Laird™
CONNECTIVITY

Connectivity Choices for your Medical Device and IoMT Application

Introduction

Medical devices and IoMT (Internet of Medical Things) encompass a wide variety of wireless technologies across an array of healthcare applications. This includes Enterprise Wi-Fi for RF-challenging hospital environments, zero provisioning support for home healthcare applications, Bluetooth considerations for interfacing with the millions of available smartphones and tablets, and connectivity technology for low-cost sensor deployment and wire replacement.

Devices, machines, buildings, and countless other products; virtually anything can be connected to the internet. Not only can anything be connected, the results of this connectivity benefit everyone involved. With an abundance of technologies available at your fingertips such as Bluetooth, Wi-Fi, LoRa, and Cellular, where do you start? How do you even begin to choose the correct connectivity choice for your medical devices and IoMT applications?

As a hospital or medical device company decision-maker, it's important that you not only understand the concept of IoMT, but also market dynamics in the current healthcare environment and the best type of connectivity for your particular situation.

As a hospital or medical device company decision-maker, it's important that you not only understand the concept of IoMT, but also market dynamics in the current healthcare environment and the best type of connectivity for your particular situation.

Market Dynamics in Healthcare

Healthcare providers around the globe know it is imperative that patients' health information is accurate, accessible, and captured in near real-time. The market continues to demand smart devices with interoperability to healthcare systems such as EMR, billing, and asset management to drive accuracy of data and workflow efficiencies. These requirements are driving the integration of wireless connectivity into more and more devices; and the increased adoption of wireless sensors worn by patients and sensors for monitoring environmental conditions. Healthcare providers across acute and clinical care along with the home health environment are increasing their reliance on IoMT technology for workflow efficiencies, improved patient treatment, and decreasing costs.

This IoMT environment includes smart devices that provide and communicate vital data in real time. There is a plethora of ways in which this technology can assist with and advance healthcare worldwide.

For example, let's say a patient is extremely anxious about doctors' appointments. Because of this anxiety, the patient's blood pressure tends to run high when at the doctor's office. With a 'connected' blood pressure monitor, the doctor receives more reliable readings from the patient's normal day-to-day routine which could change the diagnosis and treatment.

Here's another example... a recently-diagnosed diabetic teenager is struggling to manage blood glucose levels and is experiencing frequent and extreme high or low readings. Rather than scheduling a doctor appointment, the doctor can download the patient's glucose readings remotely because the patient is wearing a 'connected' continuous glucose monitor (CGM) system. This allows real time analysis and diagnostics for the patient versus relying on an in-patient visit to react to the changing conditions.

It's important to understand the healthcare environment being targeted before you make crucial decisions about connecting your medical devices to IoMT applications. There are a few market conditions that continue to drive the development and deployments of IoMT.

And so many other ways IoMT can assist with healthcare:

- Patient data automatically entered into the EMR to increase work flow efficiencies and decrease errors.
- Connect medical staff to patients no matter the distance between them.
- Allow doctors to remotely monitor patients with chronic conditions.
- Allow hospital staff to not only keep track of a patient's regimen of medications but also monitor drug and treatment compliance.
- Allows a potential shift to remote/home healthcare as a mainstream healthcare practice.
- Helps non-medical individuals to track many aspects of their own health via fitness trackers, blood pressure machines, and glucose monitors ... just to name a few.
- Automate patient workflow, decreasing errors and inefficiencies.
- Promote asset tracking, environmental monitoring, and predictive maintenance for expensive healthcare equipment.
- Automate tracking and recording environmental and storage conditions to meet compliance requirements.

Connectivity is what brings these four market dynamics – data, cloud analytics, innovation, and mobility – together, successfully connecting people and devices to the healthcare network no matter the medical purpose or the location of the connected device.

Data

The amount of medical knowledge and data is exploding. Consider this... in 1950, it took 50 years for the amount of medical data to double. By the year 2020, that doubling time will be just 73 days. Doctors, nurses, and providers in general are required to utilize electronic medical records (EMR) to monitor and maintain patients' medical data. Data collection from patients is becoming more automated across the continuum of care through wireless technologies.
There is also an increased focus on leveraging connected devices for asset tracking (knowing where medical devices/equipment are located and how they are being used), predictive maintenance (determining the condition of in-service equipment to better know when maintenance is required), and environmental monitoring (ensuring that temperature-sensitive devices and material are maintained at the proper temperature, for example). The number of asset-tracking and inventory management solutions deployed are expected to double in the next couple of years.

Cloud Analytics

With the fast-paced growth of innovation and the ever-increasing amount of data resulting from these connected technologies, more elaborate systems are also required to collect, store, and process this information. Having an abundance of data is useless without efficient means to effectively gather, maintain, and analyze it for diagnosis, treatment, and more efficiencies in healthcare settings. Analytics and the growth of Blockchain technologies will lead to rapid and accurate diagnostics. They will also be instrumental in the growth of data interchange and improved care by connecting electronic medical records to allow seamless sharing of records across healthcare providers.

Innovation

Currently, medical device innovation is accelerating faster than pharmaceutical advancements. The use of personal monitoring devices (such as fitness trackers and continuous glucose monitoring systems) is sky-rocketing and will only continue to grow in the acute care and home healthcare environments. The size of pumps and other patient monitoring devices are shrinking and going wireless allows patient mobility versus being tethered to these devices in a fixed location. The use of robotic surgeries and other wireless technologies in the operating room is increasing. The pace of innovation and the growth of IoMT technologies and applications is putting more and more pressure on healthcare providers to adopt these advancements to improve patient care and satisfaction while reducing costs.

Mobility

Hospitals and healthcare providers in general represent a significant number of employees who are in constant motion. Mobile connectivity for themselves and the instruments they work with is critical to their daily operations. The number of healthcare devices (and therefore healthcare services) are expanding from the secure environment of hospitals and doctor's offices to mobility to support improved patient quality of life. This expansion increases the need for strong, reliable wireless connectivity.

Understanding Connectivity Technologies

There are three main connectivity methods that should be considered for IoMT: Wi-Fi, Bluetooth, and LPWAN. Connectivity can be embedded within the device or added on with external modules and devices once the device has been deployed. Market expectations are that new smart devices have connectivity embedded within the device. Gateways can also be used to collect data on a local level then manage the connection to a cloud server for the transmission of this data. In this way, not every device or sensor must be connected to a cloud or network server. The following sections describe these wireless technologies and provide important aspects of and considerations for each in regard to the IoMT.

Enterprise Wi-Fi

Wi-Fi, in general, is a technology that uses radio waves to transmit information at specific frequencies. It enables high-speed and secure communication between a variety of devices, without wires, over both short and long distances within the Enterprise. In this white paper, we discuss Enterprise-grade Wi-Fi (versus consumer-grade) because it provides a higher-level of service when it comes to performance, security, standards/compliance, and life-cycle management – factors that are important for connectivity in a healthcare environment. For devices and applications to be deployed within acute care (hospitals) or ambulatory care (clinical), Enterprise Wi-Fi is the primary wireless connectivity for local area networks. Another critical performance criterion in these environments is fast, secure roaming. Dropping network connectivity while a device is moving within these environments could create critical loss of data and delays to administrating healthcare to a patient. Your Wi-Fi module must support optimized scanning algorithms to maintain network persistence for the mobile device within these noisy RF environments.

Enterprise Wi-Fi supports two communication bands. It is important to consider if the devices will be transmitting in the 2.4 GHz and 5 GHz bands. Since the 2.4 GHz band can quickly be congested with commodity devices and guest access, most hospitals have dedicated the 5 GHz band for critical devices and applications. There is increased bandwidth and performance available within the 5 GHz bands versus 2.4 GHz. Let's take a closer look at the latest Wi-Fi standards to further explain this.

802.11ac – The Standard of Choice for Enterprise Wi-Fi

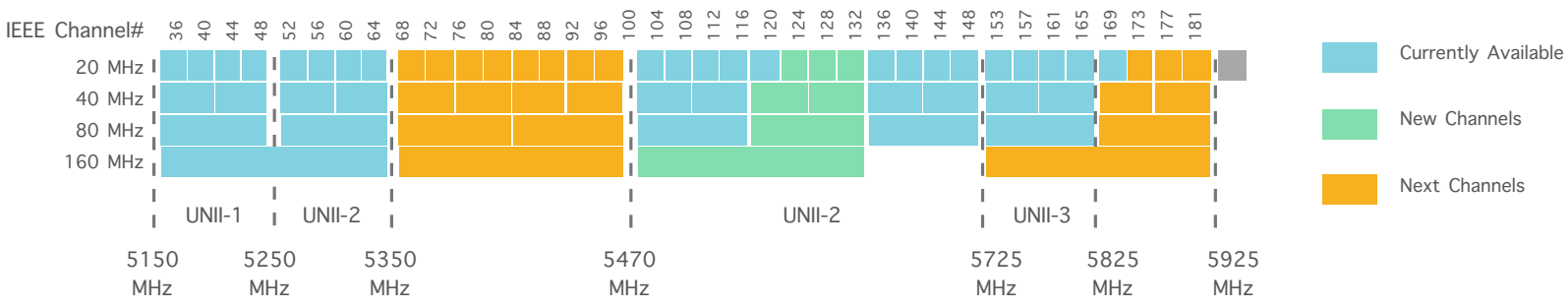
Although there are several Wi-Fi standards currently on the market, 802.11ac Wave 2 (or Wi-Fi 5) is the standard to pursue if you're actively introducing a device with embedded Wi-Fi. Wave 2 is not an official IEEE standard, but products classified as Wave 2 perform better and have additional features over 802.11ac Wave 1 (for example, MU-MIMO). 802.11ac includes significant enhancements to the Wi-Fi standard such as 80 MHz/160 MHz channels and MU-MIMO (multiple user – multiple input, multiple output)

802.11ac operates in the 5 GHz signal range which decreases interference common to 2.4 GHz and allows for the wider channel implementation. At the same time, 802.11ac devices are backward-compatible with the previous 802.11a and 802.11n 5 GHz devices. Also, most 802.11ac dual-band access points support 802.11b/g/n in the 2.4 GHz band.

80 MHz and 160 MHz Channels

802.11ac brings support for larger channel widths than previously. It's this increase in channel widths (80 MHz and 160 MHz) that primarily drives the enhanced performance and bandwidth. Previously, the general method to denote 5 GHz channels was to use the 20 MHz center channel frequencies for both 20 MHz and 40 MHz wide channels. With 802.11ac, we now reference the center frequency for the entire 20, 40, 80, or 160 MHz-wide channels. This gives us the following channels numbers for each specific channel width: *(See Figure A)*

Figure A **FCC: 5 GHz Channel Plan - Snapshot as of January 2015**



With wider channels comes higher data rates and bandwidth. But careful channel planning must take place because these wider channels come at a cost… there are fewer channels to plan around. It's possible that these wider channel widths may not be realistic in an Enterprise Wi-Fi environment where multiple access points are deployed and where co-channel interference must be avoided. As you can see in *Figure A* there is only one 160 MHz channel available in the U.S. and two in the EU (if DFS is used). With the 80 MHz-wide channels, four or five are available, depending on where you are located. To reap the benefits of improved performance from these wider channels, thorough channel planning must take place to avoid co-channel interference.

MU-MIMO

MU-MIMO (Multiple User- Multiple Input, Multiple Output) allows increased support for environments where many users are trying to access the same wireless network at the same time. With the earlier single-user MIMO, access points could only send data to one device at a time which caused some congestion. With MU-MIMO, access points can send downstream traffic to four clients simultaneously *(See Figure B).*

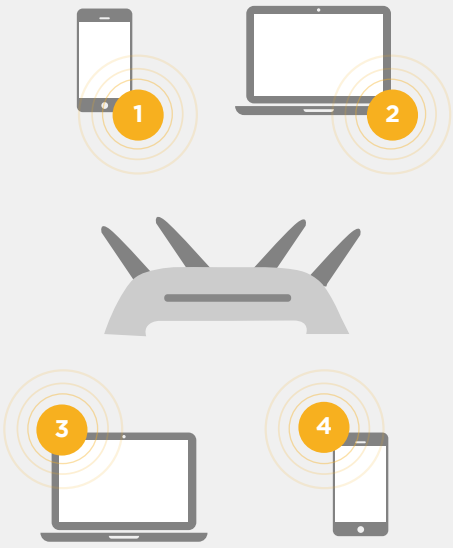
The advantages of MU-MIMO include less on-air time for multiple clients, significantly improving overall network efficiency, and improved transference of large files and streaming video. To actively participate with MU-MIMO, both the access point and clients must support it. That being said, even non-MIMO devices could experience some improved performance because, if MU-MIMO devices on the same network are served more quickly, there is likely more time for SU-MIMO and other devices to communicate.

802.11ax

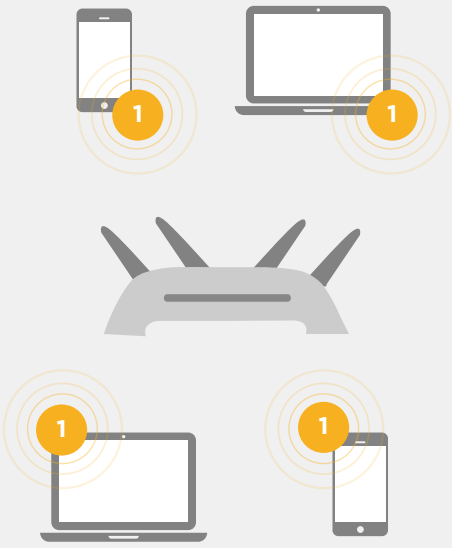
802.11ac is an important development leading to the next Wi-Fi standard, 802.11ax. 802.11ax, with a potential release date of late 2019, is the next step in the evolution of Wi-Fi. This upcoming standard will, similar to .11ac, focus on network efficiency rather than peak speed. 802.11ax is all about working smarter and more efficiently to enhance Wi-Fi performance. This latest specification will provide higher capacity and better coverage and it will reduce congestion for a better user experience.

Some features and benefits of 802.11ax will include:

- 8x8 MU-MIMO – 802.11ax extends the benefits of 802.11ac, which supports up to four transmissions at a time (downlink only). 802.11ax will support up to eight transmissions in both downlink and uplink.
- OFDMA – Access points can send multiple user packets to multiple users simultaneously. In previous specifications, OFDM could only send one packet per client. Upgrading to OFDMA allows a single packet to serve multiple clients. Each channel is broken into hundreds of smaller sub-channels. Up to 30 clients can share each channel instead of having to take turns broadcasting and listening.
- New modulation – 802.11ax uses 1024-QAM which allows devices to send denser packets. Hence, more data can be transmitted per packet.
- Resource scheduling – This new feature is a more efficient way to handle packets. It significantly increases a device's sleep time, improving battery life. Think of it like a traffic light at an intersection, allowing cars to flow without congestion and in an orderly manner.
- Backwards compatibility – 802.11ax is backwards compatible with 802.11a/b/g/n/ac.
- Increased spectrum use – 802.11ax provides better coverage, operating in both the 2.4 GHz and 5 GHz frequency bands, while 802.11ac only works in 5 GHz.



Single-User MIMO



Multi-User MIMO
(Up to 4 simultaneous)

Figure B

Enterprise Wi-Fi Security

Obviously, when dealing with healthcare and the IoMT, secure communication is vital. Wi-Fi data level security consists of two parts. Encryption, which is scrambling of data so it cannot be intercepted (key); and authentication (802.1x), which verifies that the client receiving the data is the client who should be receiving the data (certificate).

Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), and Wi-Fi Protected Access II (WPA2) are the primary security algorithms you'll see when setting up a wireless network. WEP is the oldest and has proven to be vulnerable as more and more security flaws have been discovered. WPA improved security but is now also considered vulnerable to intrusion. WPA2, while not perfect, is currently the most secure choice. Temporal Key Integrity Protocol (TKIP) and Advanced Encryption Standard (AES) are the two different types of encryption you'll see used on networks secured with WPA2. AES is a more secure encryption protocol introduced with WPA2. AES isn't some creaky standard developed specifically for Wi-Fi networks, either. It's a serious worldwide encryption standard that's even been adopted by the US government.

Extensible Authentication Protocol (EAP) is an authentication framework, not a specific authentication mechanism. It provides some common functions and negotiation of authentication methods called EAP methods. There are currently about 40 different methods defined. Commonly used modern methods capable of operating in wireless networks include EAP-TLS, EAP-SIM, EAP-AKA, **LEAP**, and EAP-TTLS.

WPA2-PSK (Pre-Shared Key)

- Also known as WPA2-Personal
- Involves a single password to access the wireless network
- Should only be used:
  - If the network has only a few trusted devices (i.e., home or small office)
  - To restrict casual users from joining an open network (i.e., guest network or coffee shop)
  - For devices that are not compatible with 802.X (i.e., game console)

WPA2-Enterprise

- Has an authentication process based on the 802.1X standard
- Each client receives a unique encryption key after log-in that are not saved on the device (AES)
- Includes EAP types
- Because each device is authenticated prior to connection, a personal tunnel is created between the device and the network

Figure C

WPA2-PSK versus WPA2-Enterprise

See *Figure C* for a brief comparison of the less secure WPA2-PSK to WPA2-Enterprise.

The security scheme is defined by the end user's IT organization. Nearly all enterprise networks within the medical market expect support for the WPA-2 Enterprise within the clients joining the network. The EAP supplicant of choice is also driven by the end user and the RADIUS authentication selected. The challenge for the medical device manufacturers is in implementing a Wi-Fi communications module that supports WPA2 – AES encryption and provides updated EAP supplicant drivers.

WPA3

In January of 2018, the Wi-Fi Alliance announced Wi-Fi-certified WPA3, the next generation of Wi-Fi security for both personal and enterprise networks. This newest version adds four features that were not present in WPA2. To market devices as *Wi-Fi Certified™ WPA3™*, manufacturers must fully implement these four new features:

- **Individualized data encryption** – When you connect to an open Wi-Fi network (such as in a coffee shop or airport), the traffic between your device and the access points is encrypted even though no password was entered during the connection process.
- **New handshake** – When a device connects to an access point, it performs a handshake to ensure you've used the correct password to connect and negotiates the applicable encryption that will secure the connection. This new handshake delivers stronger protections even if the user assigns a password that doesn't meet typical strength recommendations.
- **Simpler connection process** – Because many devices today do not have displays, WPA3 includes a feature that simplifies the security configuration process.
- **192-bit security suite** – Intended for government, defense, and industrial applications, this suite aligns with the Commercial National Security Algorithm (CNSA) Suite from the Committee on National Security Systems.

A number of the Wi-Fi solutions available today can support a software migration to WPA 3. The exception is in the support for the 192-bit encryption. This may require a hardware upgrade for some Wi-Fi modules and chipsets.

Securing of the Networked Medical Device

Along with network encryption and authentication, there are other security components to consider in keeping the device itself safe from threats propagating through the network.

Hardware Root of Trust

Because of the potential vulnerability of IoMT devices, there's a strong need for a robust, secure system surrounding them. Roots of trust (RoT), in general, refer to highly-reliable hardware, firmware, and software components that perform critical security functions. In order to be trusted, these components must be secure themselves. Embedding an RoT within the hardware ensures only signed and trusted software images are loaded on the device. This is the first defense from a malicious hacker loading suspect software on a device.

Firewall

Basically, a firewall is a barrier designed to prevent hackers from accessing secured, sensitive, vital information. By placing a firewall function within your device, it increases the trust level of network connections and potential attacks can be prevented.

OTA Updates

An OTA (over-the-air) update is a method for remotely performing software or firmware updates to connected devices. Because many IoMT systems are large and spread out, performing manual security updates to individual devices is ineffective and unrealistic. It simply doesn't scale well to widely-dispersed or high numbers of devices. A strong OTA update mechanism can facilitate keeping devices updated with the latest security fixes and is valuable in regard to Wi-Fi security.

Bluetooth for Healthcare

Initially, Bluetooth was shunned across healthcare organizations due to concerns of yet another RF technology in a congested wireless space. But as the security aspect of Bluetooth is enhanced along with increased signal range, there are more and more applications leveraging Bluetooth in the medical space. The adoption of Bluetooth technology has grown significantly since its integration with smart phones and tablets. Because Bluetooth is a frequency hopping technology, it can avoid congested spectrum channels being used by other wireless technologies such as Wi-Fi access points.

Numerous personal monitoring devices (Fitbit, glucose monitoring, neuromodulation) leverage Bluetooth for device connectivity and provisioning. We are seeing more and more of these types of monitoring devices introduced into the critical care environment. Bluetooth is also being used effectively as a wire replacement within operating rooms, ICU's, and other locations with a high number of devices in use. Finally, as a customer service benefit, Bluetooth can be utilized for wayfinding applications to assist patients and visitors in navigating across hospitals and campuses.

Understanding Bluetooth Technology

Bluetooth is a wireless technology that allows mobile Bluetooth devices to exchange data over short distances. The original Classic Bluetooth was designed to continually stream data over short distances. To put it simply, you can exchange a lot of data with Bluetooth as long as it's exchanged at close range.

The more recently developed Bluetooth Low Energy, also known as BLE or Bluetooth LE and introduced in Bluetooth 4.0, is a low-power yet robust technology intended for situations where battery life is more important than high data transfer speeds. Although it far exceeds Classic Bluetooth on many fronts, the two are similar in a variety of ways:

- They are both WPAN standards that operate in the 2.4 GHz frequency band
- They both operate in a basic master-slave model where both Bluetooth devices must be paired before they can transmit data
- Both use the same pairing, authentication, and encryption technologies.

The most significant difference between the two technologies is that BLE uses far less power consumption than Classic Bluetooth. BLE is perfect for applications that sporadically send small amounts of data. In the healthcare world, this would be applicable to a variety of medical devices such as blood glucose monitors and pumps, asthma inhalers, and implantables (such as pacemakers and ICDs). The lower power properties of BLE make it effective for deploying environmental sensors and room monitoring to meet compliance requirements. BLE is an effective connectivity choice for distributed gateways that collect this data and pipeline it to cloud and server applications for analysis.

The following chart summarizes the differences between Classic Bluetooth and the much-preferred Bluetooth Low Energy.

	Optimized For...	Data Rate (Max)	Frequency Band	Range	Security	Typical Use Examples
Classic Bluetooth (BR/EDR)	Continuous data-streaming	Up to 3 Mbps	2.4 GHz	Up to 30 meters	Secure Simple Pairing (SSP)	• Wireless headsets • Wireless Printers • File transfer b/t Bluetooth devices
Bluetooth (LE)	Short burst data transmission	1 Mbps	2.4 GHz	Up to 150 meters	LE Secure Connections	• Healthcare monitoring/reporting devices/sensors • Fitness tracking devices • Building automation (i.e., lights)

Bluetooth 4.0 entered the technology market in 2011. Since that time, additional versions, including 4.2, 5.0, and 5.1 have been released. The following summarizes some of the enhancements each of these technology versions provide.

Bluetooth 4.2	• Dramatically increased speed – 2.6x faster than older versions • Added privacy upgrades • Allowed chips to use Bluetooth over IPv6 (Internet Protocol version 6) for direct internet access
Bluetooth 5.0	• Provides improved speed and range – 2x the speed, 4x the range, 8x broadcasting message capacity • Devices can synchronize their scanning (for connection) with other Bluetooth devices • Allows audio devices to communicate which reduces power use and increases battery life • Provides dual audio capabilities – Audio can play simultaneously on two connected Bluetooth devices. It can also stream two different audio sources to two separate Bluetooth devices at the same time
Bluetooth 5.1	• Pinpoint location accuracy – It combines distance and direction to pinpoint the physical location of a connected device to the centimeter. If one of the devices has an array of multiple antennas, AOA (angle of arrival) and AOD (angle of departure) make distance measurement and direction more precise • Enables a quicker connection and less energy by performing a more aggressive caching of service discovery information. This allows the device to skip the service discovery stage if nothing has changed • Randomized indexing of advertised channels – It selects channels at random (rather than cycle through channels in a strict order as with Bluetooth 5.0). This decreases the chance that two Bluetooth devices will interfere with each other which is helpful in this every-expanding Bluetooth device environment

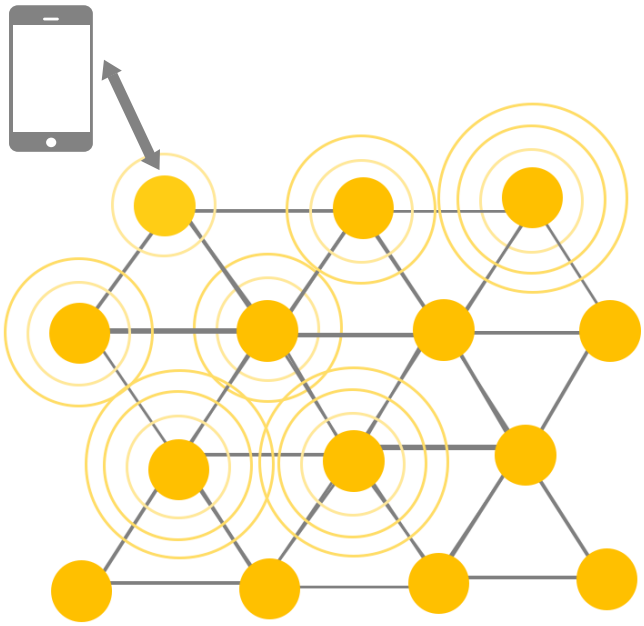
Bluetooth Mesh Network

As technology develops and as people become more reliant on wireless networks, the demands placed on these networks also continues to grow. Adopted in 2017, Bluetooth mesh is a networking Bluetooth technology that replaces the one-to-one Bluetooth exchange with a many-to-many (m:m) relationship between Bluetooth devices.

Mesh networks, in general, can effectively meet communication requirements over large areas while monitoring and managing many devices. Bluetooth mesh networking, more specifically, accomplishes these things while also maintaining compatibility with current PCs/tablets/smartphones and, because it depends on Bluetooth LE technology, does so with low-energy efficiency.

This type of mesh capability can enhance the development of large device networks. For example, one IoMT use case for a Bluetooth mesh network is a hospital that needs to track patients, equipment, and even hospital staff from any laptop, PC, or other device located on the hospital premises. Using non-mesh technology, it may not be possible to connect the entire hospital effectively or consistently due to the vast number of obstacles (walls, electronic equipment, people, etc.). Bluetooth mesh networking allows some devices to function as relays, retransmitting messages they receive from other devices. In this manner, devices can communicate with other devices that are not within their radio range.

This mesh network technology is effective because it uses a technique called *managed flooding*. A mesh node transmits (or "floods") data omnidirectionally to all nodes within its direct range. Those nodes each then do the same – flood all nodes within their direct range. This pattern continues until the published data reaches all nodes within the network. Only applicable nodes (ones that are addressed or subscribed) act on this transmitted data. The rest simply relay the messages.



With no single-purpose centralized routers, multiple paths available for a published message, and the ability to self-heal, Bluetooth mesh networking is an extremely reliable system. All of this is achieved while maintaining its low-power feature. Bluetooth mesh enables low-power devices to work with other nodes ("friends") which are not power-constrained. These non-power-constrained nodes do the hard, high-energy work: they store messages intended for low-power nodes and only deliver the messages when the low-power nodes request them.

Low-Power Wide-Area Network

The growth of IoMT implies more and more devices connecting to a central application server which is usually based in the cloud. Enterprise Wi-Fi and Bluetooth are effective local area network technologies that can leverage the Enterprise network to connect back to the cloud. But in some instances within the Enterprise space, it is not practical or there are security concerns with devices connecting directly to the Enterprise network. In these cases, devices and sensors may leverage LPWAN technology to bypass the local network and connect to a carrier network to connect back to the cloud. With some applications, using a LPWAN protocol like LoRa operating in the 900 MHz range allows greater range and better propagation through various building materials than Wi-Fi or BLE. Therefore, LoRa can be a cost-effective gateway technology that gathers data from distributed sensors and then communicates that data back to the cloud server from one fixed point. This allows low-cost sensor deployment and IoMT across a healthcare provider's campus without requiring the need for the sensors to connect to the LAN.

The emerging LPWAN technologies like LTE CAT-M1 and NB-IoT are becoming very effective in connecting remote sensor devices including medical devices being utilized in the home. These protocols are different from standard cellular services because they are meant to support low data rates at much lower cost than support for standard voice and data cellular service. This is empowering more and more patient care to be administered within the home while the provider stays connected and receives real time updates from the point of care. An important consideration for deployment in the home for these technologies is zero provisioning from the patients. Basically, they turn on the devices and automatically begin connecting. No extra steps by the patient should be needed to establish the IoMT connection.

Rather than being a single technology, LPWAN (low-power wide-area network) is a broad term to describe a group of protocols that operate using low powered devices to communicate small amounts of data over long-distances. There are several technologies competing within the LPWA realm including LoRa and LoRaWAN and cellular protocols such as LTE CAT-M1 and NB-IoT.

The following table compares basic characteristics and features of LoRaWAN, LTE CAT-M1, and NB-IoT. The following sections provide more in-depth information on each of these technologies.

	LoRaWAN	LTE CAT-M1	NB-IoT
Bandwidth (uplink)	125 kHz	Up to 3 Mbps	2.4 GHz
500 kHz	1.4 MHz	180 kHz	2.4 GHz
Data Rate	50 kbps	384 kbps	62.5 kbps
Mobility	Yes	Yes	No

LoRaWAN

LoRaWAN (Long Range Wide-Area Network) is a LPWAN, media access control (MAC) layer protocol built on top of LoRa or FSK modulation. LoRaWAN enables low-powered, battery-operated devices to wirelessly communicate over long-distances (2-3 km in urban settings and 6-10 km in rural settings). LoRaWAN can span these extremely long distances by decreasing its data rates to very low levels (0.3-22 kbps).

LoRaWAN operates in the unlicensed ISM band; the actual frequency band varies by region. For example, in the U.S. it operates in the 902-928 MHz frequency band while in Europe, it operates in the 863-870 MHz frequency band.

Of the various LPWAN protocols, LoRaWAN is unique in that it can be deployed on either a public network or its own private network. The fact that it can be deployed on its own private LoRaWAN network is advantageous for several reasons including:

- **Location** – The area/environment in which you plan to deploy your network may not have a public LoRaWAN network in place.
- **Remote or inaccessible sensor locations** – If you need to deploy sensors in extremely remote areas or in difficult to access areas (such as deep basements), a public network may not be accessible.
- **Large deployment area** – If your plan is to deploy a very large number of LoRa sensors, having your own LoRaWAN network can decrease the overall cost.
- **Security** – Healthcare environment especially are concerned about secure data communications. Avoiding a public LoRaWAN operator and using your own private network heightens the amount of security.

With LoRaWAN, the applications are endless: cold chain monitoring, environmental monitoring, facility security monitoring, monitoring in remote areas, and asset location, just to name a few.

LoRaWAN Summary:

- **Long range** – Up to 10+ km
- **Low power** – Can last years on a battery
- **Secure** – 128-bit end-to-end encryption
- **Low bandwidth**
- **Inexpensive**
- **For situations where real-time data is not required** (since you can only send periodic packets)

LTE Cat-M1 versus NB-IoT – A Look at Cellular IoMT Technologies

Cellular IoMT technologies allow you to connect devices, such as sensors, to the internet via the same mobile networks used by smartphones. Your smartphone uses larger amounts of bandwidth for voice and data. IoT applications usually require a lot less. Cat 1 and Cat M1 modems allow a lot more IoT traffic to fit in the same LTE network bandwidth. **LTE Cat 1 uses less network bandwidth** than traditional LTE modems, and Cat M1 uses significantly less. Cat 1 supports higher bandwidth (10 Mbps) at a higher power consumption than Cat M1. With a focus on battery powered devices, the two cellular IoMT technologies we discuss here are LTE Cat-M1 and NB-IoT.

LTE Cat-M1, or Long-Term Evolution (4G) Cat-M1, is a low-power, wide-area protocol that allows IoMT devices to connect directly to a 4G network without a gateway. With LTE CAT-M1, you have low bandwidth at a lower cost, long battery life, and with lower complexity. LTE Cat-M1 is designed for devices that are moving or that require near real-time speeds.

NB-IoT (Narrowband IoT) is a cellular-grade wireless technology that is intended for extremely-low data rate devices that must connect to a mobile network. NB-IoT sends and receives small amounts of data. Like LoRaWAN, it is message-based but it has a faster modulation rate and can handle much more data and has better in-building penetration. With NB-IoT, you have very low bandwidth with very low power and no roaming capabilities. NB-IoT is perfect for stationary devices and device that only send updates every couple of minutes.

LTE Cat-M1 and NB-IoT Summary Comparison

LTE Cat-M1

- Low bandwidth
- Lower cost
- Lower complexity
- Supports both fixed and mobile applications
- Service providers – AT&T and Verizon

LTE Cat-M1

- Very low bandwidth
- Very low power
- Better in-building penetration
- No roaming capabilities*
- More appropriate for simpler, stationary applications
- Service provider – T-Mobile, AT&T, Verizon (U.S.); Vodafone (Europe and China)

Wireless Gateways for Medical Applications

So far, we have reviewed a number of connectivity technologies with a focus on connecting individual devices. Within the IoMT, we are also seeing growth in adoption of gateway technology. A gateways is a physical device or software program that serves as a connection point between the cloud server/application and devices and/or sensors. All data moving to the cloud, or vice versa, goes through the gateway, which can be either a dedicated hardware appliance or software program. Smart devices along with environmental, pressure, positioning **sensors** can generate thousands of data points per second. A gateway provides a device to collect and pre-process or package the data locally before sending it on to the cloud. In this way, the end user can minimize the volume of data needed to be sent and can manage a secure connection through the Internet and into the target cloud provider. Because the gateway manages information moving in both directions, it can protect data from leaks and IoT devices from being compromised by malicious outside attacks.

A gateways is a physical device or software program that serves as a connection point between the cloud server/application and devices and/or sensors. All data moving to the cloud, or vice versa, goes through the gateway, which can be either a dedicated hardware appliance or software program.

A gateway can support multiple connection technologies such as Wi-Fi, BLE, LORA, Ethernet, and serial port connections. These technologies can be used as ingress to the gateway in collecting data from the local devices.

Most deployments use the Ethernet or a Wi-Fi connection to the local area network as the doorway to manage the cloud connection. If using the local area network is not feasible, then a cell modem can be integrated into the gateway to leverage cellular connectivity to connect back to the cloud. The LTE CAT-M1 and/or NB-IoT service connections can be a cost-effective egress technology for lower data rate applications. Maintaining a secure connection across all the technologies is critical, specifically for a gateway in use for medical application or data gathering.

There are several popular cloud service providers available in the market today including Amazon, Microsoft Azure, and Google. These providers offer secure connections back to the cloud and enhanced security to protect the data while it is in the cloud. If any patient data is transferred or stored, the cloud service must be HIPAA-compliant to meet the privacy security compliance requirements. The previously-mentioned providers do offer HIPAA-compliant cloud hosting as an additional feature.

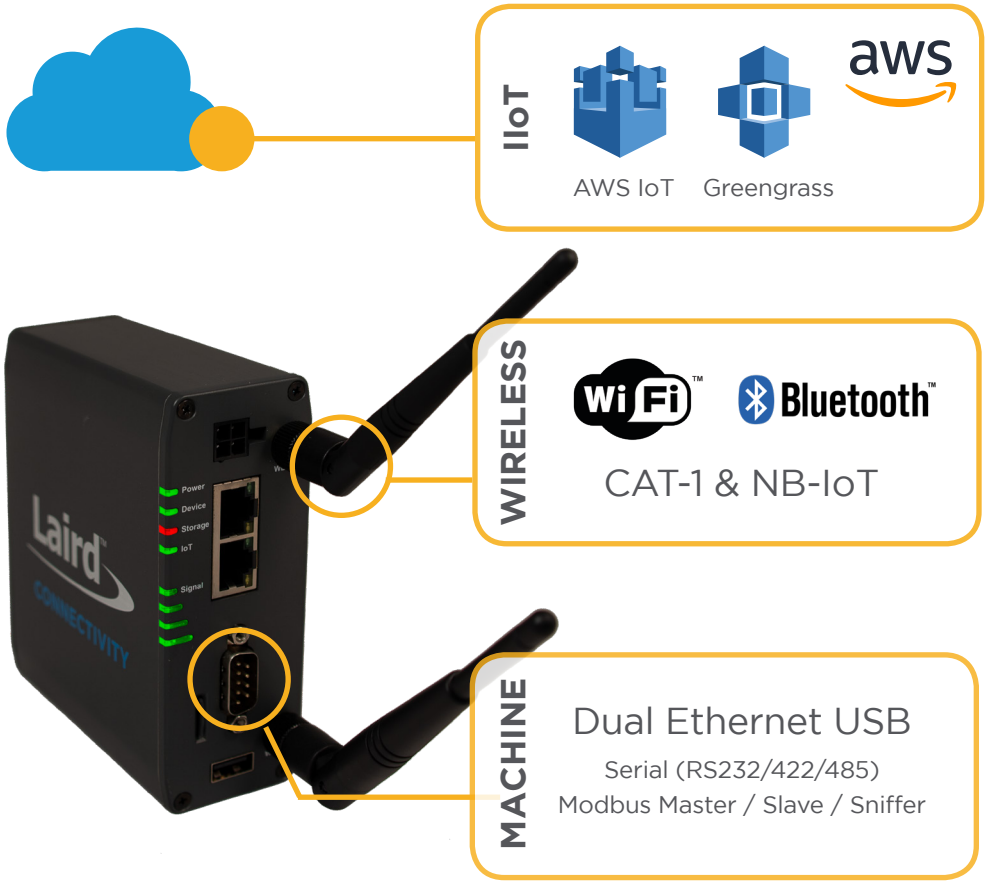
They also offer software connectors such as Amazon's Greengrass or Microsoft Azure IoT Edge that can be run on the gateway to manage secure connections back to the target cloud service. With these connectors, you can use familiar languages and programming models to create and test your device software in the cloud and then deploy it to your devices. The cloud connector can be programmed to filter device data and only transmit necessary information back to the cloud. You can also connect to third-party applications, on-premises software, and other services with cloud connectors. Several gateways can come bundled with the cloud connectors already active. They also can support programing languages such as Python to enable fast integration of your software application.

Leveraging cloud connectors and high-level programming languages enables rapid prototyping of applications and collecting and transmitting target data into the cloud. Some applications can be up and running and transferring sensor data into the cloud within minutes.

Gateways accomplish several tasks:

- They collect many types of vital information – sensor data, device status and location, serial readouts, and machine status… just to name a few.
- They help various sensor protocols and technologies (such as Wi-Fi, Bluetooth, cellular, serial ports, and Ethernet) communicate to one another.
- Process the collected data before sending it on to the cloud.

Not only does a gateway provide rugged connectivity with a variety of interfaces, it accomplishes this while maintaining high levels of security.



Conclusion

Choosing the correct connectivity choice for your medical device/medical environment and IoMT applications is a complicated, yet vital, decision to make. The more you understand the concept of IoMT, connectivity technologies, market trends, and your own healthcare environment and requirements, the better prepared you will be to make these decisions.

Learn more by visiting
lairdconnect.com/market/connected-devices-healthcare

About Laird Connectivity:

Laird Connectivity simplifies the enablement of wireless technologies with market-leading wireless modules and antennas, integrated sensor and gateway platforms, and customer-specific wireless solutions. Our best-in-class support and comprehensive engineering services help reduce risk and improve time-to-market. When you need unmatched wireless performance to connect electronics with security and confidence, Laird Connectivity delivers — no matter what.

Learn more at lairdconnect.com

Laird™
CONNECTIVITY

# # #