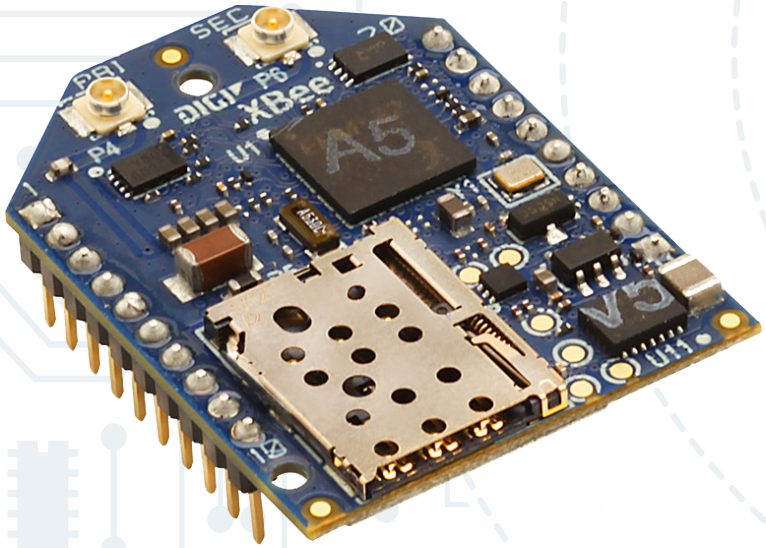
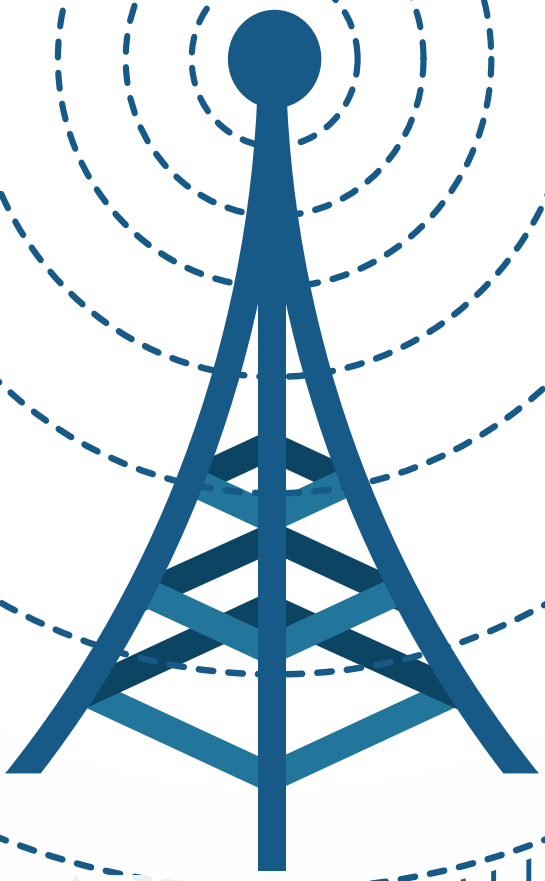
DIGI®

MOUSER ELECTRONICS®





Digi XBee® Wireless Modules

Contents

Foreword

Digi XBee®: One Socket Simplicity

With over 10 million modules deployed, Digi XBee® is the world's choice for embedded wireless connectivity. Whether it's Zigbee, Thread, Wi-Fi, cellular, or new and emerging LPWA standards, Digi XBee has you covered. In the fall of 2017, we are introducing Digi XBee Cellular for LTE-M and NB-IoT.

What makes Digi XBee such a great fit for wirelessly connecting a wide range of applications? Digi XBee provides secure, reliable connectivity in a simple, consistent, and compact footprint. Digi XBee's common footprint enables the industry's fastest path to embedded wireless connectivity through end-device, pre-certified simplicity. Furthermore, the Digi XBee Ecosystem™ offers a full range of hardware, software, and resources to quickly bring connectivity to devices.

Digi XBee offers the largest selection of global protocols and frequencies, with one-socket-simplicity, to connect IoT networks around the world. Simple software tools enable the convenience to connect to locally or remotely configured devices. The Digi XBee form factor can future-proof designs with ongoing connectivity to new technologies as they emerge, giving product designers flexibility to swap out radios for different regions of the globe.

Digi XBee allows customers to accelerate time to market and minimize costs with the right combination of easy-to-use hardware, software, and a library of helpful resources. Digi XBee modules also share a common API and AT command set allowing customers to substitute one module for another, or event switch protocols with minimal development time and risk. And if that isn't enough, you can embed your own custom logic using the popular MicroPython environment.

Digi XCTU: Software to Easily Configure and Manage Simple and Sophisticated Solutions

Sidestep the frustrations, roadblocks, and pitfalls of RF projects thanks to Digi XCTU, the free, multiplatform, intuitive application that lets you easily set up, configure, test, and deploy Digi XBee modules.

Digi XCTU includes all of the software tools you need to get up and running with Digi XBee—fast. The unique graphical network view visually presents your Digi XBee network along with the signal strength of each connection. And the intuitive API frame builder helps you build and interpret API frames for Digi XBees being used in API mode. Digi XCTU is the developer's toolkit that makes Digi XBee development easier than ever.

Digi XBee® Ecosystem™: Tap Into Worldwide Experience And Expert Resources

The Digi XBee® Ecosystem™ offers a complete selection of hardware and software tools with unmatched resources and support. From a full library of technical documentation and articles to the largest collection of Digi XBee projects on the Web, you can draw inspiration from a broad range of useful examples, guides, videos, and tutorials for your next idea.

Whether you're just learning about wireless communication and Digi XBee or you're an experienced developer, you can consult the Digi Knowledge Base for M2M and IoT information and tips—and the Digi Forum where you can ask questions and receive answers from other members in the community. From prototyping to end-to-end connectivity solutions, count on Digi XBee Ecosystem examples, guides, tips, libraries, and software tools for guidance.

Digi is proud to partner with Mouser to bring all of the advantages of the Digi XBee Ecosystem, including the hardware, software and resources, to quickly bring secure connectivity to your ideas. See why Digi XBee is world's choice for wireless connectivity.

Warm regards,

Joel Young, CTO

Digi International, Inc.

Who is Digi International?

ALWAYS CONNECTED

Digi International, Inc. (Digi) was formed in 1985—long before anyone coined the term the Internet of Things. We've always focused on connecting things, starting with intelligent multiport serial boards for PCs.

As wireless data technologies evolved, we invented right along with it, expanding our product lines with RF modules, gateways, and cellular routers to build critical communications infrastructures, plus embedded wireless system on module (SoM) and single-board computer (SBC) offerings for makers of next generation connected products.

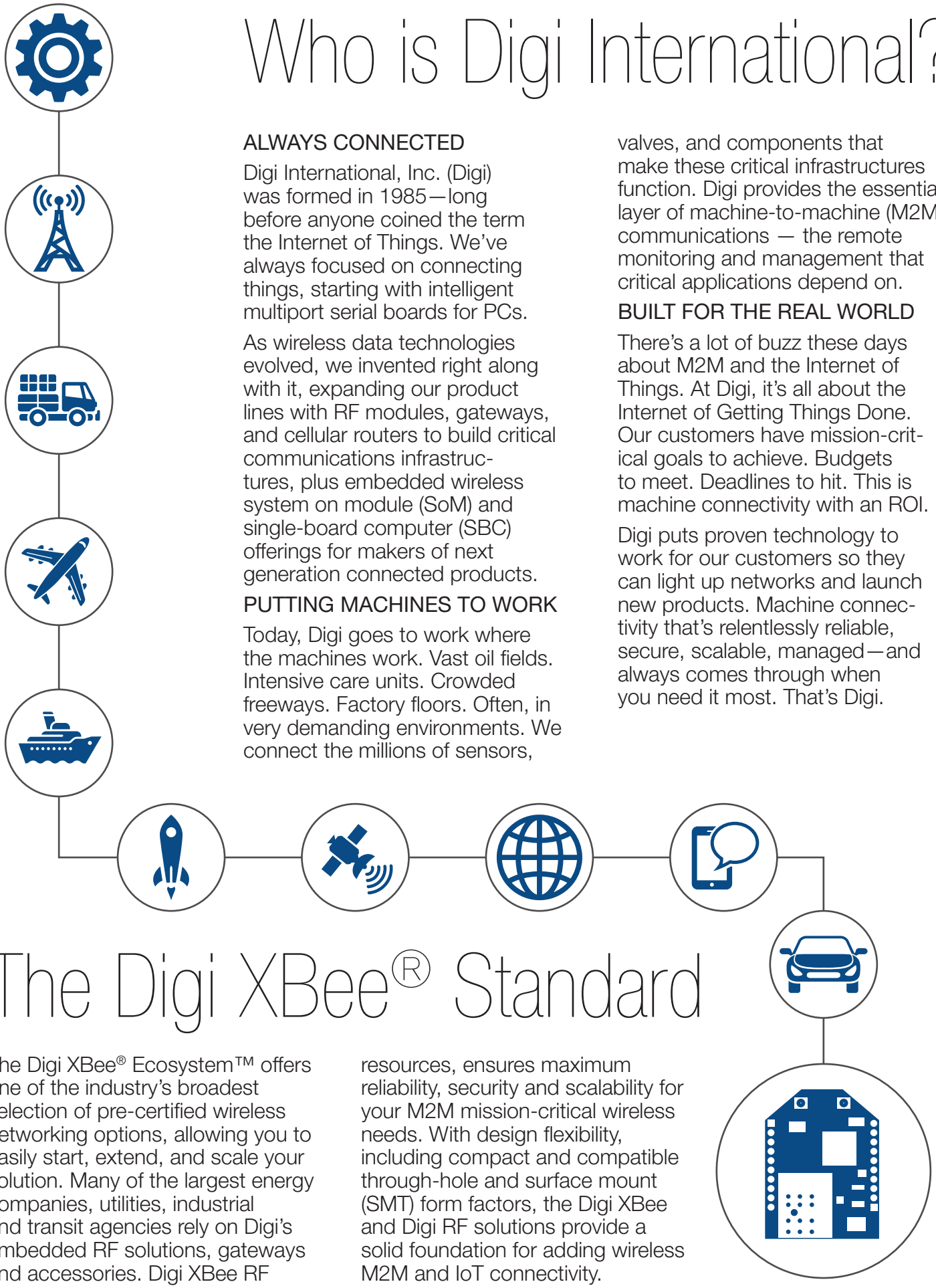
PUTTING MACHINES TO WORK

Today, Digi goes to work where the machines work. Vast oil fields. Intensive care units. Crowded freeways. Factory floors. Often, in very demanding environments. We connect the millions of sensors, valves, and components that make these critical infrastructures function. Digi provides the essential layer of machine-to-machine (M2M) communications — the remote monitoring and management that critical applications depend on.

BUILT FOR THE REAL WORLD

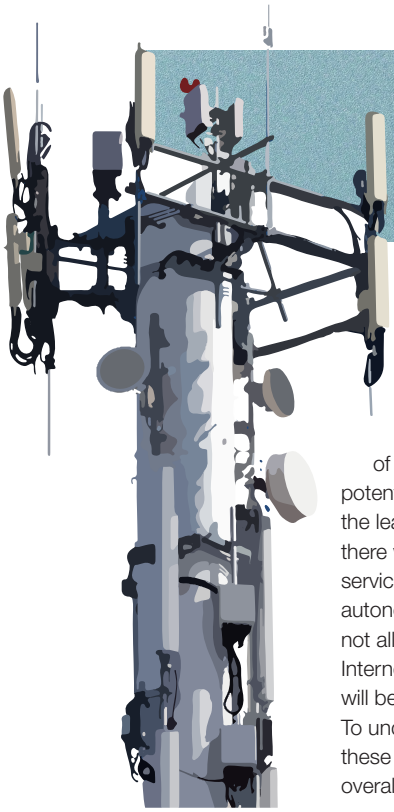
There's a lot of buzz these days about M2M and the Internet of Things. At Digi, it's all about the Internet of Getting Things Done. Our customers have mission-critical goals to achieve. Budgets to meet. Deadlines to hit. This is machine connectivity with an ROI.

Digi puts proven technology to work for our customers so they can light up networks and launch new products. Machine connectivity that's relentlessly reliable, secure, scalable, managed—and always comes through when you need it most. That's Digi.



The Digi XBee® Standard

The Digi XBee® Ecosystem™ offers one of the industry's broadest selection of pre-certified wireless networking options, allowing you to easily start, extend, and scale your solution. Many of the largest energy companies, utilities, industrial and transit agencies rely on Digi's embedded RF solutions, gateways and accessories. Digi XBee RF hardware, software and expert resources, ensures maximum reliability, security and scalability for your M2M mission-critical wireless needs. With design flexibility, including compact and compatible through-hole and surface mount (SMT) form factors, the Digi XBee and Digi RF solutions provide a solid foundation for adding wireless M2M and IoT connectivity.



The Cellular Industry Crafts Its Plan for IoT Connectivity

By Barry Manz

The cellular industry is taking steps to ensure that wireless carriers, rather than Low-Power Wide Area Network (LPWAN) providers, will secure the bulk of the revenue from long-range Internet of Things (IoT) connectivity solutions. The potential rewards are enormous, as even the least optimistic analysts project that there will be at least 20 billion IoT devices in service by 2020 and far more than that once autonomous vehicles hit the streets. Although not all these nodes will be connected to the Internet and cloud, owners of those that are will be charged a fee for connecting each one. To understand how the industry hopes to reap these rewards requires an exploration of its overall roadmap and underlying technologies.

The cellular industry has good reason to be confident that its solutions will fare well in the market because it has enormous inherent advantages that LPWAN providers do not. More than three decades of development have resulted in nearly ubiquitous coverage delivered by hundreds of thousands of macro-cell base stations and even more small cells. Most of this infrastructure requires only enhanced software to address the requirements of IoT, dramatically reducing the amount of new RF and microwave hardware. The industry also has enormous financial resources and support from thousands of device vendors and a single global organization, the Third-Generation Partnership Project (3GPP), which is responsible for standards development.

Taken together, these advantages logically seem likely to overwhelm even the most aggressive LPWAN competitors such as LoRaWAN, Sigfox, and Weightless. However, LPWAN providers have been feverishly building out their networks in key areas to establish a substantial customer base before the cellular industry charges forward. LPWAN networks are considerably less expensive to build and deploy than cellular networks, and they operate mostly in unlicensed spectrum, so don't have the regulatory burdens of the cellular industry.

Table 1 – Cellular Industry IoT Goals

Metric	Goal
Low power consumption	About a nanoamp, allowing 10-year life with battery capacity of five watt-hours
Continuous device cost reduction	For both infrastructure user equipment
Enhance coverage	Better performance outdoors and especially indoors
Enhanced security	Strong authentication and other features
Efficient data transfer	Enabled by small, intermittent blocks of data
Advanced network design	Simplified topology and deployment
Network scalability	More than 50,000 per base station
Increased coverage	Improvement of 15 to 20 dB (5 to 6 times)
Decreasing data rates	As low as possible while maintain QoS

The Long History of Cellular and IoT

Contrary to popular opinion, the IoT isn't all that new, and wireless carriers haven't just started providing connectivity solutions for it. The ability to connect machines with other machines has a long history, beginning when Supervisory Control And Data Acquisition (SCADA) systems were created in the 1960s. Since then, various wired and wireless solutions have been used to connect sensor-enabled equipment such as pumps, valves, and other components in the utility, fossil fuel delivery and processing industries, and other industries (**Figure 1**). Some have been using cellular technology since its second generation, and Verizon, AT&T, T-Mobile, and Sprint all offer data services based on Second-Generation (2G) technology. Verizon's IoT-related revenue has been growing by double digits, generating more than $500 million in profits in 2015, even before the coming IoT-centric enhancements are in place.

Figure 1: *A SCADA network allows an operator to monitor the status of arsenic removal system absorber vessels in a water treatment plant.*

To provide available spectrum for cellular IoT service, both domestic and international carriers have discontinued or soon plan to discontinue 2G service. AT&T turned off its 2G service at the end of 2016 and other carriers will follow, ultimately resulting in a total discontinuance of 2G service by the end of 2019. In the interim, wireless carriers have been upgrading current IoT customers to 3G spectrum or more recently to IoT-centric Long-Term Evolution (LTE) technology such as LTE-M, which is LTE for Machine-To-Machine (M2M) connectivity. In short, M2M and cellular have been linked for years, but the future for cellular technology lies in its road map for the future.

Refining Cellular Technology for IoT

The cellular industry has a solid strategy for making its technologies better suited for IoT. The overall goals of the industry are shown in **Table 1**. From a technical perspective, the approach is the near opposite of what is being developed for its traditional voice and data markets. That is, the next major benchmark for the industry is its fifth generation, 5G, which promises blazingly fast data rates delivered in part through channel bandwidths wider than those of today.

In contrast, its plans for IoT are moving in the opposite direction, from the current wideband, high-data-rate capabilities of LTE-Advanced (**Figure 2**) and LTE-Advanced Pro, to extremely narrowband, low-data-rate, low-power LTE variants such as LTE-M and Narrowband-IoT (NB-IoT). There are similarities among these paths, as each approach aims to reduce latency, increase spectral efficiency, and dramatically simplify and reduce network and end-user hardware costs. Nevertheless, providing IoT connectivity is very different from anything the industry has faced before.

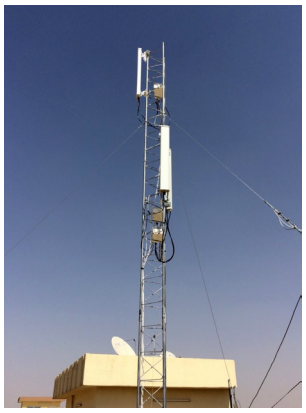


Figure 2: *An LTE Advanced base station with three tower-mounted remote radio heads used for broadband wireless.*

The overall strategy is to implement IoT connectivity today using the latest versions of LTE while consistently improving on them within the next three to four years, at which time the standards making up 5G will have been released. The industry can then use the technological wizardry within the 5G standards to further increase performance. This becomes obvious when viewing **Table 2**, which shows the variations of the 3GPP standards Release 8 to Release 13, which was finalized in 2016. Note that LoRa, one of the most significant competitors to cellular IoT solutions being deployed today, already uses very narrow bandwidths and low data rates, which is a marketable benefit for LPWAN providers using this technology.

Cellular Technologies for IoT

The cellular roadmap is based on the use of three versions of wireless technology:

LTE-M is a low-power standard that supports IoT by reducing device (modem) complexity and increasing coverage, while allowing the reuse of existing LTE infrastructure, to enable IoT devices to operate for at least 10 years in a wider range of applications. It is supported by major mobile equipment, chipset, and module manufacturers, and it benefits from current network security capabilities such as identity confidentiality and authentication, data integrity, and mobile equipment identification. It is currently being deployed by major carriers such as AT&T and Verizon.

LTE-M is energy efficient as it uses techniques called extended Discontinuous Repetition Cycle (eDRX) and Power Saving Mode (PSM). eDRX allows device to have longer sleep cycles so they can communicate with the network at different times ranging from 10 second to 40 minutes or more. PSM improves IoT device battery life by providing advanced power management, turning the device's modem on and off at scheduled intervals to save power, while allowing the modem to remain "connectable" even when most of its functions are inactive.

EC-GSM-IoT is designed to provide coverage for IoT devices in difficult radio environments and is backwards-compatible with previous releases so it can be used within existing GSM networks as a software upgrade. It provides broad coverage, allows resource sharing between EC-GSM-IoT and legacy packet-switched services, and can be introduced into a network without dedicated resources for IoT. In addition to excellent coverage, EC-GSM-IoT uses a simplified protocol layer to reduce device complexity, extend battery life, and utilize a security framework comparable to 4G standards.

NB-IoT uses the LTE physical layer and higher protocol layers and extends coverage and capacity while dramatically reducing device complexity. Designed to operate at almost any frequency range with existing cellular networks, NB-IoT focuses on transmission and reception of small amounts of data. It has the least power consumption of any cellular IoT standard while still providing long-range coverage, especially in "RF-resistant" environments such as buildings and below-ground installations such as subways.

Typical Applications and Their Needs

One of the reasons IoT is so difficult to grasp is that it encompasses a wide variety of unique applications, each with almost completely different requirements. For example, a typical wireless-enabled water meter might transmit messages twice a day and be deployed densely throughout an area where thousands of meters are installed per square mile.

When IoT is used for managing fleets of rentable bicycles, their sensors might transmit data 50 times per day from different locations that could be thinly dispersed at a rate of several hundred per square mile. In a manufacturing facility, there might be 500 sensor-enabled machines or other components that transmit infrequently, typically only when an event occurs. The autonomous vehicle environment is vastly different from all of these as thousands of vehicles each with perhaps a dozen sensors could transmit hundreds of times per day or more, and will almost always be mobile.

Both cellular IoT networks and LPWANs must accommodate all of these conditions and many more. It's arguable that cellular networks have a distinct advantage in this regard because they already serve fixed and mobile devices, deliver very high quality of service and security, and have every feature required of a robust commercial network. They also operate on licensed spectrum rather than unlicensed Industrial Scientific and Medical (ISM) bands that are densely populated by services such as Bluetooth and Wi-Fi and present interference challenges. In addition, roaming between networks of different providers has been a feature of cellular since its inception, which cannot be said for LPWANs that at least initially will be regional services based on Sigfox, LoRa, or other standards, which inhibits roaming.

Future Trends

No detailed prediction made today about how cellular and LPWAN will fare in serving IoT is likely to prove true a decade from now. The cellular industry could capitalize on its inherent strengths to simply overwhelm LPWAN providers and make them redundant. LPWAN providers could carefully craft their service offerings to serve markets and niche applications that wireless carriers either cannot or will not pursue. It's even possible that wireless carriers could make themselves indispensable by expanding their services all the way to the edge of where sensors are located, combining their long-range technologies with those such as Bluetooth, ZigBee, Z-Wave, Wi-Fi, and others that connect sensors on a local level.

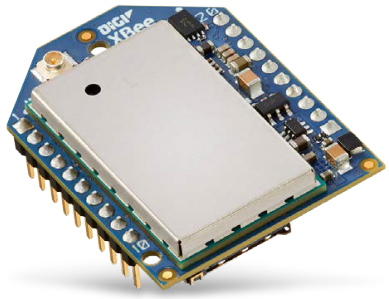
And that's not really a stretch: In September 2015, for example, Verizon introduced a platform called ThingSpace to boost the creation of IoT-enabled devices and applications. To bolster the effect, it has had multiple acquisitions. Last year it acquired fleet logistics and telematics system developer Telogis, followed by the GPS fleet tracking system of Fleetmatics and LED lighting company Sensity Systems. Additionally, they acquired LQD Wi-Fi, which, among other offerings, makes "smart" kiosks that provide free Wi-Fi, local community information, mapping, public safety announcements, transit updates, and upcoming events. Collectively, they move Verizon decisively into a broad array of applications, from consumer IoT to smart cities.

It's important to remember that, although there are many IoT devices already in service today, they represent the very beginning of IoT; the scenarios described here are just a few that may result once cellular IoT and LPWAN have fully established themselves, and there will surely be others. Regardless of how this industry evolves, we can not only expect challenges and obstacles on the way, but interesting engineering problems and opportunities as well.

Table 2 – Bandwidth and data rates compared

	LoRaWAN	LTE	EC-GSM-IoT	LTE-M	NB-IoT
Channel bandwidth	<500 kHz	1.4 to 20 MHz	200 kHz	1.08 MHz	200 kHz
Maximum data rate	<50 kb/s	10 Mb/s down, 5 Mb/s up	<140 kb/s	<1 Mb/s	170 kb/s down, 250 kb/s up

Digi XBee® Cellular 3G Global

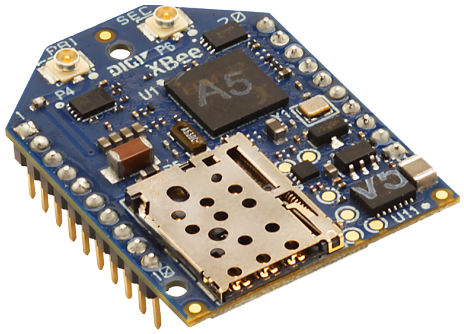


- FCC/IC, PTCRB, and AT&T certified – eliminates certification costs and risks
- Transparent and API modes simplify software integration
- Low-power modes for battery powered applications
- Integrated MicroPython programmability enables custom scripting directly on the modem
- Enhanced with Digi TrustFence™ security framework
- Manage and configure with Digi XCTU and Digi Remote Manager®

Digi XBee Cellular 3G global embedded modems provide a simple path to 3G (HSPA/GSM) with 2G fallback connectivity for OEMs with worldwide deployments. This modem is FCC/IC, PTCRB and AT&T certified which completely eliminates the cost, complexity, and risk involved in the certification process.

The modem is programmable, with support for custom MicroPython applications running directly onboard, allowing users to more efficiently manage their devices and eliminating the need for an external microcontroller in certain use-cases. It includes the full suite of standard Digi XBee API frames and AT commands, so existing customers can simply drop this modem into their existing designs to instantly achieve 3G cellular integration, without the pain and hassle of doing a complete re-design.

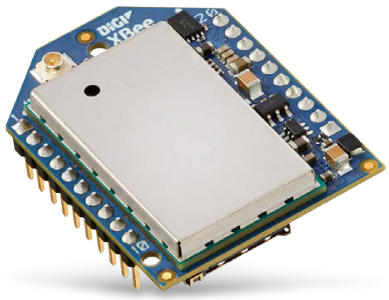
Digi XBee® Cellular LTE Cat 1



- FCC certified and Carrier End-device certified
- Authentic 20-pin Digi XBee® TH form factor; Smallest end-device certified cellular modem
- Digi XBee® Transparent and API modes simplify s/w design
- Integrated MicroPython programmability enables custom scripting directly on the modem
- OTA firmware updates

Digi is excited to bring together the power and flexibility of the Digi XBee ecosystem with the latest 4G cellular technology, with the new Digi XBee Cellular embedded modem. This solution enables OEMs to quickly integrate cutting edge 4G cellular technology into their devices and applications without dealing with the painful, time-consuming, expensive FCC and carrier end-device certifications. A bundled data plan will be included with every development kit with 6 months of free data, with the Digi XBee fully pre-provisioned and ready to communicate over the cellular network right out of the box.

Digi XBee® Cellular LTE-M

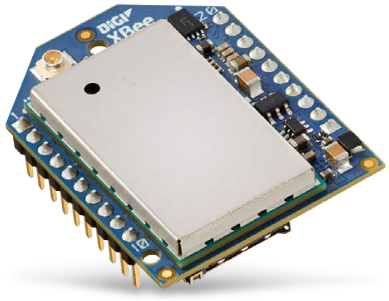


Coming Soon

The Digi XBee® Cellular LTE-M is a low-cost, low power wide area (LPWA) embedded cellular modem. It is FCC and carrier end-device certified which completely eliminates the cost, complexity, and risk involved in the certification process. The modem is programmable, with support for custom MicroPython applications running directly onboard, allowing users to more efficiently manage their devices and eliminating the need for an external microcontroller in certain use-cases. It includes the full suite of standard XBee API frames and AT commands, so existing customers can drop this modem into their existing designs to instantly achieve cellular integration, without the pain and hassle of doing a complete re-design.

- FCC certified and carrier end-device certified
- Excellent coverage and building penetration
- Digi XBee® Transparent and API modes simplify design
- Low power consumption optimized for long battery life
- Reduced hardware complexity with only 1 antenna required
- Integrated MicroPython programmability enables custom scripting directly on the modem

Digi XBee® Cellular LTE NB-IOT



Coming Soon

Digi XBee® Cellular Narrowband IoT (NB-IoT) is a low-cost, low power wide area (LPWA) embedded cellular modem designed specifically to handle small amounts of data over existing cellular networks, provide improved range, and optimized for maximum battery life.

The modem is programmable, with support for custom MicroPython applications running directly onboard, allowing users to more efficiently manage their devices and eliminating the need for an external microcontroller in certain use-cases.

It includes the full suite of standard Digi XBee API frames and AT commands, so existing customers can simply drop this modem into their existing designs to instantly achieve cellular integration, without the pain and hassle of doing a complete re-design. It is also CE/RED certified, making it ideal for use in LPWA applications in Europe.

- Extremely low power consumption for battery life of 10+ years
- Excellent coverage and building penetration
- Reduced hardware complexity with only 1 antenna required
- Transparent and API modes simplify software integration
- Integrated MicroPython programmability enables custom scripting directly on the modem
- CE/RED certified and network tested

Sorting Out IoT's Proliferating Short-Range Connectivity Solutions

By Barry Manz

The electronics industry has a long history of developing standards to serve the same goal: Betamax versus VHS, Windows versus Mac OS, USB versus Thunderbolt, and in the cellular world CDMA versus GSM (TDMA); however, competition between more than two or three standards has been rare. IoT changes this paradigm, as at least seven different solutions are available for connecting IoT devices over short distances—nearly all of which are incompatible. Each one has unique advantages and disadvantages, and all are continuously evolving. The result: A fragmented IoT industry leading to frustration, confusion, and skepticism about IoT, ranging from designers to potential customers—the opposite of what's necessary for IoT to achieve its projected massive growth.

To grasp what all this means for IoT requires digging down into the details of the competing connectivity technologies and their applications. First, it's important to differentiate between IoT connectivity solutions, which can be grouped into two broad categories: Short-range and long-range. The former, covered in this article, is the domain of technologies such as Wi-Fi, Bluetooth, ZigBee, Z-Wave, Thread, 6LoWPAN, and ANT+. This article explores key capabilities of short-range solutions, compares the seven primary solutions available today, identifies two leading solutions, discusses challenges that design engineers face in implementing short-range solutions, and looks ahead to continued improvements in these solutions.

Short-Range Communication Functionality

Short-range solutions comprise multiple requirements and capabilities:

- Support a large number of IoT devices to communicate with each other over a network, preferably a mesh
- Enable IoT devices to operate for many years on a coin cell battery
- Provide robust security
- Achieve the lowest possible complexity and hardware costs
- Accommodate Internet Protocol Version 6 (IPv6)

Network Connectivity

In nearly all IoT applications, IoT devices must be able to connect to each other so the information they gather can be aggregated and sent on for processing and analysis, performed both locally and over long distances to reach data center resources (i.e., the cloud). In the comparatively simple example of home automation, the amount of gathered information is much less than in a massive network of electric meters; however, rather than simply gathering one type of measurement (e.g., voltage and current), measurements can be numerous, including temperature and humidity, power usage, video, equipment status, and many others. Nevertheless, both applications require information to be gathered by wireless-enabled sensors.

All short-range IoT connectivity solutions incorporate networking capability except for Wi-Fi, which was never designed for IoT-type applications, and can accommodate from several hundred to tens of thousands of devices. Not all network types have the same capabilities, though. The one best suited for IoT is the mesh network (**Figure 1**), in which all devices can communicate with each other without needing to first pass information through a hub such as a router or a gateway. Mesh networking is crucial for the largest applications where IoT devices may span vast areas, such as on a farm, large production facility, and hundreds of other environments.

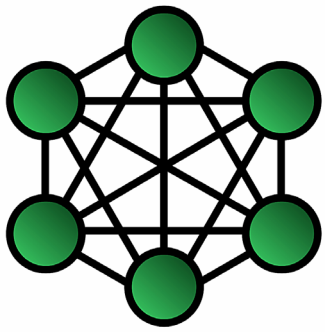


Figure 1: *In a mesh network, all devices can connect directly to each other.*

Low Power Consumption

In home automation systems, most devices can be powered by $120V_{AC}$, but others such as "smart" door locks and alarm system sensors are powered by coin cells or other small batteries. In most other applications, such as in a production facility or a farm, nearly all the devices are powered by batteries or possibly by solar cells. As envisioned, the majority of IoT devices would be powered by batteries, so connectivity solutions have been designed to accommodate this requirement.

To achieve this, the devices themselves must consume very little power, and the network must use communication techniques that feature very low data rates and minimal sensor RF transmit power. IoT devices rarely, if ever, need to communicate continuously, but they still need to be able to receive a command from an external source such as a long-range communication system and from the components that they serve. IoT devices meet this need by enabling the devices to "sleep," keeping only those functions awake that are required to detect activity from the component the sensor serves or from the network. Except for Wi-Fi, every IoT connectivity solution has been designed with this in mind.

Security

Every IoT connectivity solution incorporates multiple types of security ranging from AES encryption to multiple levels of authentication. Although solutions might implement security features differently from one another, they are all at least reasonably secure, with the caveat that every type of communication network is vulnerable. Various attack types have been used to infiltrate every IoT connectivity solution, and this situation will become increasingly challenging in the future when thousands or tens of thousands of sensors may constitute a single network. Knowing this, all participants in IoT connectivity are working to establish greater end-to-end security.

Simplicity and Low-Cost Hardware

In the earliest days of IoT, hardware was expensive, and there were few resources to help designers implement a connected environment. Fortunately, this is no longer the case, as every silicon vendor provides a broad array of tools that aim to ensure their products can be easily incorporated into solutions. Some vendors also have complete "ecosystems" that range from design resources to complete system descriptions incorporating all aspects that must be considered. In addition, the cost of IoT devices is rapidly decreasing as volumes increase; this is predicted to continue even as devices have greater levels of function integration.

IPv6 Capability

Internet Protocol Version 4 (IPv4) is the underlying technology that makes it possible to connect devices to the Web. It's been used since 1983 and, having reached its maximum of 4.29 billion addresses, will run out in the relatively near future. IPv6, however, will provide enough for a very long time, even with the massive increase in addresses attributable to the billions of new deployed IoT devices in the coming years.

Implementing IPv6 rather than IPv4 in every new IoT system is essential, but it's not as simple as it might seem. It requires significant changes to many types of software, and exchanging data between these protocols requires special gateways. Nevertheless, as IoT systems are (or should be) designed to be massively scalable over time, IPv6 is a standard requirement. All current connectivity solutions either natively employ IPv6 or can be configured to do so.

Comparing the Major IoT Connectivity Solutions

Table 1 summarizes the primary IoT connectivity solutions. While this list was made as inclusive as possible, there are no doubt others that might ultimately gain momentum in the future.

The outlier among those in Table 1 is Wi-Fi, which is fundamentally different in many ways, in part because it has been around longer than any other short-range technology. Wi-Fi was also never intended to deal with tiny, power-sipping devices like IoT sensors, as the goal was to replace wired local area networks with wireless versions delivering comparable performance, primarily high speed.

Wi-Fi requires relatively power-hungry access points, and its components remain comparatively expensive. Consequently, no other connectivity solution comes close to the throughput achievable by Wi-Fi, which keeps it very appealing as an adjunct to some low-power solutions for connecting them to the Internet. This is especially true for IoT applications like video surveillance that require broad channel bandwidths and high data rates.

Wi-Fi, ZigBee, Z-Wave, and Bluetooth are further along in their development than others, and ZigBee is currently used by the most IoT applications. Thread, which was created by Nest Labs (acquired by Google), is increasing in popularity and has more than 50 members (**Figure 2**), and ANT+ is somewhat popular in Europe.

Figure 2: *All Nest products like the Nest Learning Thermostat use 802.15.4 for connecting themselves together and Wi-Fi to connect to the Internet.*

Table 1 – Most Common Short-Range IoT Connectivity Solutions

	Bluetooth 5	6LoWPAN	ZigBee	Wi-Fi	Z-Wave	Thread	ANT
Standard	802.15.1	802.15.4	802.15.4	802.11a,b,g,n,ac	802.15.4	802.15.4	250
Frequency	2.4 GHz	868 and 915 MHz, 2.4 GHz	800 and 900 MHz, 2.4 GHz	2.4 and 5 GHz	908.4 MHz	902 to 928 MHz, 2.4 GHz	2.4 GHz
Maximum data rate	2 Mb/s	250 kb/s	250 Kb/s	Up to 1 Gb/s	100 Kb/s	250 Kb/s	60 Kb/s
Maximum range (m)	200	10	100	40	100	30	30
Power consumption	Very low	Low	Low	High	Low	Low	Low
Battery life	Up to 10 years		Hours	NA	3 years	Years	Low
Network size	Unlimited		64,000+	255	232+	300	65,533
Mesh support	Yes	Yes	Yes	No	Yes	Yes	Yes
Beacon support	Yes	No					
IPv6 support	Yes	Yes					
Overall cost	Low	Decreasing	Moderate	High	Moderate	Low	Low
Industry support	Ubiquitous	Growing	Growing	Ubiquitous	Less	Moderate	Least

Two Breakout Stars

Two IoT connectivity solutions have recently shaken up the industry:

- Bluetooth
- 6LoWPAN

Bluetooth

Bluetooth 5, the latest version of the standard, builds on its predecessor, Bluetooth Low Energy (Versions 4.0 and 4.2), while doubling maximum data rate to 2Mbs, increasing distance from about 30m to about 120m under ideal conditions, and adding mesh networking capability. With these improvements, Bluetooth has all the trappings now to serve almost any application. It also has the benefit of being, along with Wi-Fi, the most widely used short-range connectivity standard in the world with massive industry support and integration within every smartphone, tablet, newer laptop, and hundreds of other types of products.

Bluetooth also has a feature offered by no other solution: Beaconing. Beacons are tiny short-range transmitters that send short messages to smartphones whose owners have installed beaconing apps. The Bluetooth receiver on the phone receives the messages, and the app places notifications on the display for coupons, reward points, or almost anything. Beacons are so small and inexpensive they can be deployed throughout a location, from display cases to checkout lanes. Retailers can use the information gathered by beacons to determine what products shoppers like and whether they buy something. Museums, zoos, and similar organizations can place beacons at every painting, display, or creature someone is viewing. Similarly, attendees at trade shows and other events can register automatically, and airports can help visually impaired people identify their surroundings. The potential applications are practically limitless.

6LoWPAN

The other solution getting more attention recently is the awkwardly-named 6LoWPAN, which stands for IPv6 over Low-Power Wireless Personal Area Networks. 6LoWPAN is usually referred to as a competitor to Zigbee and Z-Wave because they are the industry leaders and all three are based on the 802.15.4 standard. But 6LoWPAN has advantages over ZigBee, Z-Wave, and other options as well. For example, while ZigBee devices can interoperate with other ZigBee devices, 6LoWPAN can interoperate with any solution based on 802.15.4 using a very simple IPv6-enabled bridge or any other devices in an IP-based network.

This also includes Bluetooth, so-called sub-1 GHz solutions, power lines, and even Ethernet. To achieve the same capability, ZigBee and Z-Wave require more complex application layer gateways. With 6LoWPAN, every node in the network has its own IPv6 address, so it can be directly connected to the Internet using open standards. Because 6LoWPAN has the other ingredients to make it well suited for IoT and is unique in its ability to interoperate with other IP-based standards, it solves one of the thorniest problems facing developers. In short, 6LoWPAN and Bluetooth are the new players to watch as IoT evolves in the coming years.

The Challenges for IoT System Manufacturers

Although 6LoWPAN is a highly appealing answer to the problems of having too many competing standards, manufacturers of end-user solutions still face the issue of which standard to choose today that will hold up as new solutions emerge. The home automation market provides a good example of these challenges.

A “typical” home has many types of devices that can be connected wirelessly, from door locks to lights, HVAC systems, surveillance cameras and alarm systems, entertainment suites, and even appliances. An “ideal” connectivity solution would be able to serve both wall-powered and battery-operated devices, communicate at both low and high speeds (and, thus, use both narrow and wide bandwidths), and work with products from different manufacturers that use different connectivity solutions.

Perhaps needless to say, this is not the current situation, and manufacturers use multiple connectivity solutions to meet market product demands. For example, manufacturers of smart lighting use Bluetooth, ZigBee, or Z-Wave to connect the lights to each other and use another solution to connect to the Internet. A manufacturer that has committed to say, ZigBee, is effectively stuck with it if a better solution comes along. The company could choose to update to the newer solution but would still need to support its legacy devices, so its products would now have to support two solutions along with the connection to the Internet. It’s also conceivable that this could happen again, presenting an even more vexing problem. As the emergence of Bluetooth 5 and multi-solution capabilities of 6LoWPAN illustrate, this is more than a hypothetical situation.

Conclusion

Currently, designers have at least seven different solutions to choose from in connecting IoT devices over short distances: Wi-Fi, Bluetooth, ZigBee, Z-Wave, Thread, 6LoWPAN, and ANT+. Nearly all of these solutions are incompatible and offer various advantages and disadvantages as they continue to evolve. In several market sectors, especially home automation, manufacturers have been forced to employ more than one connectivity solution in their products, and they may ultimately may need to include even more, as this is far from a “one size fits all” environment.

The problem hasn’t been lost on manufacturers of devices such as IoT radios, RF front-ends, controllers, and other components that increasingly support multiple standards. This allows designers to use a single device or set of devices to support multiple product lines, and enables manufacturers of end-user systems to more easily and cost-effectively “future-proof” their products. What it does not do is completely simplify the design process, as some solutions are inherently better suited for specific applications and each connectivity solution must typically be configured differently. But in today’s current massively-fragmented IoT connectivity environment, any new technology that partially solves interoperability problems is a welcome sight.

Short-Range Connectivity Solutions for Specific Use Cases

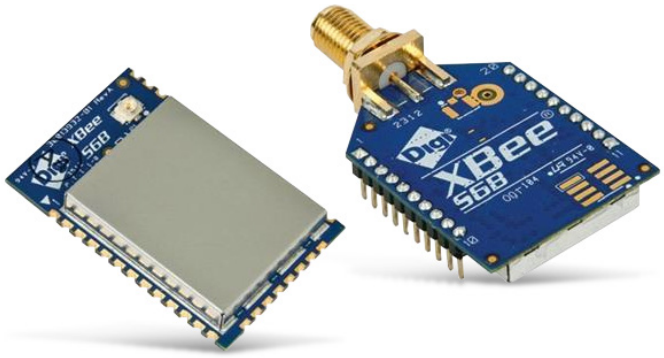
EnOcean: A spin-off from Siemens, EnOcean GmbH is located in Germany, and its wireless modules are built and marketed by the company. It’s primary claim to fame is the energy harvesting, which enables devices to work without a battery. It has a range of 300m in free space, has data rates below 125kbs, and optimizes the amount of power required to transmit a given amount of data. EnOcean operates at 902, 928.35, 868.3, and 315MHz depending on the country.

Insteon: This solution from Smartlabs enables IoT devices to communicate wirelessly or through power lines in a dual-band type of mesh networking and is compatible with the X10 wired network standard. It has considerable support from industry including Apple, Microsoft, Amazon, Logitech, and others. Maximum sustained data rate is 180bs, free-space range is up to about 45m, and operating frequency is 902 to 924MHz.

Microchip Wireless Networking (MiWi): This Microchip-proprietary protocol is based on the 802.15.4 standard, operates at 2.4GHz or below 1GHz, is compatible with ZigBee, and can be configured in star, cluster, mesh, and tree network topologies.

Wireless Highway Addressable Remote Transducer Protocol (WirelessHART): Designed to serve process field device networks in process automation, this open standard developed by the HART Communication Foundation uses a time-synchronized, self-organizing, self-healing mesh architecture, and it operates at 2.4GHz using 802.15.4 radios.

Digi XBee® Wi-Fi Module

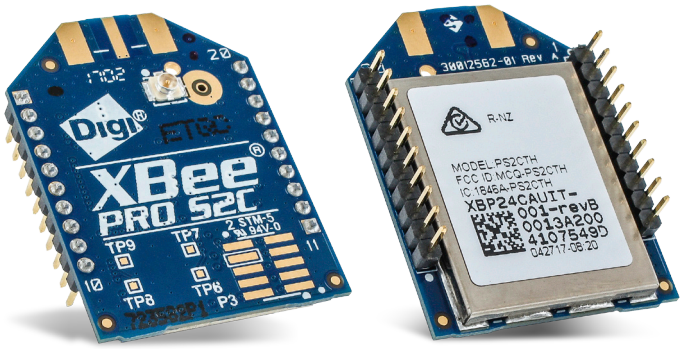


Developing a cloud-connected product requires expertise in both hardware and software development, and merging these worlds together to create a new product can be costly and time-consuming.

The Digi XBee® Wi-Fi embedded module brings the popular Digi XBee® platform to the Digi Remote Manager, allowing developers to build cloud-connected Wi-Fi products quicker and more efficiently than ever before.

- Build cloud-connected Wi-Fi prototypes in under an hour
- Popular Digi XBee® Through-Hole and Surface-Mount footprints
- Ideal for Industrial Applications that require fast time to market
- Easily connect to a smartphone or tablet for configuration or data transfer
- 802.11b/g/n provides up to 72Mbps data rate
- Native Remote Manager support: Module can automatically connect to Digi Remote Manager
- Simple provisioning tools: SoftAP, WPS, and a local WebUI are all available to make provisioning the module a breeze

Digi XBee® 802.15.4 Module



Digi XBee® 802.15.4 RF modules are ideal for applications requiring low latency and predictable communication timing. Providing quick, robust communication in point-to-point, peer-to-peer, and multipoint/star configurations, Digi XBee® 802.15.4 products enable robust end-point connectivity with ease.

Whether deployed as a pure cable replacement for simple serial communication, or as part of a more complex hub-and-spoke network of sensors, Digi XBee® 802.15.4 RF modules maximize performance and ease of development.

- Simple, out-of-the-box RF communications, no configuration needed
- Point-to-multipoint network topology
- 2.4GHz for worldwide deployment
- Common Digi XBee® footprint for a variety of RF modules
- Industry leading sleep current of sub-1uA
- Firmware upgrades via UART, SPI or over the air
- Migratable to DigiMesh and ZigBee PRO protocols and vice-versa

Digi XBee® Thread Module

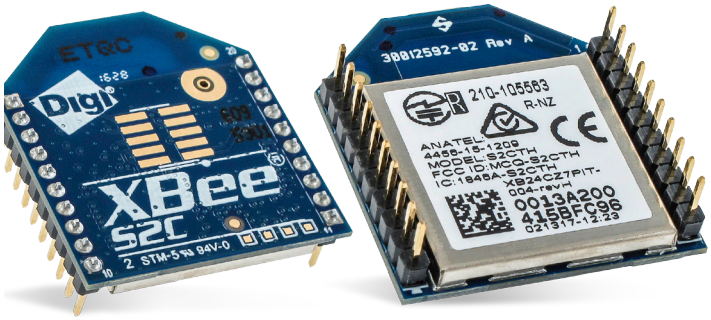
- Simple to setup and use
- Highly secure
- Power-efficient
- An open protocol that carries IPv6 natively
- A robust mesh network with no single point of failure
- Runs over standard 802.15.4 radios
- Support for a wide variety of host devices

Thread is a new open global wireless standard developed to balance and improve on the increasingly important requirements of reliability, security, power efficiency and cost effectiveness.

Thread runs on the IEEE 802.15.4 physical radio specification and operates in the unlicensed ISM bands including 2.4GHz (v1.0).

The network layer implements IPv6 addressing architecture with 6LoWPAN header compression and mesh capabilities for maximum routing efficiency and redundancy. Another key advantage of Thread is that the application layer is separated from the actual Thread stack, making it agnostic and flexible for use with independently defined application layer standards, including the familiar ZigBee protocol as well as other popular protocols. This allows a level of forward compatibility between existing and new devices, making Thread attractive for designers and consumers alike.

Digi XBee® Zigbee Module



- Programmable versions with on-board microprocessor enable custom ZigBee application development
- Through-hole and surface mount form factors enable flexible design options
- Link budgets of 110dB for Digi XBee® and 119dB for Digi XBee-PRO®
- Industry-leading sleep current
- Firmware upgrades via UART, SPI or over the air (OTA)

Digi XBee® and Digi XBee-PRO® ZigBee modules are ideal for applications in the energy and controls markets where manufacturing efficiencies are critical.

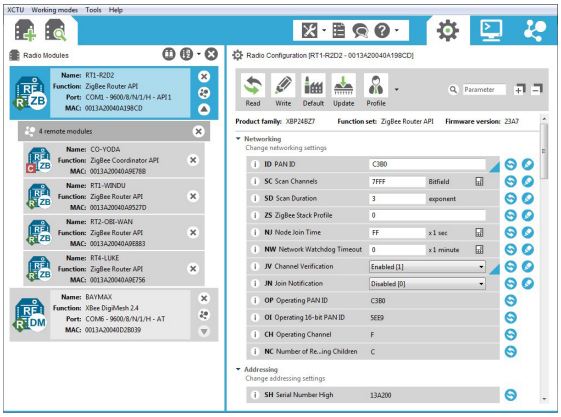
The Serial Peripheral Interface (SPI) provides a high-speed interface and optimizes integration with embedded microcontrollers, lowering development costs and reducing time to market.

Products in the Digi XBee® family require little to no configuration or additional development. Programmable versions of the Digi XBee® and Digi XBee-PRO® ZigBee module make customizing applications easy.

Programming directly on the module eliminates the need for a separate processor. Because the wireless software is isolated, applications can be developed with no risk to RF performance or security.

DIGI XCTU
Configuration & Test
Utility Software

Next Generation Configuration Platform for Digi XBee®/RF Solutions



Free, multi-platform application compatible with Windows, MacOS and Linux

Graphical Network View for simple wireless network configuration and architecture

API Frame Builder is a simple development tool for quickly building Digi XBee® API frames

Firmware Release Notes Viewer allows users to explore and read firmware release notes

Digi XCTU is a free multi-platform application designed to enable developers to interact with Digi RF modules through a simple-to-use graphical interface. It includes new tools that make it easy to set-up, configure and test Digi XBee® RF modules.

Digi XCTU includes all of the tools a developer needs to quickly get up and running with XBee. Unique features like graphical network view, which graphically represents the Digi XBee® network along with the signal strength of each connection, and the Digi XBee® API frame builder, which intuitively helps to build and interpret API frames for Digi XBees® being used in API mode, combine to make development on the Digi XBee® platform easier than ever.

Other highlights of Digi XCTU include the following features:

- You can manage and configure multiple RF devices, even remotely (over-the-air) connected devices.
- The firmware update process seamlessly restores your module settings, automatically handling mode and baud rate changes.
- Two specific API and AT consoles, have been designed from scratch to communicate with your radio devices.
- You can now save your console sessions and load them in a different PC running Digi XCTU.
- An update process allows you to automatically update the application itself and the radio firmware library without needing to download any extra files.
- Digi XCTU contains complete and comprehensive documentation which can be accessed at any time.

Digi XCTU includes a set of embedded tools that can be executed without having any RF module connected:

Frames generator: Easily generate any kind of API frame to save its value.

Frames interpreter: Decode an API frame and see its specific frame values.

Recovery: Recover radio modules which have damaged firmware or are in programming mode.

Load console session: Load a console session saved in any PC running Digi XCTU.

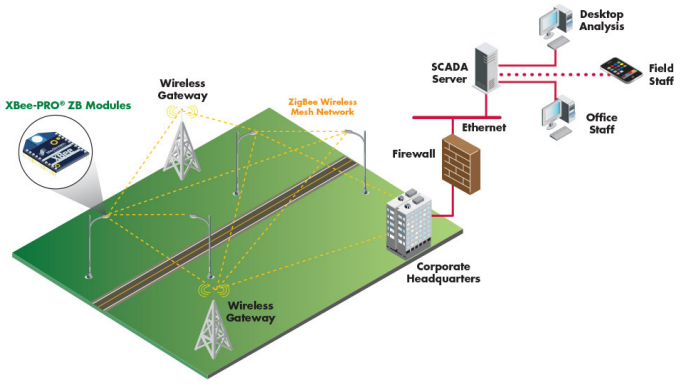
Range test: Perform a range test between 2 radio modules of the same network.

Firmware explorer: Navigate through Digi XCTU's firmware library.

Digi XBee® Enables Street Light Management System

CIMCON Software, a leading developer of automated street light control systems, helps communities reduce the maintenance cost and environmental footprint of street lights. CIMCON's LightingGale system replaces traditional street light photocells with a Street Light Controller (SLC). The SLC can monitor pertinent electrical parameters and control the light in a variety of ways – from dimming the lights during peak hours to setting schedules so groups of lights can be turned on and off at set times to conserve energy. The system can also send alerts when something goes wrong. This eliminates the need to physically inspect the system on a regular basis which greatly reduces maintenance costs.

To overcome these issues, CIMCON chose Digi's XBee-PRO® ZB module for the project because of its rugged design, ease of use and reliability.



Mesh networking with the Digi XBee-Pro ZB Modules

BUSINESS CHALLENGE

CIMCON needed a rugged mesh networking solution to connect island street lights and remote electrical monitoring reclosures across the entire island of St. John, a mountainous region with dense vegetation, warm temperatures, high humidity, regular thundershowers and a hurricane season. Under these conditions, CIMCON felt the highest risk would be the communication between the SLCs and the gateway.

"We needed something that was easy to use and could withstand the harsh elements," said Anil Agrawal, director, CIMCON Software. "We also needed a solution that could traverse great ranges and dense brush. Digi offers the industry's leading ZigBee products, and we felt confident its XBee® modules would prove reliable under the severe island conditions. In addition, Digi's K-Node service allowed us to simulate our ZigBee network performance so that we were able to deploy with 100% confidence."

SOLUTION

More than 650 SLCs are attached to street lights scattered across the island of St. John. Because of the ruggedness and range of Digi's XBee-PRO ZB module, CIMCON was able to establish full communication across the entire island by deploying only two gateways. The gateways then connect the mesh network to Cimcon's LightingGale management software where customers can easily access street light energy consumption data and control individual lights.

"The island only has two gateways covering 28 square miles of land," Agrawal added. "I was pleasantly surprised that the Digi modules could cover the entire island with only two gateways. The products provide tremendous range through dense brush and over mountains – and we even have some modules covering 1.7 miles over water."

RESULTS

In addition to street lighting control, the solution enables smartphone applications where customers can set up alarms and receive notifications regarding energy consumption and faults – improving customer satisfaction and reducing energy consumption. The XBee-powered mesh network will also be used by the Virgin Island Water and Power Authority to connect its electrical monitoring reclosures. Approximately 60 reclosures are located throughout the three US Virgin Islands, transmitting power to homes and businesses. When completed, the Virgin Island Water and Power Authority will be able to easily monitor and control each reclosure remotely over the mesh network.

"Digi was extremely supportive before we were even in there with customers," Agrawal concluded. "Tech support was very helpful in the beginning in trying to determine where the load would be. We were able to simulate up to 15 hops in 500 nodes using Digi's K-Node service and established parameters that would work for the network. Once we were on the island, everything just worked like it did in the lab. We were so well prepared going in that we haven't needed any tech support since.

Getting to IoT Ubiquity: Cellular Versus LPWAN Connectivity

By Barry Manz

Connectivity is one of the most frustrating aspects to tackle for designers of IoT networks. At the "edge" where sensors communicate with each other, there are multiple, mostly incompatible, competing standards. From the edge to the Internet and cloud there are only two: Wireless carriers and Low-Power Wide Area networks (LPWANs) in competition. LPWAN providers use more than one standard, and some are proprietary, while the cellular industry roadmap focuses on streamlining and enhancing the capabilities of current offerings centered on the Long-Term Evolution (LTE) standard. So even though there are only two basic competitors in the longer-range market, it's still necessary to have basic knowledge about each one, along with their advantages, disadvantages and applicability for specific applications.

Why All the Attention About Connectivity?

Why all the focus on connectivity? It comes down to money: Wireless carriers and LPWAN providers charge a fee for every connected device, and the number of IoT devices is growing rapidly. It took more than three decades for global wireless carriers to reach the current 2.3 billion subscribers, but in the few years that IoT services have been available, more than 8.4 billion IoT devices have been connected, and by 2020 there should be at least 20 billion. Even though all IoT devices won't ultimately connect to the Internet, "only" 10 billion of them would still create immense annual revenues for service providers. Needless to say, this is a huge revenue opportunity. However, there are broad differences between IoT applications, and the current capabilities of cellular-based and LPWAN solutions are different, so there is no single standard that will satisfy every need.

To illustrate these differences, consider that connecting "smart" electric utility meters (**Figure 1**) to the Internet in a city with 100,000 residences, businesses, and other water-using entities is vastly different from sending data outward from 250 machines in a single industrial facility. On a sprawling farm, many types of sensors are spread over miles of land rather than in a single building, and the seeming inevitability of autonomous vehicles will create a unique IoT environment of immense complexity requiring connectivity between vehicles as well as fixed infrastructure.

Figure 1: *There are already nearly 70 million "smart" electricity meters in the U.S., each one transmitting periodic usage updates typically via a LPWAN but soon via cellular networks a well.*

However, regardless of the application, services provided by wireless carriers and LPWAN providers have the common goal of allowing tiny sensors installed on host devices—such as valves, motors, and pumps—to communicate periodically to an external point for years while powered by a coin cell battery. Although both types of service providers attack this problem in somewhat different ways, both use a variety of techniques expressly designed for the IoT environment. For example, they limit the amount and duration of data transmission and times at which sensors must be communicating, and they also use very low data rates that require only narrow bandwidths.

In addition, as low-power signals transmitted by wireless-enabled sensors are very weak, the base station receivers that detect them must be extremely sensitive. The base stations themselves must also use techniques such as Multiple Input Multiple Output (MIMO), illustrated in **Figure 2**, and in some cases use highly directional antennas to ensure constant connections.

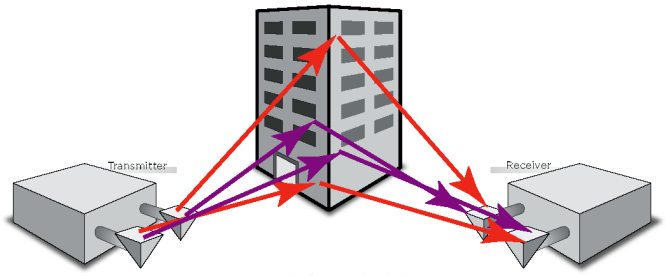


Figure 2: *Multipath propagation is generally considered highly undesirable, but MIMO exploits it to significantly increase network capacity using multiple transmit and receive antennas at both ends of the transmission path to minimize errors and optimize throughput.*

Finally, many small base stations (the so-called small cells) will be needed to shorten the distance signals must travel, which reduces latency to the almost instantaneous levels that some IoT applications require.

Cellular And LPWANs Compared

The cellular industry has unique advantages for IoT. Carriers already have almost ubiquitous LTE coverage in the U.S. delivered by several hundred thousand macro base stations and perhaps three times that many small cells. Updating this infrastructure to accommodate communication with IoT devices in most cases requires just a software upgrade rather than a major investment in hardware such as RF and microwave transceivers. In addition, even before IoT was widely recognized as the next big thing, wireless carriers were already providing connectivity to wireless-enabled sensors using legacy Second-Generation (2G) technology.

The industry has also been working for years to accommodate IoT. The Third Generation Partnership Project (3GPP) that manages development and issuance of wireless standards has included substantial specifications dedicated to IoT in its latest standard called Release 13 that was finalized in June 2016. These capabilities will continue to be enhanced between now and when the first standards for the fifth generation of cellular will be released, most likely in 2019. By that time, wireless carriers will have a solid foundation in IoT connectivity.

In contrast, LPWAN providers have no such advantages. As they are entirely new entities in the wireless world, every system in every area where coverage is desired must be built from the ground up. They also have a limited time in which to deploy these networks in key (typically urban) areas, as the cellular industry is rapidly rolling out its IoT-centric data plans. Fortunately, LPWAN systems are less expensive to build and deploy than cellular networks, do not always require leasing space on a tower, and can cover wide geographical areas with fewer base stations.

The question today is whether LPWAN providers can survive in a cellular-dominated world. Most analysts believe they will, as they offer similar capabilities to cellular networks such as carrier-grade security and other mandatory features, and may become cost-competitive for customers. Analysts also suggest that at least half of IoT use cases can be served by LPWANs. So, it's a relatively safe bet that, while the cellular industry will have a commanding presence in delivering IoT connectivity, there will still be room for LPWAN providers in what is likely to become a price war within individual markets.

Cellular IoT

As mentioned previously, the cellular industry is developing solutions for IoT connectivity based on LTE. The industry's overall roadmap is to build on current versions of LTE and continue to refine it, including reducing its complexity and cost. As this process unfolds, cellular technology will become better suited to a wider variety of IoT applications, ultimately leading to the introduction of the fifth generation of cellular technology, 5G.

The consensus in the industry appears to be based on the use of three different standards mostly introduced in Release 13 to achieve this goal, ultimately resulting in what is included in the 5G standards. These solutions should ideally be implemented at frequencies below 1GHz where propagation conditions are more conducive to longer-range and building penetration:

- LTE-M: Also called enhanced Machine Type Communication (eMTC), evolved from the LTE standard in Release 12 (2014) with further advances included in Release 13.
- NB-IoT: A narrowband version of LTE for IoT included in Release 13.
- EC-GSM-IoT: Extended Coverage-GSM for IoT is an extended coverage variation of Global System for Mobile Communications technology that was optimized for IoT in Release 13 and can be deployed along with a GSM carrier.
- 5G: Will be standardized by 2020, enhancing NB-IoT and EC-GSM-IoT.

The presumption is that, as the requirements for IoT are significantly different than those for traditional cellular operation, future developments should positively impact battery life using a power saving mode, reduce the complexity and thus cost of devices, reduce the cost of deployment by sharing carrier capacity, and enable broad coverage through the adoption of more advanced coding and increasing signals' spectral density.

Table 1 illustrates the evolution of cellular technology. For example, Release 8 offered peak downlink rates up to 150mbs as it was designed for traditional cellular applications. However, data rates decline precipitously to 150kbs in narrowband to accommodate IoT requirements. The same is true for the channel bandwidths of user equipment, which declines from a maximum of 18MHz in Release 8 to 180kHz in narrowband IoT. Another important factor is the complexity of the modem, which decreases by 85 percent over time. In short, the evolution of cellular technology to meet the needs of IoT is in many respects precisely the opposite of what is hoped to be achieved in 5G for traditional voice and data services. That is, rather than increasing data rates, it reduces them along with the overall complexity of cellular IoT networks and their components.

The LPWAN Alternatives

LPWAN providers use either open standards such as LoRaWAN, administered by the LoRaWAN Alliance, or proprietary solutions like Sigfox, both of which operate in unlicensed spectrum. Although Sigfox claims it's the world's leading IoT connectivity service with service available in 32 countries (mostly in Europe), LoRaWAN has gained the widest industry acceptance with more than 400 members in the alliance. This translates into continually decreasing cost of LoRa baseband and RF hardware, which has already dropped by more than half and will likely decline further as volume increases.

LoRaWAN

It's important to differentiate LoRa, LoRaWAN, and offerings by LinkLabs, as it can be a bit confusing. LoRa is the physical layer of the open standard administered by the LoRaWAN Alliance, while LoRaWAN is the Media Access Control (MAC) layer that provides networking functionality. LinkLabs is a member of the LoRaWAN Alliance that uses the Sematech LoRa chipset and provides a solution called Symphony Link that has features unique to the company, such as the ability to operate without a network server. Symphony Link uses an eight-channel base station operating in the 433MHz or 915MHz Industrial, Scientific, and Medical (ISM) bands as well as the 868MHz band used in Europe. It can transmit over a range of at least 10 miles and backhauls data using either Wi-Fi, a cellular network, or Ethernet using a cloud server to handle message routing, provisioning, and network management.

Sigfox

Sigfox was created by the French company by the same name. One of the major differences between it and LoRaWAN is that Sigfox owns all of its technology from the edge to the server and endpoint, and it effectively functions as the supplier of the entire ecosystem or, in some cases, as the network operator itself. However, the company allows its endpoint technology to be used free of charge by any organization that agrees to its terms, so it has been able to establish relationships with major IoT device suppliers and even some wireless carriers. Along with LoRaWAN, Sigfox continues to gain in market share, especially in Europe where its transmission length adheres to European Union guidelines. The version used in the U.S. is significantly different in order to meet Federal Communication Commission (FCC) rules. The only drawback of Sigfox is its proprietary nature.

Weightless

Weightless is an anomaly among IoT connectivity solutions, as it was developed as a truly open standard managed by the Weightless Special Interest Group. It gets its name from its "lightweight" protocol that typically requires only a few bytes of data per transmission. This makes it an excellent choice for IoT devices that communicate very little information such as some types of industrial and medical equipment, as well as electric

Table 1: The Evolution of Cellular IoT Technology

Specification	Release 8, Cat. 4	Release 8, Cat. 1	Release 13, Cat. 1 (eMTC, LTE-M)	Release 13, Cat. NB1 (NB-IoT)
Peak download rate	150 Mb/s	10 Mb/s	1 Mb/s	170 kb/s
User device receive (channel) bandwidth	1 to 18 MHz	1 to 18 MHz	1.08 MHz	180 kHz
Maximum user device transmit power (dBm)	23	23	20/23	20/23
Modem complexity (%)	100 (baseline)	80	20	15

and water meters. Unlike many other standards, Weightless operates in the so-called TV white spaces below 1GHz that were vacated by over-the-air broadcasters when they transitioned from analog to digital transmission. As these frequencies are in the sub-1GHz spectrum, they have the advantages of wide coverage with low transmit power from the base station along with the ability to penetrate buildings and other RF-challenged structures.

There are currently two Weightless versions:

- Weightless-N is an ultra-narrowband, unidirectional technology.
- Weightless-P is the company's flagship bidirectional offering that provides carrier-grade performance and security with extremely low power consumption in additon to other features.

Nwave

Nwave is an ultra-narrowband technology based on Software-Defined Radio (SDR) techniques that can operate in both licensed and unlicensed frequency bands. The base station can accommodate up to 1 million IoT devices over a range of 10Km with RF output power of 100mW or less and a data rate of 100bps. The company claims that battery-operated devices can function for up to 10 years. When operating in bands below 1GHz, Nwave takes advantage of the desirable propagation characteristics in this region.

Ingenu

Ingenu (formerly called On-Ramp Wireless) has developed a bidirectional solution based on many years of research, which resulted in a proprietary direct-sequence spread spectrum modulation technique called Random Phase Multiple Access (RPMA). RPMA was designed to provide a secure, wide-area footprint with high capacity operating in the 2.4GHz band.

A single RPMA access point covers 176mi.^{2} in the U.S., which is significantly greater than either Sigfox or LoRa. It has minimal overhead, low latency, and a broadcast capability that allows commands to be sent simultaneously to a very large number of devices. Hardware, software, and other capabilities are limited to those provided by the company, and the company builds its own public and private networks dedicated to machine-to-machine communications.

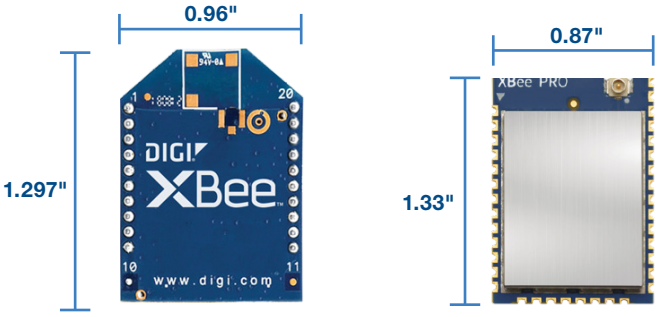
Summary

As only the cellular industry and LPWAN providers are competing for supremacy in the longer-range market, it's easy to assume that the designer's job is simple when compared with that required for short-range solutions. Nothing could be further from the truth; each competing technology offers an extraordinary range of variables, all of which contribute to their capabilities yet present major design challenges.

For end users, choosing the "right" solution will generally come down to which services are available in their area and how much they charge for connecting each device. However, if multiple wireless carriers and LPWAN providers operate in a given area, the decision becomes more challenging. But for IoT connectivity in general, it will take years before clear winners are established.

Why Choose Digi XBee®?

Future Proof Footprint



Mesh Networking

zigbee

ZigBee is an open, global wireless standard designed for resilience and reliability communicating through noisy RF environments common in industrial applications.

DigiMesh®

DigiMesh is similar to ZigBee mesh networking, but unlike ZigBee, DigiMesh only has one node-type that can route data and are interchangeable.

THREAD

Thread is an open, global, IPv6-based, low-power mesh networking protocol that is simple to setup and deploy.

Point to Multi-point

802.15.4

802.15.4 is a standard which specifies the physical layer and media access control and is ideal for applications requiring low latency and predictable communication timing.

Wi Fi

802.11, or more commonly known as Wi-Fi, has a variety of sub-protocols represented by the suffix a/b/g/n/ac, each with varying degrees of bandwidth.

LTE Cellular Networking

LTE CAT1

LTE Cat 1 technology makes LTE viable now for M2M and IoT applications.

LTE CATM1

LTE Cat M1 is an IoT-centric flavor of LTE designed for sensor applications and devices requiring lower throughput.

LTE CATNB1

LTE Cat NB1, also called Narrowband-IOT, also supports lower bandwidth applications and addresses challenges of poor signal strength and range limitations.

IoT Device Security: Built-In, Not Bolt-On

The 10 Security Factors Every Device Designer Should Consider

The Rising Tide of Security Threats

Limited only by designers' imaginations, the Internet of Things (IoT) is changing how people live. From medical devices and fitness trackers to tank sensors, smart thermostats, intelligent streetlights, water monitors, and more, the IoT is in more places than ever.

However, by relying on wireless networks, those hundreds of millions of IoT devices present a greater "attack surface," making them tempting frontline targets for competitors, hackers, disgruntled employees, and other bad actors. Unfortunately, the tools and techniques we've applied to PC/smartphone platforms often don't work well in the IoT, for several reasons:

RESOURCE LIMITATIONS

Small-footprint IoT devices typically have far less battery power, processing speed and memory. They lack the power and sophistication required to support traditional security measures.

DATA COMPLACENCY

Many companies view the data in their IoT networks as mundane and having little intrinsic value outside the organization. But many breaches are motivated by other factors, such as competitive advantage, social status, or revenge. The data isn't the goal – the hack is.

AVAILABILITY OF TOOLS

The tools and expertise to analyze and modify embedded/IoT devices are widely available – even to hobbyists.

NO PHYSICAL ACCESS REQUIRED

One of the advantages of the IoT is that devices can be remotely configured/upgraded without the need for dispatching a truck. However, thanks to wireless connections, hackers don't need physical access to devices such as USB or other I/O ports.

INTERFACE DIFFERENCES

Embedded devices have no GUIs, and error messages can be as basic as a coded series of beeps or flashing lights. This is particularly true for security status and control functions allowing for security alarms to be overlooked.

HARDWIRED PORTS

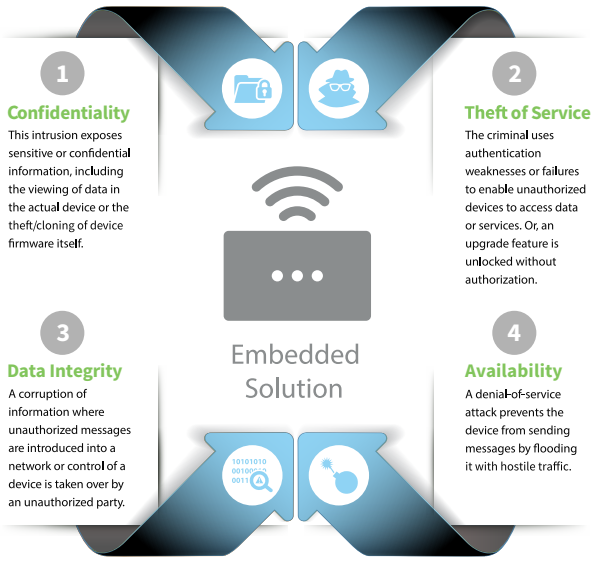
These provide unfortunate opportunities for compromise.

IoT solutions can't simply implement a strong password over a TLS connection – the most common approach for PC/Internet applications. IoT solutions need a different approach, and the effort required to identify and mitigate unique security risks in embedded systems is often underestimated, if not overlooked entirely.

Thanks to wireless connections, hackers don't need physical access to devices such as USB outlets or network ports.
But the risks of this rising tide of security threats are significant. Beyond reputational damage, competitive threats, eroding customer confidence, and safety challenges, regulators are paying increasing attention as well. For instance, security breaches that violate HIPAA regulations can lead to fines of $50,000 per violation. Credit card processors that fail to comply with the PCI DSS standard may be fined up to $100,000 per violation.

Distributed Denial of Service (DDoS) attacks are becoming more and more prevalent. These attacks may not necessarily be targeted at the average IoT edge device but a hijacking of a connected IoT edge device may be used to create a 'BotNet', a group of hijacked devices working together to work in unison to attack a central point on the IoT network or an external server/computer outside of the local network. Even if these attacks are not targeted at the local IoT network, they still pose multiple problems by preventing regular IoT work to take place or even simply draining the battery on a mobile IoT edge device creating maintenance cost for the administrators leaving them wondering why the battery didn't last longer.

Four Types Of Security Threats That Disrupt IoT Devices



Security is a Balance Between Economic Cost and Benefit

Given enough time, money and expertise any system can be hacked, so it is important to design a system to deter an attacker by making it uneconomic (i.e. the cost or effort of an attack far outweighs any benefit to an attacker).

Types of attacks can be classified in terms of investment, the type of attacker and equipment used.

These range from:

EXPENSIVE INVASIVE ATTACKS

(such as reverse engineering, or sophisticated micro-probing a chip) To lower cost:

PASSIVE SOFTWARE ATTACKS

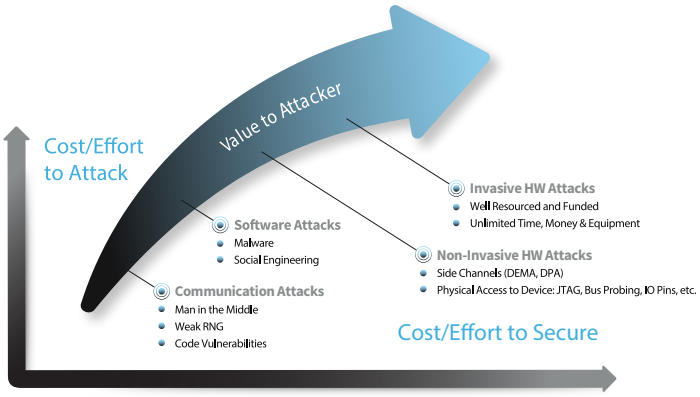
(exploiting unintentional security vulnerabilities in the code)

COMMUNICATION ATTACKS

(e.g. exploiting weaknesses in the internet protocols, crypto or key handling)

Security is always a balance between economic cost and benefit, dependent upon the value of assets on the one hand and the cost of security features on the other.

The success of the Internet of Things will depend on data and services being protected, and when the security balance is right, it can open up new opportunities and markets.



Hacks can be categorized by the cost and effort involved

The 10 Security Techniques Every IoT Designer Should Consider

For design engineers who are striving to enhance the security of their IoT devices, there are numerous options at hand. In the following pages, we describe 10 strategies that can have a direct impact on improving device security.

Method Notes	Complexity, Resources Needed	Notes
Packet Encryption	Low	Foundation for most embedded system security
Replay Protection	Low	Prevents resubmission of recorded messages
Message Authentication Code	Low	Prevents messages from being changed
Port Protection	Low	Secures ports that may be physically accessed by an attacker
Secure Bootloader	Moderate	Ensures only authorized firmware is allowed to run
Pre-Shared Keys	Low	Preferred for smaller systems
SSH	High	Generally on OS-based systems; can prevent malicious connections
Public Key Exchange	High	Generally on OS-based systems; can prevent malicious connections
TLS	High	Generally on OS-based systems; can prevent malicious connections
WPA2	High	Generally on OS-based systems; can prevent malicious connections

Packet Encryption

This is the "go-to" method for protecting data exchanges in IoT solutions with smaller embedded terminal devices. Most systems have the resources to implement basic encryption, such as FIPS-197/AES, which can protect messages from unauthorized viewing or malicious changes. This method is easy to implement and use, especially in conjunction with private keys

Message Replay Protection

In this approach, encrypted packets are enhanced with data fields that vary in a way known to the recipient (which could be as simple as a date stamp). The recipient enforces a rule that messages are only accepted once or in a sequence. This prevents recorded, but not necessarily decrypted, messages from being resubmitted at a later time to cause the original action, such as "open door." This method is also simple to implement and is often used when individual messages can cause state changes. This can also be part of an encryption mode that will use this information within a block cipher. Examples of this is the AES counter mode block cipher.

Message Authentication Code

In this method, we run a cipher or hash algorithm on the content of a data packet to create a short signature that accompanies the message packet. The recipient uses the same cipher or hash to confirm that the message has not changed. Message authentication provide explicit protection from tampering and enables some systems to safely use clear-text messages. For example, we can use this method for systems that transmit non-confidential data (e.g., air temperatures) that nonetheless must not be tampered with. This is another low-complexity method that is useful for many types of embedded systems.

Debug Port Protection

Hardware ports used for configuration, control, and analysis (e.g., JTAG ports and serial logging ports for firmware development and debugging) are also vulnerable and tempting targets for security attacks. To start, these ports can be protected with a different factory password per unit before further actions are allowed. Of course, the better move is to internally disable these ports in field-deployed units.

Secure Bootloader

Even for a development team with unrestricted access to required technical information, it can be daunting to correctly build and load firmware into a resource-limited embedded device, which makes it unlikely you'll experience a successful attack based on a malicious firmware modification. But the rapidly increasing sophistication of embedded-system attackers, combined with product requirements for easier field upgrades of device firmware, have created a risk that must not be overlooked. One best practice is to configure the device to check for a HMAC signature in the firmware image during startup to ensure it is authorized to run on the product. The image may also be encrypted for further protection. Secure bootloader solutions demand careful management of keys and support for debugging

Pre-Shared Keys

Secure IoT communications requires access to compatible keys. The use of pre-shared keys (PSKs) minimizes the demands on the resourceconstrained device. Keys can be transferred through an independent, secure channel and then manually entered into the terminal device. While the overall system to share the keys may have some complexity, the demands on the actual terminal device are minimal. When allowed by the application.

Secure Shell

The Secure Shell (SSH) protocol protects ports used for debug and configuration operations. SSH implements a standard protocol to encrypt console connections (e.g., Linux shell access) to prevent unauthorized viewing or operations. This substantially extends protection beyond a simple debug port password. This can often be too complex to implement on smaller embedded systems. But it's quite straightforward and feasible on larger OS-based systems because the necessary resources are typically present.

Public Key Exchange

Sometimes, pre-shared keys aren't a viable option, such as when the terminal device can't have the key configured at the factory, the necessary field-installation expertise is unavailable, or there is no keydistribution system available. In these instances, public-key exchange (PKE) is an ideal solution – thought it adds considerable complexity. With PKE, one of several methods is used to select and combine two large numbers, and then send one number and the resulting combination to the recipient. The recipient derives a session key that is known to the sender and this establishes a channel to encrypt/decrypt traffic. While technically

complex and potentially too resource-intensive for an embedded system, PKE can actually simplify system deployment and operation because the sender and receiver don't need prior knowledge of one another and manual configurations can be minimized. This approach is often used on Linux-based systems that communicate over IP, because the necessary resources for PKE are often already present.

Transport Layer Security

Transport Layer Security (TLS) is the current standard for the widely implemented Secure Sockets Layer (SSL) protocol. It provides a standard framework for PKE and encryption to secure traffic between devices. However, for resource-limited embedded systems, the memory and processing requirements for the TCP/IP stack may be impossible to support. That's why TLS is often used on larger embedded systems (e.g., those running Linux) where communication occurs in IP sessions such as TCP. Even smaller embedded systems may have the resources to support TLS, but this requires careful evaluation.

Wi-Fi Protected Access (WPA2)

When an embedded terminal device uses Wi-Fi (802.11) for communication, the WPA2 suite of standards can secure the communication channel. This widely deployed protocol allows interoperability of systems from different design authorities. However, it is generally beyond the reach of smaller embedded systems unless specialized Wi-Fi-dedicated coprocessors are present. For certain applications on larger OS-based (e.g., Linux) systems, WPA2 can be an attractive option.

Digi TrustFence™ Featuring the Digi ConnectCore® 6UL and NXP i.MX 6 and i.MX6 UL® Applications Processor

To help designers and builders effectively respond to the IoT security mandate, Digi offers Digi TrustFence™, a fully integrated, tested, and complete Linux device security framework for the Digi ConnectCore® 6UL system-on-module solutions featuring the NXP i.MX6 and i.MX6 UL applications processors.

By leveraging multiple H/W security components of the i.MX series, Digi TrustFence simplifies efforts to build secure, trusted, and reliable connected products; speeds your time to market; and lets you focus on your core competency. You gain immediate access to critical features such as secure connections, authenticated boot, encrypted data storage, access-controlled ports, secure software updates, and seamless integration of the dedicated on-module Secure Element (SE).

Build connected, embedded products on Digi ConnectCore® 6UL for the NXP i.MX6UL to capitalize on out-ofthe-box, integrated security with Digi TrustFence. The result: you can protect your brand's reputation. You focus on delivering products that take advantage of the benefits of connectivity. Digi TrustFence handles the security for you. Digi TrustFence offers:

SECURE BOOT

TrustFence ensures only signed software images run on your device.

ENCRYPTED STORAGE

Local file system encryption keeps your internal data safe.

PROTECTED PORTS

Protected, access-controlled internal and external ports prevent unwanted "back doors."

DEVICE IDENTITY

Root of trust, certificate management, and secure key storage protect the identity of your device.

DEVICE INTEGRITY

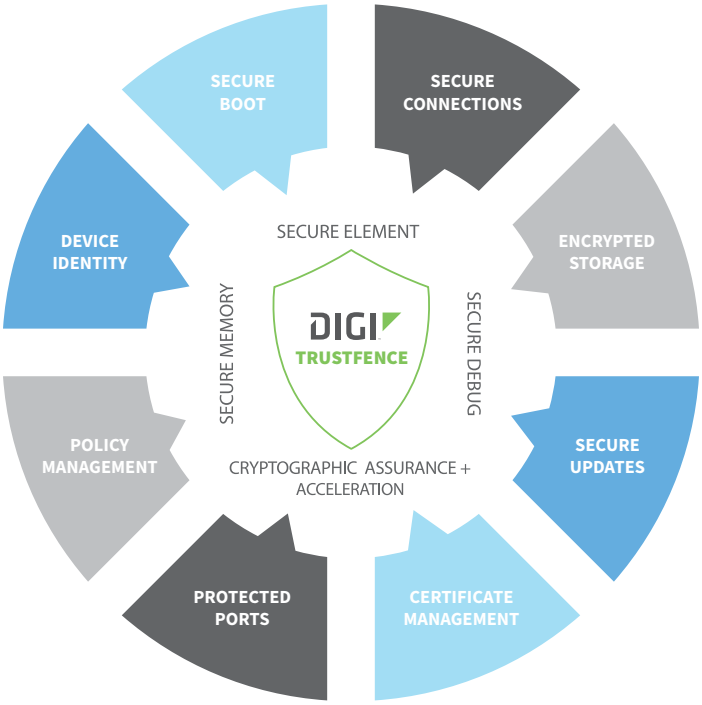
Tamper-proofing and device-integrity monitoring with low-power support protect against physical intrusion.

SECURE CONNECTIONS

Enterprise-level data encryption provides privacy for wired and wireless network connections.

FUTURE-PROOFING

Digi platforms are built for longevity and long-life product lifecycles with availability for years to come.



Summary

Security threats to embedded devices in IoT solutions are increasingly common, as attacks have become easier to carry out. These can include confidentiality breaches, service theft, data integrity, and service availability. IoT systems have unique security requirements and challenges, mostly due to resource limitations. Six core methods (packet encryption, message replay protection, message authentication code, debug port protection, secure bootloaders and pre-shared keys) are typically compatible with the unique needs of M2M terminal devices. Increasingly, four other methods (SSH, PKE, TLS and WPA2) can be used with smaller M2M terminal devices as available system resources expand.