McKinsey&Company

The future of connectivity: Enabling the Internet of Things

High Tech December 2017

Daniel Alsén
Mark Patel
Jason Shangkuan

The future of connectivity: Enabling the Internet of Things

With new connectivity technologies unlocking opportunities along the IoT value chain, companies must create detailed plans to harness their potential.

The Internet of Things (IoT)—the network of connected "smart" devices that communicate seamlessly over the Internet—is transforming how we live and work. At farms, wireless IoT sensors can transmit information about soil moisture and nutrients to agricultural experts across the country. IoT alarm systems, equipped with batteries that last for years, provide homeowners with long-term protection. Wearable fitness devices—for both people and pets—can monitor activity levels and provide feedback on heart rate and respiration. Although these applications serve different purposes, they all share one characteristic: dependence on strong connectivity.

IoT stakeholders seeking connectivity solutions include radio and chipset makers, platform vendors, device manufacturers, and companies in various industries that purchase IoT-enabled products, either for their own use or for sale to the public. These companies can now choose from more than 30 different connectivity options with different bandwidth, range, cost, reliability, and network-management features. This wide variety, combined with constantly evolving technology requirements, creates a quandary. If stakeholders bet on one connectivity option and another becomes dominant, their IoT devices, applications, and solutions could quickly become obsolete. If they hesitate to see how the connectivity landscape evolves, they could fall behind more aggressive competitors.

Cellular 5G networks—now being refined—might eventually become a universal solution for IoT connectivity. Although some global telecommunications networks and industrial applications now use 5G, this technology will not be widely available for at least five years, because of high development and deployment costs. With annual economic benefits related to the Internet of Things expected to reach $3.9 trillion to $11.1 trillion by 2025, companies cannot afford to defer their IoT investment until 5G arrives.

To help business leaders identify the connectivity solutions that best meet their current needs, we analyzed 13 sectors, including automotive, manufacturing, construction, and consumer, where IoT applications are common.[1] In each sector, we focused on connectivity requirements for likely use cases—in other words, the tasks or activities that may be most amenable to IoT solutions. We then identified the most relevant connectivity solutions for each one. In addition, we examined business factors that may influence how the connectivity landscape evolves, as well as the elements of a strong connectivity strategy.

A vast assortment of connectivity offerings

When contemplating their options for IoT connectivity, companies must choose among solutions from four categories: unlicensed; low power, wide area (LPWA); cellular; and extraterrestrial. Companies may find it difficult to choose among these technologies because each IoT use case presents unique requirements for bandwidth, range, and other connectivity features. LPWA options are also difficult to evaluate because they are still in the early stages of deployment, and their full potential and drawbacks will not become obvious until they are implemented on a greater scale.

Unlicensed connectivity solutions

These solutions are not exclusively licensed to a particular company, allowing the public to access them on any IoT device that uses this technology. Unlicensed solutions are relatively inexpensive and allow businesses to manage their

own networks, rather than relying on a mobile operator to do so. On the downside, unlicensed technologies are vulnerable to interference from electrical or environmental obstacles, such as a large number of buildings that may interfere with signal transmission. They also face difficulty providing connectivity over long distances (more than 100 meters). Companies have various options for unlicensed connectivity, all of which have distinct features. For instance, Wi-Fi—perhaps the most well-known unlicensed option—has bandwidth of up to one gigabyte per second. That is higher than the bandwith for Bluetooth, Zigbee, and Z-Wave.

Low-power, wide-area connectivity

LPWA technologies are relatively new. As their name implies, they have two characteristics:

- *Low power.* They can allow devices to operate for years, assuming that they collect and analyze data hourly and factoring in the typical impact of battery self-discharge and degradation.

- *Wide area.* These technologies deliver at least 500 meters of signal range from the gateway device to the end point. Coverage is lowest in challenging deployment environments, such as urban or underground locations.

In addition to providing long battery life and extensive range, LPWA technologies are reliable and associated with low costs. No other technology offers these four characteristics in combination. For instance, unlicensed technologies are unreliable, while cellular technologies are expensive and cannot provide power for multiple years on a single charge. Thus, LPWA fills an unmet need in IoT connectivity.

Only 20 percent of the global population is now covered by LPWA networks, so they cannot become the default solution within the next five years, but their availability is growing rapidly. By 2022, we expect that most IoT applications will use LPWA networks, which will make connectivity choices less confusing. (5G will still not be widely available at that point).

Some companies have developed proprietary LPWA technologies, including Ingenu (formerly On-Ramp Wireless), Link Labs, LoRa, Sigfox, and Weightless. The 3rd Generation Partnership Project, an organization that develops connectivity guidelines, is also working to standardize several nonproprietary technologies that are supported by many or all mobile-equipment, chipset, and module manufacturers. These include narrowband IoT (NB-IoT), which is the newest LPWA option and was specifically developed for the Internet of Things. Other nonproprietary technologies include LTE machine-type communications (user equipment categories 1, 0, and M), extended-coverage GSM (EC-GSM), and low-throughput networks.

Each LPWA technology has different advantages and implementation requirements. For instance, Sigfox manages its own networks, while LoRa is supported by more than 400 partners. NB-IoT relies on existing cellular infrastructure for the small pilots in which it is being tested. This will also be the case when NB-IoT becomes more widely available and is applied in larger-scale programs. Since the LPWA market is still in its early stages, it is difficult to predict which LPWA solution will emerge as the winner.

Cellular connectivity

Current 4G LTE technology offers high bandwidth of up to 100 megabytes per second and a large range of more than ten kilometers. Reliability and availability are also good. On the downside, 4G LTE technology is associated with high costs—several dollars or more for a module compared to less than a dollar for Wi-Fi. Cellular connectivity also has high power-consumption requirements, making it less than ideal for IoT applications, where battery life should extend over multiple years.

Companies can deploy 4G LTE connectivity over public or private networks. Public networks use the same connectivity infrastructure as mobile

phones, while private networks segregate devices into a separate system by sublicensing unused frequencies from mobile operators with enterprise-owned infrastructure. Some companies in our analysis managed private networks, but most lacked the necessary capabilities and budget. This will also be the case within the wider population.

Extraterrestrial connectivity

This connectivity option includes satellite and other microwave technologies. IoT stakeholders generally use it only when cellular and fiber options are not feasible, since it has the highest costs. For instance, organizations within national defense may use satellite connectivity for unmanned drones. Extraterrestrial options have low-to-medium bandwidth, high range, and medium-to-high reliability and availability. Only a few industries rely on extraterrestrial connectivity for IoT apps.

Exhibit 1 summarizes the different categories of connectivity solutions.

Connectivity requirements across industries

While no connectivity solution is perfect, we were able to determine the most appropriate options for each industry by identifying the likely use cases in each sector. Many of these involved cost reduction and productivity improvement. For instance, companies in many industries value IoT solutions that reduce machine downtime by providing predictive maintenance, as well as those that give them better visibility into the supply chain and eliminate bottlenecks. There is not yet an IoT-based "killer application" for these services, or any other task, but one could emerge over the next few years as connectivity technology advances. That could increase both the volume and value of IoT.

Our research showed that connectivity requirements often varied by industry, even when the potential use cases were identical (Exhibit 2). For instance, predictive maintenance and operations optimization are potential IoT use cases for manufacturing, mining, construction, and oil and gas. Range and reliability requirements varied by industry, however, as did the willingness and ability to manage networks.

After identifying the likely use cases and associated requirements, we determined what connectivity solutions are likely to gain traction in each industry over the next five years (Exhibit 3). We believe that many companies will switch from unlicensed technologies to LPWA as it becomes more widely available, because it better meets their connectivity requirements. Consider mining. One company in this industry had to run cables far below the earth's surface and install frequent access points to deliver Wi-Fi connectivity at one of its sites. (It could not use other connectivity technologies because cellular and extraterrestrial solutions cannot transmit signals so far below the earth's surface.) LPWA can penetrate walls and other barriers more easily, and it may become the company's preferred connectivity solution once it becomes commercially available in its area. Companies in many other industries, including agriculture and manufacturing, may also shift from unlicensed technologies to LPWA. In fact, we could see a situation in which IoT grows in tandem with LPWA, since improved connectivity will increase both the number of IoT devices in use and the locations where they are used.

Despite LPWA's growing popularity, cellular options will still enable connectivity for use cases in numerous industries. The highest cellular demand will involve public LTE networks, since private ones are costly to build and maintain.

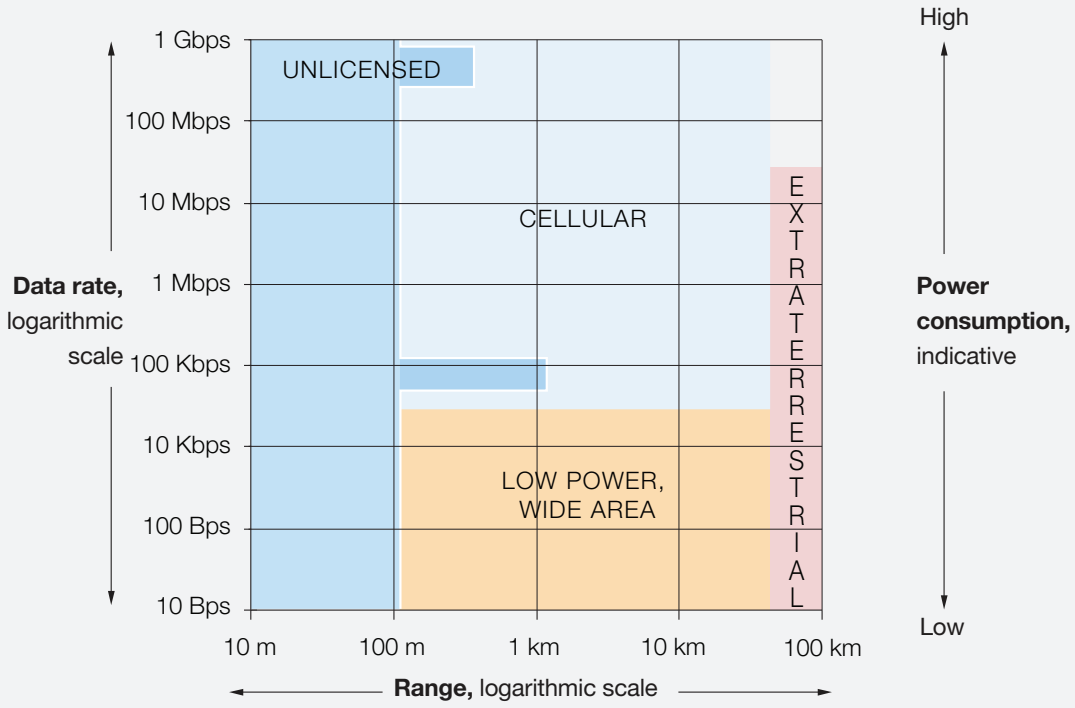
Satellite and other extraterrestrial communication solutions will continue to play a niche role, providing connectivity only in situations where cellular or fiber technologies are not feasible.

Business factors will help determine which connectivity solutions gain the most traction

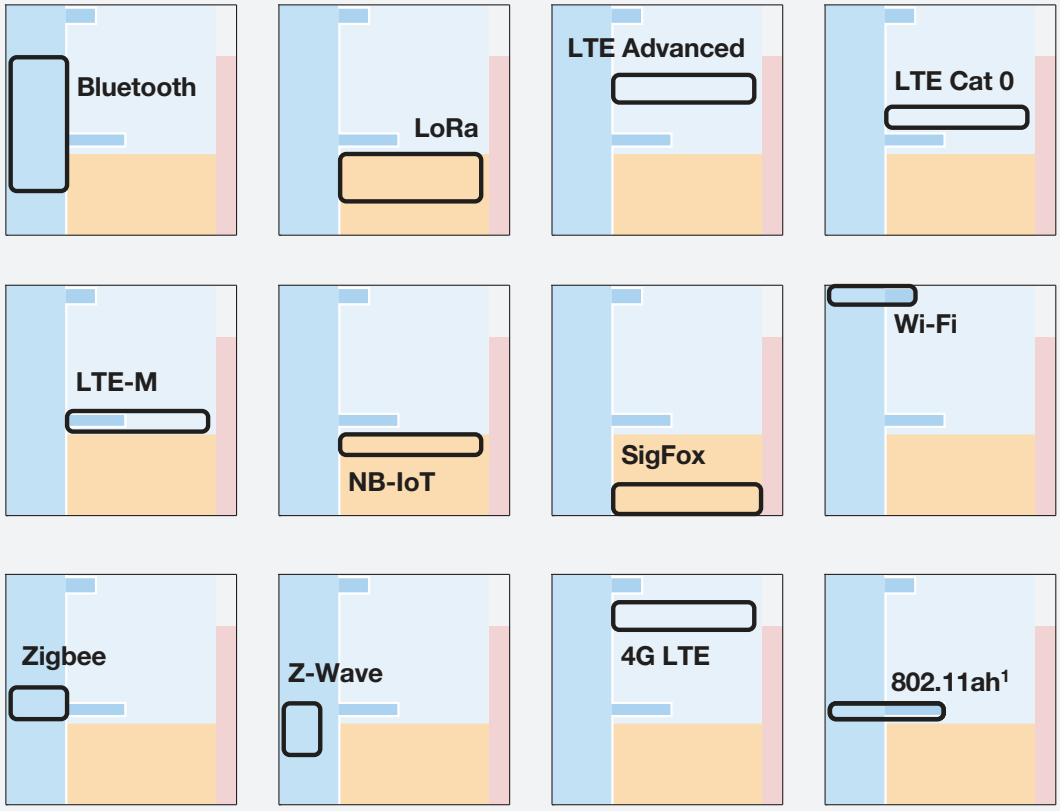
Our analysis suggests that technology advances will not be the only force that determines which connectivity solutions become dominant. In fact, the following business factors—including those

Exhibit 1

The Internet of Things connectivity solutions fall into four categories, with significant overlap in specifications.



Technology segments



[1] 802.11ah is a new low-power Wi-Fi standard.

Exhibit 2

Connectivity requirements vary by sector.

Sector	Potential use cases	Bandwidth	Range	Reliability	Willingness and ability to manage a network
Automotive	Over-the-air updates, predictive maintenance	Primarily low, high for entertainment content	Medium–long	High	Low
Manufacturing	Operations optimization, predictive maintenance	Low	Short–medium	High	Low
Defense	Asset management, remote monitoring	Medium	Long	High	Medium
Agriculture	Yield optimization, asset management	Low	Short	High	Low
Mining	Predictive maintenance, operations	Low	Medium–long	High	Low–medium
Construction	Predictive maintenance, operations optimization	Low	Short	Medium	Low
Oil and gas	Predictive maintenance, production optimization	Low	Medium–long	High	Low–medium
Insurance	Patient monitoring, asset management	Low	Long	Medium	Low
Healthcare	Remote monitoring, safety	Low	Short–medium	Medium	Low
Cities	Traffic control, security	Low	Medium–long	High	Low–medium
Utilities	Asset management, remote monitoring, energy management	Low	Long	High	Low
Travel, transport, and logistics	Predictive maintenance, logistics optimization, automation	Low	Long	High	Low
Consumer	Productivity optimization, personalization, energy monitoring	Medium–high	Short	Medium	Low

Source: Expert interviews; publicly available information.

Exhibit 3

Each sector will have different Internet of Things connectivity needs for its top use cases over the next five years.

● High ● Medium ● Low

Sector	Noncellular short range	LPWA[1]	Cellular and other long range
Automotive	● Wi-Fi/Bluetooth for in-car connectivity	●	● Deliver content to vehicle
Manufacturing	●	● Connectivity within factories	●
Defense	●	●	● Satellite for connectivity in remote locations
Agriculture	●	● Sensor monitoring in fields	● Satellite if there's no coverage
Mining	●	● Sensor monitoring and machine control	● Fiber to reach mines
Construction	● Site connectivity, geofencing	●	●
Oil and gas	●	● Sensor monitoring	● Private cellular network possible
Insurance	●	●	● Public LTE is sufficient and deployed for use cases
Healthcare	● Deployed today and can be used to locate positions	●	●
Cities	●	● Sensor connection and device control	● Private LTE deployed only in select cities
Utilities	●	● Meter connections	● Select utilities utilizing private networks
Travel, transport, and logistics	● Cargo tracking	● Cargo tracking	● Private network on ships
Consumer	● Consumer devices	●	● Consumer devices

[1] Low power, wide area.

over which IoT stakeholders have little control—may play an equally important role.

Changing business models of industrial-device manufacturers

Most device manufacturers that create industrial IoT solutions originally followed a pay-per-unit business model in which they charged a single fee for each device sold and made most of their income from long-term maintenance contracts. This model inadvertently created a conflict of interest between customers, who wanted their devices to work uninterrupted, and manufacturers, who profited from servicing faulty devices. But this conflict may soon cease. Manufacturers are now transitioning to a device-as-a-service (DaaS) model in which they sell customers a subscription to their products. The subscription covers both the initial device purchase and later maintenance costs, which allows manufacturers to make money even if the products do not require service. In fact, they have an incentive to keep their devices running, since service costs could reduce their revenues. To facilitate the DaaS model, manufacturers want connectivity solutions that allow them to connect, monitor, and perform updates remotely. LPWA solutions best meet their needs, since unlicensed technologies such as Wi-Fi do not work well in "noisy" environments with a lot of electrical and environmental interference, including those in manufacturing plants.

Associated costs

Although IoT connectivity chipsets may be relatively inexpensive, companies may face additional costs to enable the solutions, including those for modules, retrofitting, and infrastructure. For instance, companies may pay less than a dollar for a Wi-Fi module, but they might need to purchase multiple access points, install wiring, and undertake system integration to enable connectivity—all costly endeavors. If LPWA is an option in such circumstances, companies may favor it because their associated costs will be lower.

Even connectivity technologies in the same category can have different associated costs, and this may determine what solution a company chooses. Consider the various LPWA options. While companies must build communication towers and purchase modules to deploy Sigfox connectivity, NB-IoT requires only a module purchase, since it can use existing cellular infrastructure.

Supporting ecosystems

Some IoT connectivity solutions are easier to deploy because they have a strong ecosystem that supports their use. For example, LoRa is an attractive LPWA option because there are already hundreds of members in the LoRA Alliance, and the numbers are growing.

Commercial readiness

Some emerging connectivity solutions remain untested on a large scale. Consider NB-IoT, a new LPWA technology that can be deployed through existing cellular infrastructure and has very low power requirements. This technology is not widely available commercially, although it is being tested in pilots. It may thus be at a disadvantage against other LPWA solutions such as LoRa and Sigfox that have been on the market for several years and are now part of a growing ecosystem.

The elements of a strong near-term connectivity strategy

As companies design their IoT strategy, they must be open to change, adapting their game plan to suit new connectivity standards and customer preferences for simplicity. Likewise, they should be prepared to investigate new business models, since advances in IoT connectivity may open some surprising opportunities.

Betting on multiple IoT connectivity standards

Multiple groups are attempting to establish connectivity standards for IoT, including the Industrial Internet Consortium and individual companies that sponsor open-standard initiatives. Such groups have successfully set standards for connectivity in other technological spheres, but their efforts often move slowly, which can delay

growth. Some consortia of companies and single strong players are also attempting to set de facto standards before standard-setting bodies can align and define one.

Experience with other technologies suggests that the IoT connectivity standards that are most likely to become dominant will provide clear value for all stakeholders, such as reduced costs or technical advantages. They will also have the support of all players within one or more strong ecosystems that cover a large number of products. Finally, the preferred standards will allow for rapid rollout and scale-up, as well as easy adoption—something that is more likely to occur if they have the support of a partnership or multiple groups.

Until IoT stakeholders have more certainty about standards, they must remain flexible. For instance, Ericsson and Huawei are introducing different versions of NB-IoT, but it is unclear which one will become more popular. Therefore, platform vendors that want to enable out-of-the-box device connectivity for IoT offerings may want to make their products compatible with both versions. While this strategy ensures that devices can communicate, it also creates additional complexity and could potentially increase product costs.

Focusing on simplicity

We have talented engineers and leading-edge technology companies to thank for the wealth of connectivity technologies now available or in development. The most sophisticated and complex solutions reflect well on the technological prowess of their creators, and they may be best suited for many products. Within IoT, however, companies must focus on use cases, rather than technological sophistication, when selecting connectivity solutions. That means they should be satisfied with connectivity solutions that satisfy the basic requirements for device functionality, even if more advanced options are available, if they can procure them at a lower cost.

Exploring new business models

One of the greatest needs in IoT is ubiquitous connectivity—the ability to connect to any device, regardless of location. Mobile virtual-network operators (MVNOs) are the only players who currently provide this capability. These players lease wireless capacity from other companies that own cellular networks in various locations—ideally, in every major country. They then resell their capacity to IoT stakeholders, such as device manufacturers. MVNOs will not necessarily emerge as the leaders in IoT connectivity, however, because they do not bridge the gap between companies that must use the same application. For instance, if a shipping company is off-loading boxes to a truck, it needs to hand over its data to the trucking company and then to the factory where the boxes will eventually arrive. Companies that develop connectivity solutions to bridge these gaps could emerge as IoT leaders.

IoT is complex by nature, with devices and apps requiring the cooperation of multiple vendors. Likewise, providing end-to-end IoT connectivity can be complicated because it requires multiple vendors and companies may find that they need different solutions for their potential use cases. Winning companies will try to sort through the confusion and establish connectivity solutions now, even though uncertainty abounds, so they can emerge as leaders in IoT.

[1] Our research included both data analysis and expert interviews with operators, connectivity-technology providers, and industry experts. The sectors are automotive; manufacturing; defense; agriculture; mining; construction; oil and gas; insurance; healthcare; cities; utilities; travel, transport, and logistics; and consumer.

Daniel Alsén is a partner in McKinsey's Stockholm office, **Mark Patel** is a partner in the San Francisco office, and **Jason Shangkuan** is a consultant in the Dallas office.

Contact for distribution: Jenna Gravino
Phone: +1 727 561 5805
Email: Jenna_Gravino@McKinsey.com

November 2017
Designed by Global Editorial Services