WHITE PAPER

Gil Reiter
IoT strategic marketing manager
Texas Instruments

Texas Instruments

Wireless connectivity for the Internet of Things

One size does not fit all

Introduction

In the rapidly growing Internet of Things (IoT), applications from personal electronics to industrial machines and sensors are getting wirelessly connected to the Internet. Covering a wide variety of use cases, in various environments and serving diverse requirements, no single wireless standard can adequately prevail. With numerous standards deployed in the market, spreading over multiple frequency bands and using different communication protocols, choosing the right wireless connectivity technology for an IoT application can be quite challenging. In this paper we review the predominant wireless connectivity technologies in the market, discuss their key technical concepts and engineering tradeoffs and provide guidelines for selection of the right wireless technology for different applications.

Frequency bands and worldwide regulations

Radio transmissions are regulated worldwide by agencies such as the Federal Communications Commission (FCC) in the United States and the Conference of Postal and Telecommunications Administrations (CEPT) in Europe. These organizations allocate frequency bands for specific use and drive standards and certification plans for radio transmitters. Most of the usable spectrum in most regions is designated as *licensed*, i.e., users need to buy a license from the local regulator to operate a radio transmitter in a designated frequency channel. A familiar example for licensed frequency bands use is cellular communication. Government auctions are used worldwide to sell spectrum bands to mobile operators to regulate commercial frequency allocation.

The International Telecommunication Union's Radio communication sector (ITU-R), which coordinates the shared global use of radio spectrum, has reserved several frequency bands for Industrial, Scientific and Medical (ISM) applications. ISM bands are *unlicensed*, and vary slightly from country to country. Popular ISM bands in recent years are 433 MHz, 868 MHz, 915 MHz and 2.4 GHz, which are used by wireless communication systems such as remote controls, cordless phones and Wi-Fi® respectively. Figure 1 shows a map of popular ISM

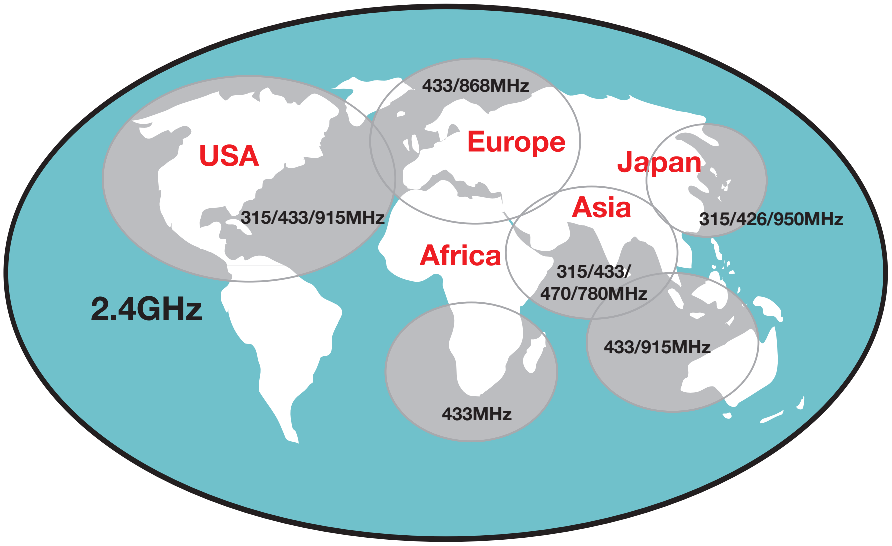

Figure 1. Worldwide unlicensed frequency bands

bands allocated worldwide. The 2.4 GHz band became very popular because it is allowed for unlicensed use in all regions. The ubiquity of the 2.4 GHz band makes development and distribution of 2.4 GHz-based products across nations easier.

As a general rule, higher frequency bands offer more channels and more bandwidth, hence can serve larger networks and drive more data throughput. Lower frequency radio waves propagate better than higher frequency; therefore they can achieve better range, especially inside buildings.

Communication protocols

Communication systems utilize a set of rules and standards to format data and control data exchange. The most common model in data communication systems is the Open Systems Interconnection (OSI) model, which breaks the communication into functional layers allowing easier implementation of scalable and interoperable networks. The OSI model has 7 layers; a 4-layer simplified version of the model is shown in Figure 2 along with example of the TCP/IP stack.

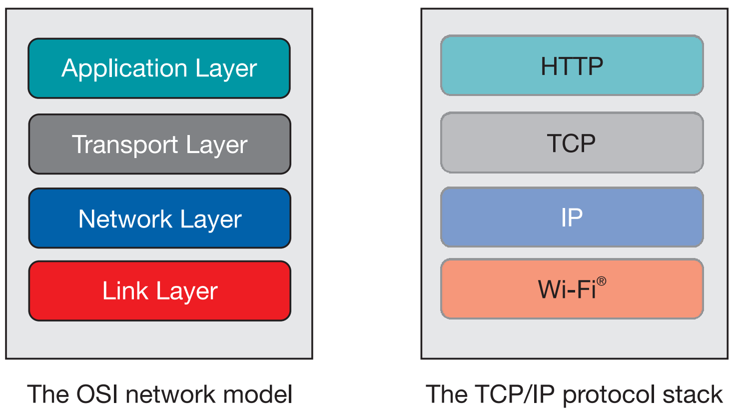

Figure 2. Simplified OSI model (left) and an example of a TCP/IP protocol stack (right)

The ***Link layer*** provides conversion of bits to radio signals (and vice versa), takes care of data framing for reliable wireless communication and manages the access to the radio channel. In the TCP/IP example in Figure 2, Wi-Fi is shown as the link layer protocol.

The ***Network layer*** addresses and routes data through the network. IP (Internet Protocol) is the network layer protocol of the Internet, providing an IP address to devices and carrying IP packets from one device to another.

The ***Transport layer*** generates communication sessions between applications running on two ends of the network. It allows multiple applications to run on one device, each using its own communication channel. TCP (or Transmission Control Protocol) is the predominant transport protocol in the Internet.

The ***Application layer*** is responsible for data formatting and it governs the data flow in an optimal scheme for specific applications. A popular application layer protocol in the TCP/IP stack is HTTP (or Hyper-text Transfer Protocol) which was created to transfer web content over the Internet.

A layered network implementation introduces complexity and requires more code and memory. It also introduces data overheads because every layer requires additional framing and control messages. On the other hand, layered networks enable more flexibility and scale – so much so that most wireless networks today are designed using a similar scheme to the one in Figure 2. One example of a simple network design, with no or little layering, is a proprietary application protocol running directly over the physical layer provided by a simple radio transceiver. A proprietary implementation like this can be very efficient, but it is mainly used in simple, single-function networks.

To IP or not to IP

The IoT is all about connecting things to the Internet. Devices that are (directly) connected to the Internet must use the IP suite to be able to exchange data with devices and servers over the Internet. Nevertheless, devices in a local network can use non-IP protocols to communicate within the local network. Connectivity to the Internet of non-IP devices can be achieved via an Internet gateway. The gateway communicates with local devices using a non-IP method on one side, and with other devices on the Internet using IP on the other side. The gateway in this case is an *application layer gateway* because it needs to strip down the data coming in from the local network and restructure it with a TCP/IP stack to enable communication with an Internet service.

The benefit of using the IP in devices is that it allows the gateway to be application agnostic and enables flexibility to modify or add applications to the devices without changing anything on the gateway. The reason we can install new Internet applications on our laptops without changing anything in our home network is because our laptop runs a TCP/IP stack, and home routers (using a wired Ethernet or Wi-Fi) are only manipulating data at the Link layer.

In many cases, a local network is formed for one specific application. For example, alarm systems with wireless sensors form a local network with one function – sending sensor activation messages to the alarm controller. If the alarm controller is relaying messages to your phone over the Internet, then it uses TCP/IP. But the communication between the sensors and the alarm controller does not have to be based on TCP/IP. In fact, in most cases today, it is not.

Other, often overlooked, advantages of the TCP/IP stack come from the unprecedented widespread use of Internet applications. The number of application protocol implementations created for TCP/IP over the last 20 years is overwhelming. Many of them can be used in a local network, even if Internet connectivity is not required. Reusing existing proven protocol implementations can dramatically shorten development time. Tools for diagnostics, management and commissioning of IP networks already exist and can help shorten development cycles as well.

One of the disadvantages of the TCP/IP stack is that it is fairly complex and large, and therefore requires a fair amount of processing power and sizeable memory, implying more development time and more expensive devices. The complexity also results in larger data packets, hence consuming more power to send and receive. For these reasons many simple networks, such as the wireless sensors in the alarm system example, choose to implement simpler and often times proprietary protocols.

As silicon technology advances, processing power and memory become more available and affordable. With wireless network processors and wireless microcontrollers (MCUs) available today, TCP/IP communication becomes more attractive than ever, even for small and simple networks. With integration of a full TCP/IP stack into products like TI's SimpleLink™ family, we expect more and more applications to move from proprietary protocols to IP-based protocols, enabling flexible Internet connectivity and faster development cycles.

Network range

As shown in Figure 3, a network's range is typically categorized into four classes: Personal Area Network (PAN), Local Area Network (LAN), Neighborhood Area Network (NAN) and Wide Area Network (WAN).

Figure 3. Different ranges and applications for personal, local, neighborhood and wide area networks.

PANs are usually wireless and cover a range of about 10 meters. A common wireless PAN is a smartphone connected over *Bluetooth*® to handful of accessories such as wireless headset, watch or fitness device. Wireless PAN devices usually have low radio transmission power and run over small batteries.

LANs are either wired or wireless (or a combination of the two). Wireless LANs (WLANs) usually cover a range up to 100 meters. A predominant example is a home Wi-Fi network providing Internet access to personal computers, smartphones, TVs and today even to IoT devices such as thermostats and home appliance.

NANs are usually wireless and can reach more than 25 km. They transmit high power levels, but usually relay relatively low data traffic. An example of NAN is a smart grid network used to transmit electric meters readings from homes to the utility company using a proprietary protocol over a 900-MHz radio.

Finally, WANs are spread across a very large area – as big as the entire globe. The Internet is considered a WAN and it is built of a complex mix of wired and wireless connections.

Network topology and size

Wireless networks can be also be categorized by their *topology* – the way nodes in the network are arranged and connected to each other. The first two fundamental network topologies are ***star*** and ***mesh*** as depicted in Figure 4. In a star topology, all the nodes are connected to one central node, which is typically also used as the gateway to the Internet. A popular example of a star topology is a Wi Fi network, where the center node is called an *access point* (AP) and the other nodes are called *stations*.

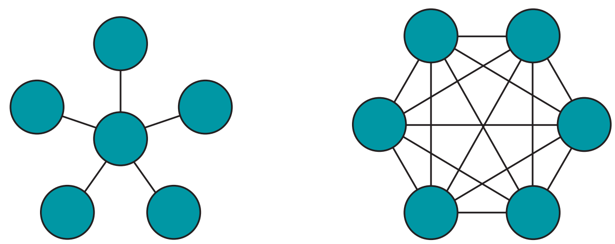

Figure 4. Star topology (left) and Mesh topology (right)

In a mesh network, every node can connect to multiple other nodes. One or more nodes in the network serve as an Internet gateway. In the example of Figure 4 every node in the network is connected to every other node. In real life mesh topology is simpler. A popular example of a mesh network is a ZigBee® Light Link™ network where multiple lights form a mesh network to extend the network reach in large buildings. One of the ZigBee nodes is called a coordinator, and it usually serves also as an Internet gateway.

However, mesh networks are more complex to design and can exhibit a longer delay routing a message from a remote node through the mesh, compared to star networks. The benefit of a mesh topology is that it can extend the range of the network through multiple hops, while maintaining low radio transmission power. They can also achieve better reliability by enabling more than one path to relay a message through the network.

Network size, or the maximum number of simultaneously connected devices, is also an important consideration in system design. Some technologies like *Bluetooth* support up to 20 connections; others technologies, like ZigBee, can support thousands of connections.

Standards and interoperability

One of the biggest challenges in communication systems is interoperability – the ability of devices from different vendors to exchange data. Addressing this challenge is the main goal of many standards organizations that define specifications and testing procedures designed to assure interoperability between devices. Recalling the OSI network model from Figure 2 – some standards define one or several network layers, while others define the entire end-to-end network specifications.

The Institute of Electrical and Electronics Engineers (IEEE) is a nonprofit organization formed in 1963. It has a considerable focus on communication and radio engineering, and one of its well-known contributions to the networking technology is the IEEE *802.x* family of standards. To name a few members of the 802.x family – *802.3* defines the Ethernet specification, which governs most wired computer networks today. *802.11* defines the WLAN specification, which is the baseline of the Wi-Fi standard, *802.15.4* defines the wireless PAN standard used in ZigBee, 6LoWPAN and WirelessHART. It is important to point out that the 802.x standards define only the *link layer* of the network.

The Internet Engineering Task Force (IETF) is an open standard organization formed in 1986 that is responsible for development of Internet standards, particularly the TCP/IP suite. IETF specifications are established through the publication of draft specifications under the title “request for comments” (RFCs). An RFC is followed by multiple reviews and edits done by IETF members until the specification is approved to a “best current practice” status. There are thousands of Internet standards defined by RFCs. A few examples are RFC 791, which describes the IPv4 protocol; RFC 793, which describes the TCP protocol, and RFC 2616, which defines the HTTP/1.1 protocol.

The IETF, like the IEEE, does not run certification programs. That is, vendors cannot get recognition from either one of these organizations that their products comply with any of the standards. The IEEE and the IETF standards set good practices for implementation. Other organizations adopt standards from IEEE and IETF and use them to create certification programs. These organizations often adopt just a portion of an IEEE or an IETF standard for various reasons.

Three well-known organizations that manage certification programs today to assure interoperability between wirelessly connected devices are the Wi-Fi Alliance, the Bluetooth Special Interest Group (SIG) and the ZigBee Alliance. All three organizations provide member companies the option to take products through an interoperability test plan, which grants rights to wear the Wi-Fi, Bluetooth or ZigBee logo.

So far we have reviewed some of the key concepts in wireless connectivity and discussed engineering tradeoffs in wireless connectivity system design. Next we will cover the predominant wireless connectivity technologies in the industry and their applications in more detail.

Wi-Fi technology, based on the IEEE 802.11 standard, was developed as a wireless replacement for the popular wired IEEE 802.3 Ethernet standard. As such, it was created from day one for Internet connectivity. Although Wi-Fi technology primarily defines the link layer of a local network, it is so natively integrated with the TCP/IP stack, that when people say they are using Wi-Fi they implicitly mean that they are also using a TCP/IP for Internet connectivity.

Riding on the huge success of smartphones and tablets, Wi-Fi has become so ubiquitous that people often refer to it as just “wireless.” Wi-Fi APs are deployed today in most homes, as well as in almost all offices, schools, airports, coffee shops and retail stores. The huge success of Wi-Fi is largely due to the remarkable interoperability programs run by the Wi-Fi Alliance and to the increasing demand in the market for easy and cost-effective Internet access.

Wi-Fi is integrated already into all new laptops, tablets, smartphones and TVs. Taking advantage of the existing vast deployed infrastructure in homes and enterprise, Wi-Fi's natural next step is to connect the new age of things to the Internet.

Wi-Fi networks have a star topology, with the AP being the Internet gateway. The output power of Wi-Fi is high enough to allow full in-home coverage in most cases. In enterprise and in large buildings, more than one AP is often deployed in different locations inside the building to increase the network coverage. In large concrete buildings dead spots may be found due to multipath conditions. To overcome dead signal receptions spots in some cases, various Wi-Fi products include two antennas for diversity.

Most Wi-Fi networks operate in the ISM 2.4-GHz band. Wi-Fi can also operate in the 5-GHz band where more channels exist and higher data rates are available. However, since the range of 5-GHz radios inside buildings is shorter compared to 2.4 GHz, 5 GHz is mainly used in enterprise applications along with multiple APs to ensure good Wi-Fi coverage.

Wi-Fi and TCP/IP software are fairly large and complex. For laptops and smartphones with powerful microprocessors (MPUs) and large amounts of memory, this imposes no issue. Until recently, adding Wi-Fi connectivity to devices with little processing power such as thermostats and home appliances was not possible or not cost effective. Today, silicon devices and modules coming out on the market embed the Wi-Fi software and the TCP/IP software inside the device. These new devices eliminate most of the overhead from the MPU and enable wireless Internet connectivity with the smallest microcontroller (MCU). The increasing level of integration in these Wi-Fi devices also eliminates all required radio design experience and reduces the barriers of Wi-Fi integration.

To enable high data rates (over 100MBps in some cases) and good indoor coverage, Wi-Fi radios have fairly large power consumption. For some IoT devices, which run on batteries and cannot be charged frequently, Wi-Fi can be too power hungry. Although the peak current of Wi-Fi radios cannot be reduced by much, new silicon devices apply advanced sleep protocols and fast on/off time to reduce the average power consumption dramatically. Since most IoT products do not need the maximum data rates Wi-Fi offers, clever power management design can efficiently draw bursts of current from the battery for very short intervals and keep products connected to the Internet for over a year using two AA alkaline batteries. Today you can buy a Wi-Fi based sports watch that uploads workout data to the Internet.

Most Wi-Fi APs claim support for up to 250 simultaneously connected devices. Enterprise-grade APs can support even larger number of connections, and some popular consumer APs handle no more than 50.

To summarize, 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 the barriers and enable Wi-Fi integration into emerging IoT applications and battery-operated devices.

Bluetooth technology, named after an ancient Scandinavian king, was invented by Ericsson in 1994 as a standard for wireless communication between phones and computers. The *Bluetooth* link layer, operating in the 2.4-GHz ISM band, was previously standardized as IEEE 802.15.1, but today the IEEE standard is no longer maintained and the *Bluetooth* standard is controlled by the *Bluetooth* SIG.

Bluetooth became very successful in mobile phones, so much that all mobile phones today, even entry level phones, have *Bluetooth* connectivity. The main use case that made *Bluetooth* popular initially was hands-free phone calls with headsets and car kits. Thereafter, as mobile phones became more capable, more use cases like high-fidelity music streaming and data-driven cases such as health and fitness accessories evolved.

As mentioned earlier, *Bluetooth* is a PAN technology primarily used today as a cable replacement for short-range communication. It supports data throughput up to 2MBps, and although more complex topologies are included in its specifications, *Bluetooth* is primarily used in a point-to-point or in a star network topology. The technology is fairly low power; devices typically use small rechargeable batteries, or two alkaline batteries.

Bluetooth Low Energy (also known as Bluetooth Smart) is a more recent addition to the *Bluetooth* specification. Designed for lower data throughput, Bluetooth low energy significantly reduces the power consumption of *Bluetooth* devices and enables years of operation using coin cell batteries. Supported by the new generation of smartphones and tablets, Bluetooth low energy has accelerated the *Bluetooth* market growth and enabled a wide range of new applications spanning health and fitness, toys, automotive and industrial spaces. Bluetooth low energy also introduced proximity capabilities that opened the door to location-based services like beaconing and geo-fencing applications.

The *Bluetooth* "classic" standard can support up to eight devices connected in a star network simultaneously. The Bluetooth low energy standard removes this limitation and can theoretically support an unlimited number of devices, but the practical number of simultaneously connected devices is between 10 and 20.

One of the advantages of the *Bluetooth* standard is that it includes application *profiles*. These profiles define in great detail how applications exchange information to achieve specific tasks. To name one example, the *Audio/Video Remote Control Profile* (AVRCP) defines how a *Bluetooth* remote control interfaces with audio and video equipment to relay commands like play, pause, stop, etc. The comprehensive certification programs defined by the *Bluetooth* SIG cover the entire protocol stack as well as the application profile, helping *Bluetooth* achieve excellent interoperability in the market.

So how is *Bluetooth* related to IoT? It connects wireless accessories the last 10 meters to a smartphone or tablet, which acts as an Internet gateway. A wearable heart rate monitor logging its data on a fitness cloud server, and a phone-controlled door lock reporting its status to a security company are just two examples of the many IoT applications enabled by *Bluetooth* technology.

ZigBee technology is interestingly named after the *Waggle Dance* that bees do when coming back from a field flight, to communicate to others in their hive the distance, direction and type of food they found. This analogy hints to the mesh nature of ZigBee, where data hops from node to node in multiple directions and paths throughout large scale networks.

Based on the IEEE 802.15.4 link layer standard, ZigBee is a low-throughput, low-power and low-cost technology. It mainly operates in the 2.4-GHz ISM band although the spec also supports the 868-MHz and 915-MHz ISM bands. ZigBee can deliver up to 250KBps of data throughput, but is typically used at much lower data rates. It also has the capability to maintain very long sleep intervals and low operation duty cycles to be powered by coin cell batteries for years. New ZigBee devices coming to the market can even enable energy harvesting techniques for battery-less operation.

The ZigBee standard is maintained by the ZigBee Alliance. The organization runs certification programs ensuring interoperability between devices, which allow products to wear the ZigBee Certified logo. The standard defines the higher networking layers on top of the 802.15.4 link layer and various application profiles enable full-system interoperable implementations. ZigBee can be used in multiple applications, but it has gained the largest momentum and success in *smart energy*, *home automation* and in *lighting control* applications, each of which has a specific ZigBee profile and certification. Another reason the ZigBee standard has done so well in these application areas is because of the mesh network topology that can include up to thousands of nodes.

Although the ZigBee standard has an *IP specification*, it is separated from the popular *smart energy*, *home automation* and *light link* profiles, and has not gotten much traction in the industry. To connect to the IoT, ZigBee networks require an application-level gateway. The gateway participates as one of the nodes in the ZigBee network and in parallel runs a TCP/IP stack and application over Ethernet or Wi-Fi to connect the ZigBee network to the Internet.

6LoWPAN is an acronym for *IPv6 over Low power Wireless Personal Area Networks*. The promise of 6LoWPAN is to apply IP to the smallest, lowest-power and most limited processing power device. 6LoWPAN is really the first wireless connectivity standard that was created for the IoT. The term “Personal Area Networks” within the 6LoWPAN acronym can be confusing because 6LoWPAN is typically used to form LANs.

The standard was created by the 6LoWPAN working group of the IETF and formalized under RFC 6282 “Compression format for IPv6 datagrams over IEEE 802.15.4-based networks”, in September 2011. As indicated by the RFC title, the 6LoWPAN standard only defines an efficient adaptation layer between the 802.15.4 link layer and a TCP/IP stack.

The term 6LoWPAN is loosely used in the industry to refer to the entire protocol stack that includes the 802.15.4 link layer, the IETF IP header compression layer and a TCP/IP stack. But sadly, there is no industry standard for the entire protocol stack, nor is there a standard organization to run certification programs for a 6LoWPAN solution. Since the 802.15.4 link layer has multiple optional modes, different vendors can implement solutions that are not interoperable at the local network level, and still call all of them "6LoWPAN networks." The good news is that 6LoWPAN devices running on different networks can communicate with each other over the Internet, provided that they use the same Internet application protocol. Furthermore, a 6LoWPAN device can communicate with any other IP-based server or device on the Internet, including Wi-Fi and Ethernet devices.

IPv6 was chosen as the only supported IP in 6LoWPAN (excluding IPv4) because it supports a larger addressing space, hence much larger networks, and also because it has built-in support for network auto configuration.

6LoWPAN networks require an Ethernet or Wi-Fi gateway to access the Internet. Similar to Wi-Fi, the gateway is an IP-layer gateway and not an application-layer gateway, which allows 6LoWPAN nodes and applications direct access to the Internet. Since most of the deployed Internet today is still using IPv4, a 6LoWPAN gateway typically includes an IPv6-to-IPv4 conversion protocol.

6LoWPAN is fairly new to the market. Initial deployments use both the 2.4-GHz and the 868-MHz/915-MHz ISM bands. Building on the 802.15.4 advantages – mesh network topology, large network size, reliable communication and low power consumption – and on the benefits of IP communication, 6LoWPAN is well positioned to fuel the exploding market of Internet-connected sensors and other low data throughput and battery-operated applications.

Radio transceivers and proprietary protocols

Many industrial applications today use proprietary protocols running over radio transceivers. The radio transceiver provides the link layer of the network, (or often times just the *physical layer*). The rest of the network protocol is implemented by the OEM. Systems architected in this way leave more flexibility to the system designer at the expense of interoperability and development effort.

These proprietary radio systems primarily use the lower ISM frequency bands 433 MHz, 868 MHz and 915 MHz and therefore are commonly referred to as *Sub-1 GHz* solutions. Sub-1 GHz solutions often transmit high power and can reach over 25 km with a simple point-to-point or star topology. Many utility companies have created proprietary NANs to relay meter readings to a neighborhood collection point. Other popular applications for Sub-1 GHz radios are security systems and industrial control and monitoring.

To connect to the IoT, Sub-1 GHz systems need an application-layer Internet gateway. In many cases this is simply a personal computer running a TCP/IP stack.

Not only wireless

The wireless connectivity market is rapidly growing because of the IoT. Nevertheless, many IoT applications are connected to the Internet with wires. Ethernet connectivity, power line communication (PLC) and industrial communication standards such as Fieldbus are just a few examples, the discussion of which is beyond the scope of this paper.

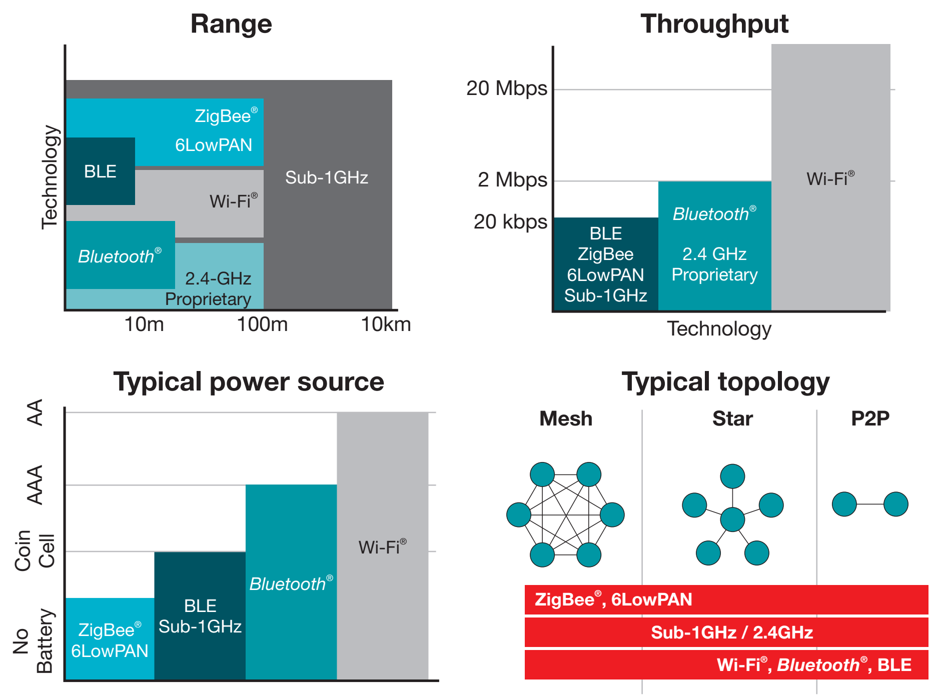

Figure 5. Summary of wireless technology parameters

Conclusion

There are many wireless technologies in the world – each one has benefits, no one is perfect. The question that you need to answer is "which technology is the best one for my application?" Hopefully this discussion has helped you better understand the popular wireless technologies for IoT and their strengths and weaknesses. Figure 5 on the following page maps connectivity technologies to range, throughput, power source and network topology. These data points should be just part of the decision process since as shown, there are many overlapping areas.

Additional considerations that go beyond the scope of this paper are cost, ease of integration and security. We see great improvement on total solution cost and ease of integration coming in many new products, that all use wireless connectivity. Cost and integration efforts should be further considered in the context of specific applications. Security aspects of IoT applications include the supported capabilities of each of the protocols, as well as additional hardware and software considerations, which are better covered in a separate paper.

TI's SimpleLink wireless connectivity portfolio

TI's SimpleLink portfolio of low-power wireless connectivity solutions – wireless MCUs, wireless network processors (WNPs), RF transceivers and range extenders for the broad embedded market – makes it easier to develop and connect anything to the Internet of Things (IoT). Spanning over 14 standards and technologies including Wi-Fi, *Bluetooth*, Bluetooth low energy, ZigBee, Sub-1 GHz, 6LoWPAN and more, SimpleLink products help manufacturers add wireless connectivity to anything, to any design, for anyone. **www.ti.com/simplelink**.

Texas Instruments and the IoT

With the industry's broadest IoT-ready portfolio of wired and wireless connectivity technologies, microcontrollers, processors, sensors and analog signal chain and power solutions, TI offers cloud-ready system solutions designed for IoT accessibility. From high-performance home, industrial and automotive applications to battery-powered wearable and portable electronics or energy-harvested wireless sensor nodes, TI makes developing applications easier with hardware, software, tools and support to get anything connected within the IoT. Learn more at **www.ti.com/IoT**.

IMPORTANT NOTICE

Products		**Applications**	
Audio	www.ti.com/audio	Automotive and Transportation	www.ti.com/automotive
Amplifiers	amplifier.ti.com	Communications and Telecom	www.ti.com/communications
Data Converters	dataconverter.ti.com	Computers and Peripherals	www.ti.com/computers
DLP® Products	www.dlp.com	Consumer Electronics	www.ti.com/consumer-apps
DSP	dsp.ti.com	Energy and Lighting	www.ti.com/energy
Clocks and Timers	www.ti.com/clocks	Industrial	www.ti.com/industrial
Interface	interface.ti.com	Medical	www.ti.com/medical
Logic	logic.ti.com	Security	www.ti.com/security
Power Mgmt	power.ti.com	Space, Avionics and Defense	www.ti.com/space-avionics-defense
Microcontrollers	microcontroller.ti.com	Video and Imaging	www.ti.com/video
RFID	www.ti-rfid.com		
OMAP Applications Processors	www.ti.com/omap	**TI E2E Community**	e2e.ti.com
Wireless Connectivity	www.ti.com/wirelessconnectivity		

Mailing Address: Texas Instruments, Post Office Box 655303, Dallas, Texas 75265