measure temperature, wind, pressure, and so on. These devices can send regular updates from a fixed location while optimizing battery use. Such a device could last for up to 10 years, or longer if solar powered and in the right geographical position.

Similarly, an asset tracker with condition monitoring through several sensors, which is mobile and roaming from country to country, is well served by an LTE-M solution that offers highway speed mobility, international roaming between countries and operators, and efficient firmware updates.

Advantages of cellular connectivity for IoT include

- The use of open standards based on existing infrastructure means coverage will reach virtually everywhere where people live.
- Many devices can operate simultaneously because of the advanced coexistence mechanisms in the LTE standard and licensed band operation, as is already proven today with the large number of cellphones used concurrently within a small area.
- No limiting regulatory regulations, so you can transmit up to 23 dBm and negotiate for as much airtime as you need.
- Standard TLS/DTLS security for end-to-end security is supported on top of the on-air encryption of the LTE network aided by the SIM credentials. This keeps data secure from the device to the cloud server.
- As cellular network coverage increases and technologies are available in low-complexity, low-power variants, cellular technology is a great choice for the world's IoT needs.

5G Cellular

The first-generation mobile network (1G) was all about voice and used analogy technology. 2G enabled voice and texting (short messaging service – SMS) using digital technology. 3G was about voice, texting, and data. 4G was everything in 3G but faster, and 5G will be even faster. 5G will be fast enough to download a full-length HD movie in seconds. The transition from 2G to 4G happened in a span of about 20 years as shown in Figure 5-14.

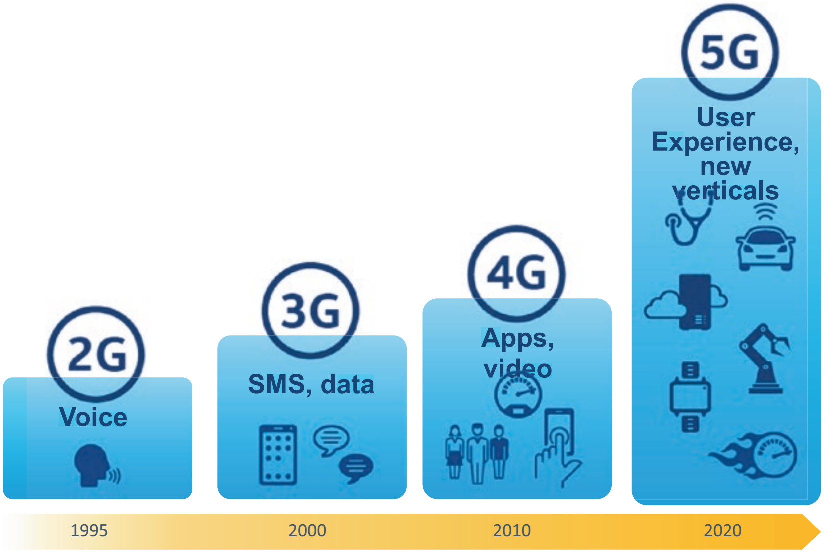

Figure 5-14. *Evolution of cellular technologies*

The real performance of a cellular network will vary by provider, their configuration of the network, the number of active connections in a given cell, the radio environment in a specific location, the capability of the device in use, plus all the other factors that affect radio performance. It is safe to assume that the throughput will be much closer to the lower bound for data throughput, and the latency will be trending toward the higher bound for packet latency for a given generation. Table 5-9 provides a summary of data rates and latency of different generations of cellular technologies.

Table 5-9. *Comparison of Data Rates and Latencies of Different Generations of Cellular Technologies*

Generation	Peak Data Rate	Practical Data Rate	Latency	Description
1G	No Data	No Data	No Data	Analog systems
2G	100s of Kbps	100–400 Kbps	300–1000 mS	First digital systems as overlays or parallel to analog systems
3G	10s of Mbps	400 Kbps–5 Mbps	100–500 mS	Dedicated digital networks deployed in parallel to analog systems
4G	100s of Mbps	1–50 Mbps	<100 mS	Digital and packet-only networks
5G	10s of Gbps	TBD	1–20 mS	Digital and packet-only networks

5G is much more than just faster networks. It supports the unique combination of high-speed connectivity, very low latency, and ubiquitous coverage, making it natively suitable for supporting IoT use cases. 5G will enable us to control more devices remotely in applications where real-time network performance is critical, enabling new user experiences in many different verticals. For example, it can be used for remote control of heavy machinery in hazardous environments, thereby improving worker safety. With its low latency, it can improve access to healthcare by enabling remote surgery. 5G connectivity will support smart vehicles and transport infrastructure such as connected cars, where the variation in delay could mean the difference between a smooth flow of traffic and an accident. It is evident that 5G will spur innovation across many industries and prove to be an enabling platform for IoT solutions to become an integral part of our economy.

Key Standards, Regulatory, and Industry Bodies Involved in 5G

There are multiple cellular standards and release versions, and the classification of any given network as 3G, 4G, or 5G is definitely too coarse. Here is a quick survey of the key players behind the evolution of various cellular technologies:

- **ITU**: (International Telecommunications Union) Agency of the UN, coordinating telecom operations and services globally. Their ITU-R sector is charged with developing future 5G standards and coordinating harmonized spectrum use.
- **3GPP**: Collaboration between seven global telecommunications standards organizations engaged in research and development of 5G standards.
- **ETSI**: Organization in Europe producing globally applicable standards for Information and Communication Technologies.
- **OCF**: Comprised of technology suppliers for product, software, platform, and silicon dedicated to driving open standards for IoT solutions.
- **IEEE**: A technical professional organization dedicated to enabling the development of new use cases and standards to accelerate time to market of technologies developed on a consensus basis.
- **5G-ACIA**: 5G Alliance for Connected Industries and Automation ensures the best possible applicability of 5G technology and 5G networks for the manufacturing and process industries by addressing, discussing, and evaluating relevant technical, regulatory, and business aspects.

New Use Cases Enabled by 5G

5G addresses existing, emerging, and future use cases. 3GPP (3rd Generation Partnership Project) has grouped the high-level use cases of 5G into three categories, based on the functionality and performance that 5G would need to enable these use cases. The three sets of use cases, primarily based on the 5G performance attributes, are listed here and are shown in Figure 5-15:

- *Enhanced Mobile Broadband (eMBB)*: Use cases requiring high data rates across a wide coverage area, providing immersive experiences such as augmented reality and virtual reality. eMBB will initially be an extension to existing 4G services and will be among the first 5G services. The three main attributes of 5G that enable eMBB use cases are

  Higher capacity: Which makes broadband access available in densely populated areas, both indoors and outdoors, like city centers, office buildings, and public venues like stadiums or conference centers.

  Enhanced connectivity: Broadband access must be available, with adequate quality of service everywhere to provide a consistent user experience.

  Higher user mobility: Will enable mobile broadband services in moving vehicles including cars, buses, trains, and even planes.

  eMBB traffic is characterized by large payloads and by a device connection pattern that remains stable over an extended time interval. This allows the network to schedule wireless resources to the eMBB devices preventing the chance of two eMBB devices accessing the same resource simultaneously. The objective of the eMBB service is to maximize the data rate while guaranteeing a moderate reliability.

- *Massive Machine-Type Communications (mMTC)*: This addresses the need to support a very large number of devices in a small area, which may only send data sporadically. IoT use cases such as smart homes, smart cities, and weather and agricultural smart sensors are good examples. A large number of mMTC devices may be connected to a given cellular network, but at a given time only a subset of them could be active and attempt to communicate their data. The large number of potentially active mMTC devices makes it infeasible to preallocate resources to individual mMTC devices. Instead, it is necessary to provide resources that can be shared through random access. The objective in the design of mMTC is to maximize the arrival rate that can be supported in a given radio resource.
- *Ultra-Reliable Low-Latency Communications (URLLC)*: These use cases impose strict requirements on latency and reliability for mission-critical communications, such as remote surgery, autonomous vehicles, or industrial control applications. The number of potential devices supported per unit area is considered to be smaller than mMTC. Supporting URLLC transmissions requires a combination of scheduling, so as to ensure a certain amount of predictability in the available resources and thus support high reliability. Random access is also required in order to ensure that too many resources do NOT idle due to the intermittent nature of scheduled traffic. Due to the low

latency requirements, a URLLC transmission should be localized in time. Diversity, which is critical to achieve high reliability, can be achieved by using multiple frequency or spatial resources. Compared to eMBB, the rate of a URLLC transmission is relatively low, and the main requirement is ensuring a high reliability level.

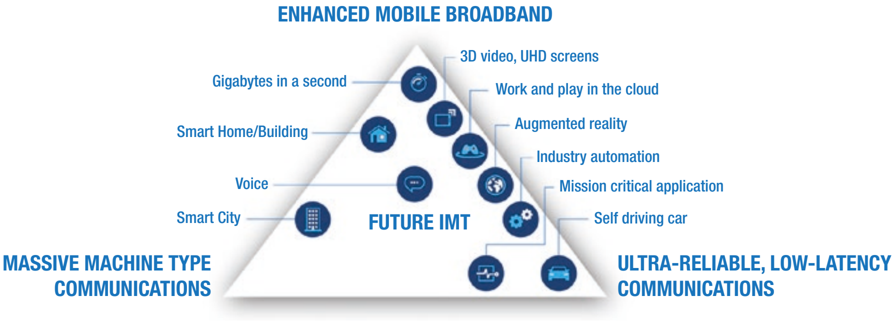
ENHANCED MOBILE BROADBAND
3D video, UHD screens
Gigabytes in a second
Work and play in the cloud
Smart Home/Building
Augmented reality
Industry automation
Voice
Mission critical application
Smart City
FUTURE IMT
Self driving car
MASSIVE MACHINE TYPE COMMUNICATIONS
ULTRA-RELIABLE, LOW-LATENCY COMMUNICATIONS

Figure 5-15. *New use cases enabled by 5G*

Key Technology Enablers for 5G

- *5G NR*: 5G New Radio is the new air interface technology being defined to support the features of 5G. The air interface specifies the radio frequency (RF) section of the connection between a mobile device and the mobile network. OFDM (orthogonal frequency-division multiplexing) family of waveforms will be used for 5G. This allows wireless network providers to more easily scale carrier bandwidth needed for each application and support diverse spectrum. 5G New Radio will use new spectrum well beyond the range of most current wireless technology, improving network availability and throughput. Massive MIMO (multiple input multiple output) technologies enable efficient use of large number of antennae and, along with 3D beamforming technologies, allow increase in capacity, coverage, and cell edge performance. The 5G NR self-contained slot structure delivers significantly lower latency than LTE thanks to support for fast uplink/downlink turnaround and scalable slot durations.

- *Network Function Virtualization (NFV)*: Today's networks are dedicated, static, and hardware resource-based and can't meet tomorrow's demands. Decoupling and shifting network functions from proprietary hardware to software-based services on open servers "virtualizes" the network. To support the many new use cases for 5G, NFV provides significant capabilities for communication service providers that will lead to more innovation, fast service deployment, and reduced operating expenses.
- *Software-Defined Networking (SDN)*: SDN is a framework for creating intelligent networks that are open, programmable, and application aware. It makes network programmable by separating the control plane (telling the network what goes where) from the data plane (sending packets to specific destinations) – centralizing and automating network engineering tasks and reducing the amount of manual intervention and coordination. This drives rapid service creation, reducing time to market for new offerings.
- *Network Slicing*: This can be employed to enable enhanced network flexibility. SDN and NFV create opportunity to "slice" networks, so that a single physical

network can be partitioned into many virtual networks. Each slice is self-contained with all necessary functions and is customized to match the level of delivery complexity required by the service-level agreement, as illustrated in Figure 5-16. Delivering customized connectivity and computing power for different types of segments, devices, and services opens new ways for communication service providers to monetize their offering. For example, they can provide third parties with access to operate their slices independently, creating new Network-as-a-Service (NaaS) business model.

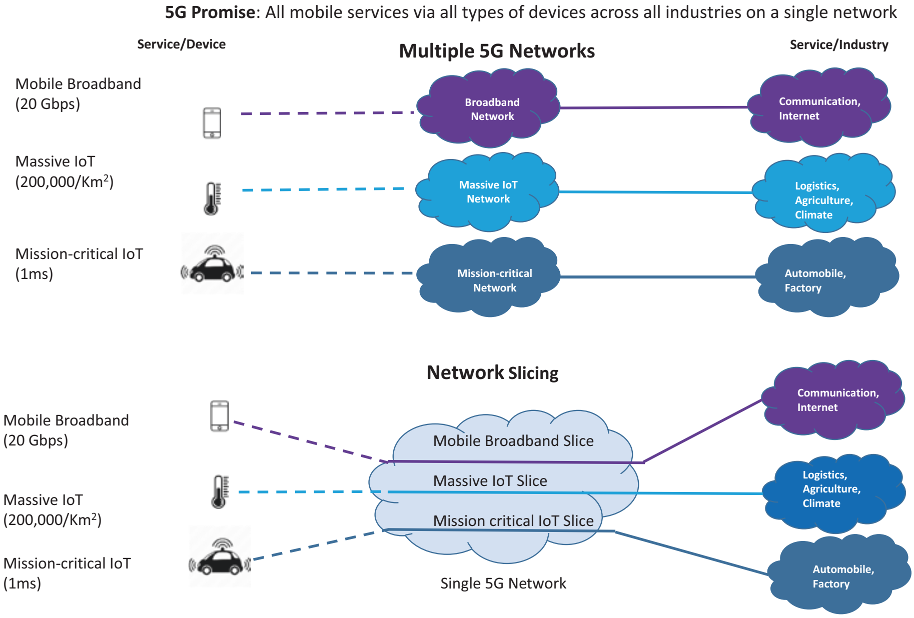
5G Promise: All mobile services via all types of devices across all industries on a single network
Service/Device
Multiple 5G Networks
Service/Industry
Mobile Broadband (20 Gbps)
Broadband Network
Communication, Internet
Massive IoT (200,000/Km^2)
Massive IoT Network
Logistics, Agriculture, Climate
Mission-critical IoT (1ms)
Mission-critical Network
Automobile, Factory
Network Slicing
Mobile Broadband (20 Gbps)
Mobile Broadband Slice
Communication, Internet
Massive IoT (200,000/Km^2)
Massive IoT Slice
Logistics, Agriculture, Climate
Mission-critical IoT (1ms)
Mission critical IoT Slice
Automobile, Factory
Single 5G Network

Figure 5-16. *Network slicing concept*

- *C-RAN*: Cloud or Centralized Radio Access Network helps to optimize network architecture by virtualizing base station functions; mobile base stations are comprised of a baseband unit (BBU), handling data processing, and a radio unit (RU), sending/receiving radio waves and managing the radio resources. Separating the BBU from the mobile base station radio unit pools data processing functions into a centralized server as shown in Figure 5-17. This allows multiple radio units to be controlled from one server reducing CAPEX and OPEX for communication service providers. This also increases the ability to address interference issue in high-density area and improves network efficiency with shared processing and load balancing.

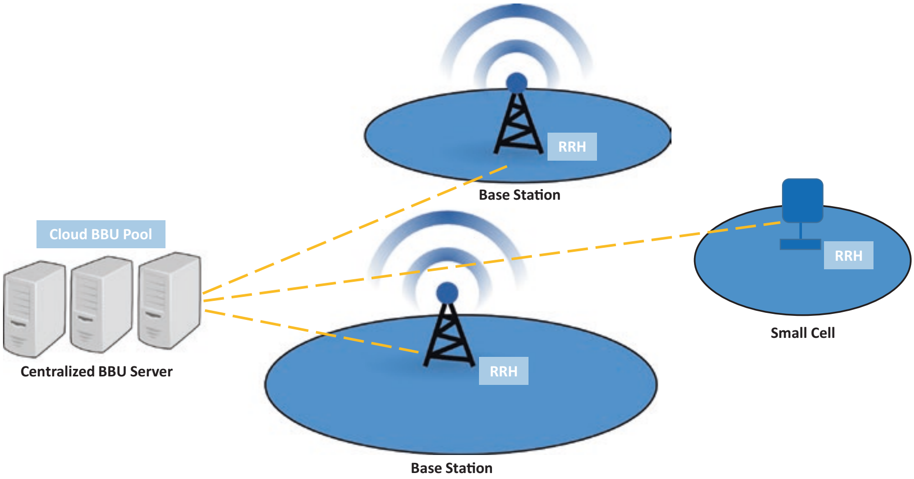

Figure 5-17. *Cloud RAN concept*

LPWAN – Low-Power Wide Area Networks

Low-power wide area network (LPWAN) technologies have low power draw and provide coverage to wide geographical areas. They provide connectivity for devices and applications that require low mobility and low speeds and infrequent data transfer, such as sensors. LPWAN technologies fill the gap between mobile cellular (3G, LTE) and short-range wireless (e.g., Bluetooth, Wi-Fi, and Zigbee) networks and are designed for machine-to-machine communications. LPWAN devices have a long battery life because they transmit only small packets of data at infrequent intervals. LPWAN solutions provide a wide area of coverage that is not limited by distance between the access points (i.e., base stations or towers) using new modulation techniques and frequency choices. They also do not typically require line-of-sight communications. They therefore require far fewer access points per unit area than traditional cellular wireless technologies.

There is no single standard for LPWAN, and there are a number of competing technologies, providing different levels of coverage and capacity. We will take a look at three of them.

LoRa

LoRa Alliance is an open, nonprofit association with over 500 members globally among telcos, system integrators, and manufacturers. LoRaWAN is an open standard with a certification program to guarantee interoperability that is governed by the LoRa Alliance. LoRaWAN network semiconductor technology is proprietary to California-based semiconductor manufacturer Semtech. See Table 5-10 for the summary of technical specifications of LoRa technology.

Table 5-10. *LoRa Overview*

Name of Standard	LoRaWAN
Frequency Band	433/868/780/915 MHz ISM
Channel Width	EU: 8x125kHz, US 64x125kHz/8x125kHz Modulation: Chirp Spread Spectrum
Range	2-5k (urban), 15k (rural)
End Node Transmit Power	EU:<+14dBm US:<+27dBm
Packet Size	Defined by User
Uplink Data Rate	EU: 300 bps to 50 kbps US:900-100kbps
Downlink Data Rate	EU: 300 bps to 50 kbps US:900-100kbps
Devices per Access Point	Uplink:>1M Downlink:<100k
Topology	Star on Star
End node roaming allowed	Yes
Governing Body	LoRa Alliance
Status	Spec released June 2015, in deployment

Sigfox

One of the most widely deployed proprietary LPWAN technologies is Sigfox, which was established in France in 2009 and deployed its first network in mid-2012. As of August 2018, there were networks in some 50 countries globally with a target of 60 by the end of the year. Table 5-11 captures the key features of Sigfox.

Table 5-11. *Sigfox Overview*

Name of Standard	SigFox
Frequency Band	868 MHz/902 MHz ISM
Channel Width	Ultra narrow band
Range	30-50km (rural), 3-10km (urban), 1000km LoS
End Node Transmit Power	-20 dBm to 20 dBm
Packet Size	12 bytes
Uplink Data Rate	100 bps to 140 messages/day
Downlink Data Rate	to 4 messages of 8 bytes/day
Devices per Access Point	1M
Topology	Star
End node roaming allowed	Yes
Governing Body	SigFox (proprietary)
Status	In deployment

Weightless

Cambridge-based Weightless SIG (Special Interest Group) was founded in 2008 to develop standards for M2M communications in white space (unused TV spectrum). Weightless originally developed three standards for different use cases which employ different technologies and provide varying levels of packet size and data rates. Today it promotes Weightless-P, which is shown in Table 5-12 – an ultra-narrowband protocol for bidirectional communications now known simply as Weightless technology.

Table 5-12. *Weightless Overview*

Name of Standard	Weightless
Frequency Band	Sub-GHZ ISM
Channel Width	12.5 kHz
Range	2km (urban)
End Node Transmit Power	17 dBm
Packet Size	10 byte min
Uplink Data Rate	200 bps to 100 kbps
Downlink Data Rate	same
Devices per Access Point	Unlimited
Topology	Star
End node roaming allowed	Yes
Governing Body	
Status	In deploymnet

Comparison of Low-Power LTE and Other LPWAN Technologies

There are several technologies upon which LPWANs can be based as seen earlier and can be classified into those based on proprietary systems and those based on open standards.

Low-power Long-Term Evolution (LTE) has taken off since the 3rd Generation Partnership Project (3GPP) introduced a specification for two forms of the technology – LTE-M and Narrowband-IoT (NB-IoT) – in Release 13 of the standard. The new specification makes it easier for manufacturers to design and develop the inexpensive, compact, and low power consumption wireless LTE modems that LPWANs demand.

LTE is an open standard, operates in a licensed portion of the RF spectrum, leverages existing infrastructure for coverage, and has coexistence mechanisms that enable scaling to high node counts per base station.

Low-power LTE operates in up to 44 different licensed frequencies across the world, ranging from 450 MHz to 2.6 GHz. By using the licensed spectrum, the owners of the spectrum allocation (the carriers) can control and prioritize data, and the bands are immune from interference from other sources of RF radiation.

Because the spectrum allocation isn't shared with other RF transmissions, the coexistence between connected devices is much easier to manage. LTE's coexistence technology is based on proven frequency- and time-domain solutions and other mechanisms such as "autonomous denials" of conflicting RF signals. Consequently, LTE can support a node density of up to 200,000 active low-power modems per base station. Finally, data carried over LTE is safe from prying eyes because the standard has incorporated advanced security from its inception. These features ensure that carriers can offer reliability and high quality of service.

In contrast, proprietary technologies limit the participation in the vendor ecosystem and innovation in technology evolution over time. As they operate in unlicensed allocations of the RF spectrum (typically sub-1 GHz), coexistence could also be a challenge. They must share RF spectrum with many other services. While basic interference avoidance techniques are employed, so many services are sharing the spectrum allocation that it is extremely to match the node density, reliability, and quality of service of LTE.

Proprietary LPWAN vendors are also faced with the major challenge of building infrastructure to support their networks. These are likely to be expensive and long-winded projects slowing adoption. In contrast, worldwide LTE infrastructure is largely in place comprising 480 networks in 157 countries. Some upgrading (mainly of software) is required to support low-power LTE, but this is relatively a less complex effort compared to building the infrastructure in the first place. Because the infrastructure is installed, support for low-power LTE is likely to be added rapidly, further encouraging its uptake.

Companies adopting low-power LTE for their IoT-connected products can leverage this infrastructure without bearing its build or maintenance costs, instead investing in their own services and business models.

A Case Study – Smart Homes

A typical smart home gateway is illustrated in Figure 5-18.

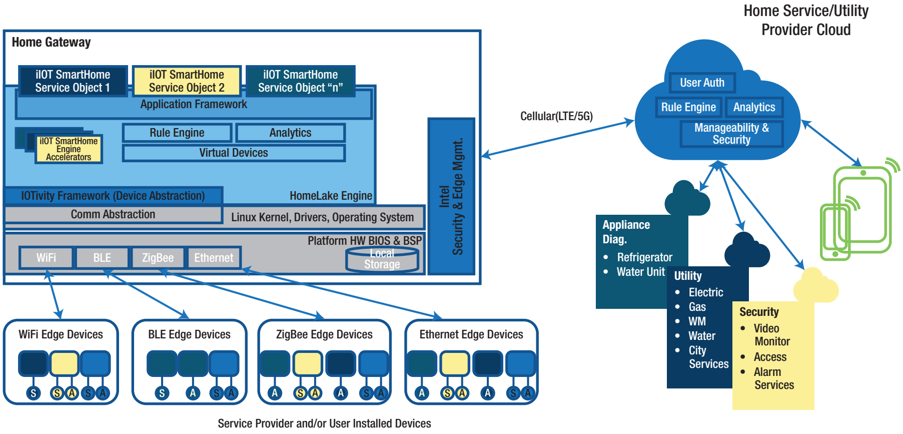

Figure 5-18. *Smart home system using multiple connectivity technologies*

In reality, many IoT endpoints and gateways will employ multiple communication technologies based on cost, improved flexibility, and interoperability. A primary example is connected thermostat which incorporates both Wi-Fi and ZigBee. Many smart meters support cellular, ZigBee, RF mesh, and Wi-Fi capabilities. A key advantage of Wi-Fi and Bluetooth is that they are already embedded in essentially all smartphones. This type of coexistence of multiple technologies in a single system is illustrated in the smart home IoT system example shown earlier. The gateway supports Wi-Fi and Ethernet for LAN connections that need higher bandwidth such as audio and video applications. PAN and mesh networks based on Bluetooth Low Energy and ZigBee are used for energy-efficient sensors and controllers for lighting, security, and so on. The gateway provides WAN connectivity to Cloud using cellular technologies like LTE and 5G. Local analytics and intelligences provided by the gateway. The cloud service providers enable cloud-based applications to deliver the various services.

Summary

There are many connectivity technologies that can be used for enabling IoT. Each one has its own benefits and shortcomings. One should choose a technology or a combination of technologies that is best suited for the application. Cost, ease of system integration, and security should also be considered along with features such as throughput, range, power consumption, network topology, and existing infrastructure.

The IEEE has already standardized dozens of use cases and applications for IoT protocols. In addition to the basic communications standards discussed earlier (layer 2 in the OSI stack), which handle the underlying communications, there is a need for standardization at higher layers of the stack as well. Working groups belonging to many industry alliances such as OPC Foundation, Industrial Internet Consortium, 5G-ACIA, and ZigBee Alliance and standardization bodies such as ETSI coordinate and establish the priorities and enabling technologies of the Industrial Internet in order to accelerate market adoption and drive down the barriers to entry.

References

1. IEEE Time-Sensitive Networking Task Group: https://1.ieee802.org/tsn/

2. P60802 – Time-Sensitive Networking Profile for Industrial Automation: https://standards.ieee.org/project/60802.html

3. Wi-Fi Alliance: www.wi-fi.org/discover-wi-fi

4. Bluetooth SIG: www.bluetooth.com/bluetooth-resources

5. Zigbee Alliance: www.zigbee.org/zigbee-for-developers/zigbee-3-0/

6. 3GPP: www.3gpp.org/

7. Industrial Internet Consortium: www.iiconsortium.org/

8. OPC Foundation: https://opcfoundation.org/

9. 5G Alliance for Connected Industries and Automation (5G-ACIA): www.5g-acia.org/

10. Time-Sensitive Networking Standards: IEEE Communications Standards Magazine (Volume: 2, Issue: 2, JUNE 2018). https://ieeexplore.ieee.org/document/8412457

11. Avnu Alliance: The Business Impact of TSN for Industrial Systems Whitepaper. https://avnu.org/business-impact-paper/

12. Time-Sensitive Networking: From Theory to Implementation in Industrial Automation. www.intel.com/content/dam/www/programmable/us/en/pdfs/literature/wp/wp-01279-time-sensitive-networking-from-theory-to-implementation-in-industrial-automation.pdf

13. Ultra-Low Latency (ULL) Networks: The IEEE TSN and IETF DetNet Standards and Related 5G ULL Research. https://arxiv.org/pdf/1803.07673.pdf

14. A Survey on 5G Networks for the Internet of Things: Communication Technologies and Challenges. https://ieeexplore.ieee.org/document/8141874

15. 5G Technology Overview, Intel: www.intel.com/content/www/us/en/wireless-network/5g-technology-overview.html

16. Intel Wireless Solutions: www.intel.com/content/www/us/en/products/wireless.html

17. Intel® IoT Industry Solutions for Smart Manufacturing: www.intel.com/content/www/us/en/internet-of-things/infographics/iot-industry-solutions-smart-manufacturing-infographic.html

18. Smart Homes with Intel® Internet of Things (IoT) Technologies: www.intel.com/content/www/us/en/internet-of-things/smart-home.html