Connectivity technologies for IoT

How enterprises can select the most suitable technology for connecting their IoT applications

Northstream
Full Report
October 2016
Selecting the most suitable connectivity technology is one of the critical decisions that enterprises need to make in their IoT launch strategy as connectivity is an important component in an end-to-end IoT solution. This decision can impact the success of the service as a poor choice can result in inferior performance or higher cost in the short-term, and in the long-term it can hinder scalability or necessitate an expensive swap if the technology is not sufficiently future proof.

There are a range of technologies available for IoT such as traditional cellular (2G/3G/4G), Low Power Wide Area, Wi-Fi, Bluetooth and more. Every use case has specific needs, which translate into certain technology considerations that determine the choice of most suitable connectivity technology. Our analysis identifies and groups these technology considerations into three categories – technical, commercial and ecosystem related, thus providing a structured approach enterprises can use to analyze their requirements:

- Technical considerations – coverage, energy efficiency, data rate, other features relevant to specific applications (bidirectional communication, mobility, localization);
- Commercial considerations – quality of service, cost, security, scalability;
- Ecosystem considerations – future proofness, global reach and interoperability.

No single technology or solution is ideally suited to serve all potential IoT use cases and certain technologies will coexist alongside, as complementing rather than competing standards. Currently, there are also various actors within these technologies that are aiming to establish their market dominance and ecosystem. The current fragmentation is not sustainable for the industry in the long run and leaders will emerge.

According to our analysis, for IoT deployments in remote/wide areas, LoRa and NB-IoT are good complements and together will address a large share of this market. LoRa’s dynamic open ecosystem is ideal for private networks with customized deployment, while NB-IoT is backed by major mobile operators offering standardized connectivity with global reach. Other proprietary technologies, like Sigfox, may address certain niche segments but their future proofness is to be time tested. For applications requiring high data rate, the most suitable technology options are either LTE, Wi-Fi or BLE, depending on the scope of the IoT deployments. For local short range applications, the choice of connectivity technology is less obvious and often the interfaces and implementation of platform and application layers become more crucial.

Finally, this paper provides some case studies and discusses the needs of various application areas, such as automotive, smart cities, industrial manufacturing, in order to illustrate which technologies can be best suited to serve those needs.
Internet of Things (IoT) is transforming many industries and will create value for both businesses and their customers. For enterprises new to IoT, an important aspect of getting started is selecting the most suitable connectivity technology. This paper aims to provide a structured approach enterprises can use to analyze their requirements, deliver insights about the landscape of connectivity technologies available, as well as illustrate how different technologies can be best suited to serve the needs of specific application areas and use cases.

1.1 CONNECTIVITY TECHNOLOGY IN THE CONTEXT OF IOT LAUNCH STRATEGY

Selecting the most suitable connectivity technology is one of a number of strategic decisions with long-term implications that enterprises need to make when deploying IoT in their business. Every process of launching IoT starts with identifying the opportunity (idea generation). The nature of the opportunity can vary, from deciding to make an existing product or asset connected to launching a completely new connected product. One of the key strategic steps is to define the vision and objectives that the enterprise is aiming to achieve with IoT both short-term and long-term – these can generally be to increase revenues by enabling new business models (from product to service) and services to customers; or decrease costs in internal production processes and supply chain. The main question to ask is how the connected product and the data generated are going to be used and deliver value to the enterprise and its customers.

After answering these key questions and analyzing both the strategic and financial impact, enterprises can proceed to identifying technology requirements and selecting the most suitable technologies and vendors. As illustrated in Figure 1, deploying IoT entails securing an end-to-end technology solution that includes hardware (device, components), connectivity technology, platform and applications (software), often brought together with the help of a system integrator/technology consultancy.

Each of these components is important and carries its own requirements. In this paper we focus on providing insights and analysis regarding how enterprises can select the most suitable connectivity technology among several alternatives such as traditional cellular (2G/3G/4G), a range of Low Power Wide Area (LPWA) options, Wi-Fi and more.

---

1 IoT is hereby used as a term that includes all connected devices, both connected directly to the internet but also deployed in a closed network.
Every use case has specific characteristics and needs that translate into certain technology requirements – technical, commercial and ecosystem related. We have identified and described these major technology considerations in the next section of this paper. For example, enterprises may have products which are:

- Simple sensors that deliver small amounts of non-sensitive data with low requirements for security, but need for low cost to deploy and manage a large number of devices in close proximity;

- (Part of) sophisticated machines that need to report data and be monitored, upgraded and maintained remotely, with the need for high level of security and to be future-proof for 5-10 years, while potentially operating in places hard to access.

For some use cases the choice of technology can be very straightforward, while for others the enterprise may need to choose among a number of technologies that can in theory satisfy the needs, but likely with different trade-offs.

1.2 THE IMPORTANCE OF CHOOSING THE RIGHT CONNECTIVITY TECHNOLOGY

Selecting the right connectivity technology (and vendor) can impact the outcome both in the short and long-term and therefore both perspectives should be considered. In the short-term, a poor choice can result in inferior performance or higher cost than budgeted; in the long run it can hinder scalability as device number increases or necessitate an expensive swap if the technology does not prove sufficiently futureproof to support the long lifecycles of some products.

There are currently a range of technologies available for IoT based on both licensed and unlicensed spectrum, and respectively actors that are aiming to build their market dominance and ecosystem. The current fragmentation is not viable for the industry in the long-run and leaders will emerge.

Some enterprises new to IoT may therefore face the question whether to launch as soon as possible or wait until standards have become more established – a choice between being first to market or best to market. The answer depends on the specific use case requirements and competitive environment. In any case, a phased approach is recommended, where customers start small and scale gradually.

Although certain connectivity technologies or players will emerge as leaders in their category, we believe that no single technology or solution is ideally suited to serve all potential IoT use cases. Certain technologies (and vendors) will coexist alongside, as complementing rather than competing standards.
Traditionally, the IoT landscape or rather the machine-to-machine (M2M) communication has been dominated by radio technologies such as ZigBee, Bluetooth and Wi-Fi for short range local area network, and traditional cellular networks such as GSM (2G), UMTS (3G), and LTE (4G) for wide area network. Many of these technologies, especially Wi-Fi and 2G/3G/4G were originally designed for consumer voice and data services.

A number of new radio technologies have emerged recently to connect things that were too expensive or too remote to be connected previously. These newcomers, characterized by their low power consumption and wide coverage are generally known as Low Power Wide Area (LPWA) technologies. We divide them into two main categories. The first one is proprietary LPWA such as Sigfox, LoRa, Ingenu, which operate on unlicensed spectrum, and are typically deployed by non-telecom actors but can be also deployed by telecom operators. The second one is cellular LPWA such as NB-IoT, LTE-CatM1, EC-GSM, which operate on licensed spectrum. The latter are specifically developed to provide a cellular option that addresses the needs of IoT and are introduced in the latest cellular standard to be deployed in cellular networks as early as 2017.

To choose the right option for a specific IoT application when facing such a diverse selection of technologies, requires understanding of technology from many different aspects. As illustrated in Figure 2, our framework divides the criteria into three main dimensions: technical, commercial and ecosystem related considerations. In the following section we will describe the relevance of these considerations.
2.1 CONSIDERATIONS IN SELECTING IOT CONNECTIVITY TECHNOLOGY

TECHNICAL CONSIDERATIONS

The three main technical requirements for any enterprise looking into IoT connectivity technology are coverage, energy efficiency and data rate. No single technology can excel in all these aspects, as they are conflicting objectives that every radio technology has to make tradeoffs with.

Coverage

All IoT applications need good coverage to connect the devices, but some need to cover only certain indoor areas while others require extensive coverage in rural or remote regions. A technology with long range is better suited to connect devices scattered in a wide area.

Traditional cellular technology, such as 3G or 4G, is a typical example of wide area solution with excellent coverage in most urban areas. LPWA technologies further improve the connectivity range by employing more robust coding schemes, which makes them ideal for reaching remote areas and penetrating deep indoors. Short range technologies, such as Wi-Fi and ZigBee, are suitable for connecting many devices deployed in close vicinity.

Energy efficiency

The energy efficiency of a connectivity technology has a significant impact on the lifetime or the maintenance cycle of IoT devices relying on battery or energy harvesting and is dependent on range, topology and complexity of the connectivity technology. The overall energy consumption of the device also depends on the usage of the application, such as the frequency and duration of message transmission.

Short range technologies like ZigBee rely on mesh topology to forward messages from one device to another over multiple hops. That way ZigBee can extend its coverage but may deplete batteries more quickly as an individual device must constantly listen and be ready to relay messages. Wide area technologies such as 2G, rely instead on star topology and keep most of the intelligence and complexity at the base station where power supply is not a limiting factor. LPWA technologies, such as NB-IoT, further reduce the energy consumption by stripping down the signaling protocol and reducing the amount of overhead to the bare minimum, thus allowing longer battery life.

Data rate

Data rate requirement for IoT applications varies from hundreds of bit per second (bps) for metering to several megabits per second (Mbps) for video surveillance.

Wi-Fi and cellular networks have used large bandwidth and complex waveforms with adaptive modulation rate to support high data rate. But they either consume more power or have a short range. In contrast, most LPWA technologies have much lower data rate and lower energy consumption as they employ more robust modulation scheme and run on commodity-priced micro-controllers with limited bandwidth.

As illustrated in Figure 3, traditional cellular technology emphasizes on data rate and range with complex designs optimized for mass consumer voice and data service; short range technologies like Bluetooth Low Energy (BLE) and ZigBee focus on data rate and battery life at the expense of connection range; LPWA technologies, including NB-IoT, sacrifice data rate for superior battery life and coverage.

Other technical features

In addition to the main technical considerations discussed above, there are other technical features that can be highly relevant for certain applications.

Bidirectional communication – for some applications it is sufficient to have only unidirectional communication (uplink only) for the end device to report data to an access point or a gateway. A bidirectional link, however, is necessary for the end device to receive data from the access point. This can improve the reliability of data transfers through handshaking and security through authentication exchanges. Most of the technologies discussed here support bidirectional communication but some such as Sigfox in our view have inadequate downlink bandwidth to support features like over-the-air-software updates.
**Mobility** – in many IoT applications, a device will be installed at a fixed location and paired to a single access point for the entire lifetime, but other applications may require the device to be operational as it moves through the coverage of different access points. While most of the technologies support device relocation to different access points, the relocation process can be as seamless as in the cellular network or occur only at scheduled intervals.

**Localization** – device location is often valuable information. But GPS tracking is not always feasible due to its limited indoor coverage and the extra cost and complexity. Therefore, native support for localization is a desirable feature. Most wide area technologies can use triangulation to determine the device location but the accuracy is rather limited for technologies with narrow channel bandwidth and situations where the device is static without direct signal path. Wi-Fi and Bluetooth are constantly improving their localization capability as the algorithm is getting more sophisticated.

**COMMERCIAL CONSIDERATIONS**

Understanding the technical requirements is only the first step in selecting the most suitable IoT connectivity technology. Depending on the IoT business model, tradeoffs often must be made among quality of service, cost and scalability, which impact the commercial aspect of the enterprise’s product or service.

**Quality of Service (QoS)**

The QoS requirement can vary significantly for different IoT applications, ranging from delay-tolerant metering applications to mission-critical remote control systems that require both high reliability and low latency. While there are connectivity suppliers for almost every technology who can provide operational support with certain degrees of QoS assurance, typically solutions that are enabled by licensed spectrum can provide higher degrees of QoS. In cellular networks, SLAs are commonly used as the tool by major actors to guarantee certain levels of quality for customers. On the other hand, technologies operating in unlicensed spectrum, such as LoRa and Wi-Fi, are generally designed on a best effort basis with limited QoS assurance as they are subject to potential interferences from other uncoordinated technologies and networks.

**Security**

With respect to security for IoT applications, better security in connectivity typically requires more processing power for data encryption/decryption and identification/authentication. This processing comes along with yet another concern that is the size of overhead data associated with IoT information. Many proprietary LPWA technologies provide only rudimentary security as they are limited by the simplicity of device and protocol.

Cellular networks rely on Subscriber Identify Modules (SIM) as the basis for the authentication, security, and privacy mechanisms. Wi-Fi and Bluetooth Low Energy (BLE) also have employed advanced encryption mechanisms.

**Cost**

The cost for IoT connectivity is comprised of the connectivity module cost and the connection cost.

The connectivity module is one of the main components of an IoT device, as illustrated in Figure 4. The connectivity module cost is directly proportional to the complexity of the technology, ranging from $30-50 LTE modules with expensive hardware and IP royalties to simple sub-$5 LPWA modules. It is expected that the price of the latter has potential for further reduction as the deployment volume increases.

![Figure 4: Main cost components of an IoT device](image)

The connection cost can be the subscription cost if connectivity is provided by a network operator, or the network cost if the enterprise owns its private network. In either case, the connection cost is ultimately driven by the cost for deploying, operating and maintaining the IoT network, and understanding those cost drivers is useful since the cost will directly or indirectly need to be paid by the enterprise.

Short range networks like Wi-Fi have low cost per access point, but they require dense deployment and fixed broadband access that drive up the cost for providing a wider coverage. Proprietary LPWA networks in contrast may require the least investment for providing a national coverage with a few low cost base stations, although more sites will eventually be needed to cope with the interferences as the unlicensed spectrum becomes more crowded. Traditional cellular networks have in most places excellent existing coverage and cellular LPWA can be implemented on top with only marginal cost. While telecom operators may charge a premium for better QoS, it is expected that cellular LPWA would be able to offer a lower price level than traditional cellular options.

**Scalability**

Wireless IoT connectivity is a commodity. Therefore, an IoT network should possess the ability to quickly and cost effectively scale up its capacity as needed. The scalability of a network is not just about the number of devices that...
can be connected to a single access point, but also about how many of them can actively transmit concurrently and if the network would be negatively affected by interferences from external sources.

Cellular networks have an advantage in this regard for applications that foresee large volume with sustained growth. Centralized coordination in cellular networks allows more devices to transmit simultaneously, and their exclusive access to licensed spectrum protects the transmissions from any external interferences. Most of the short range technologies and proprietary LPWA solutions instead employ uncoordinated and unlicensed spectrum which may impose restriction on their scalability in the long run.

**Future proofness**

The future proofness of a technology encompasses longevity to assure its availability in the future, as well as long-term economic viability, derived from long-term cost reduction potential.

Technology longevity is a crucial consideration for IoT applications with logistical and cost challenges for replacing deployed devices. Understanding the strategic intention of key stakeholders backing the technology can help predict future direction of its development. For instance, Ingenu and Sigfox are start-ups funded by venture capital, whose commitment and ability to provide long-term service continuity are yet to be time tested. Furthermore, an open standard approach adopted by the likes of LoRa promises a better sustainability than technologies with closed systems. The latter poses a risk for single point of failure while the former creates opportunities for multiple service providers and vendors.

Selecting a technology with the potential to achieve economies of scale ensures the investment is economically sustainable as the business grows. A mature ecosystem, like that of cellular or Wi-Fi, not only develops a strong technical roadmap with industry wide cooperation but also promotes heavy competition in the commercialization among numerous vendors and service providers. Proprietary LPWA technologies have the time to market advantage over cellular LPWA solution NB-IoT, but their ecosystems are still at early stages. Telecom operators are hedging on different LPWA technologies to meet the short term market demand. Fragmentation will continue until a dominant technology emerges with substantial volume backed by government stimulus and endorsement from global service providers.

**Global reach and interoperability**

Global companies need global solutions in order to achieve economies of scale and avoid having different technologies and network operators for each single market, but also because products sold in one market may be deployed by the customer in another market where they need to work “out of the box”. Global reach and interoperability (across networks of the same technology) also create a market of larger volume and global competition, both of which help to drive the cost down.

Many of the predominant short range technologies, such as Wi-Fi and ZigBee, are developed by IEEE standardization association and supported by global industrial alliances to promote international interoperability. They operate in the 2.4 GHz ISM band, which is available globally.
Many proprietary LPWA technologies have a stronger regional presence in either the U.S. or Europe. They often have to make a trade-off between global reach and interoperability. An open standard approach, as in the case of LoRa, creates a vibrant ecosystem encouraging innovation and wider adoption globally, but it leaves too much room for proprietary variants that will not be able to communicate to each other. On the other end of the spectrum, a closed standard approach as in the case of Sigfox ensures the interoperability but restricts the ecosystem scale and reach. Another challenge faced by emerging LPWA technologies is the fragmented regional regulations in sub-1GHz unlicensed spectrum – low cost devices and simple protocols might not be capable of detecting and adhering to the appropriate regional requirements.

The cellular industry has created global standards and cellular networks currently offer the best global reach. Adding to that, NB-IoT will be deployed by international operators in harmonized cellular band to offer global reach.

2.2 ASSESSMENT OF LEADING CONNECTIVITY TECHNOLOGIES

While there is no single technology that can best serve all use cases, only a few connectivity technologies can emerge as the dominant options in each category. For IoT deployments in remote/wide areas, LoRa and NB-IoT are good complements to each other and together will address a large share of this market. LoRa’s dynamic open ecosystem is ideal for private networks with customized deployment, while NB-IoT is backed by major mobile operators offering standardized connectivity with global reach. Other proprietary technologies, like Sigfox, may address certain niche segments but with uncertain future proofness. For applications requiring high data rate, the most promising technology options are either LTE or Wi-Fi, depending on the scope of the IoT deployments. For local short range applications, the choice of connectivity technology is less obvious and often the interfaces and implementation of platform and application layers become more crucial.

The key strengths and weaknesses of the three main types of technologies – traditional cellular, LPWA and short range – are summarized in Figure 6. Table 1 compares a number of the leading IoT connectivity technologies from the perspective of the different considerations discussed in the previous section.

**Figure 6. Key strengths and weaknesses of different types of connectivity technologies**
| Considerations          | Traditional Cellular | Cellular LPWA | Proprietary LPWA | Short Range |
|-------------------------|----------------------|---------------|------------------|-------------|
|                         | 2G                   | 3G            | 4G               | LTE-CatM1   | EC-GSM | NB-IoT | SigFox | LoRa | Ingenu | Wi-Fi low power | ZigBee 3.0 | Bluetooth LE |
| **Outdoor coverage**    | >10km                | >10km         | >10km            | >10km       | >15km    | >15km  | >10km  | >15km | <1km   | <300m            | <100m     |             |
| **Indoor coverage**     | High                 | Medium        | Medium           | Medium      | High     | High   | High   | High  | Very low | Very high        | Medium    | Low          |
| **Energy efficiency**   | 2-5 years            | <10 days      | <10 days         | >10 years   | >10 years | >10 years | 10-20 years | 10-20 years | 6-12 months | 6-12 months | 6-12 months |
| **Typical uplink data rate** | 50 kbps             | 1 Mbps        | 10 Mbps          | 1 Mbps      | 200 kbps | 20 kbps | 100 bps | 25 kbps | 50 kbps | 1 Mbps            | 250 kbps | 1 Mbps       |
| **Bidirectional communication** | Yes                 | Yes           | Yes              | Yes         | Yes      | Yes    | Yes    | Yes   | Yes     | Yes               | Yes       | Yes          |
| **Mobility**            | Very high            | Very high     | Very high        | Very high   | High     | High   | Very low | Low   | Medium  | Medium            | Low       | Very low     |
| **Localization**        | Yes                  | Yes           | Yes              | Yes         | n/a      | No     | Limited accuracy | n/a  | Yes     | Yes               | Yes       | Yes          |
| **QoS & security**      | Very high            | Very high     | Very high        | Very high   | High     | High   | Very low | Low   | Medium  | Medium            | Medium    | Medium       |
| **Device cost**         | $5-10                | $15-30        | $30-50           | $20-40      | $5-10    | $5     | $1-5   | $5-10 | $5-10   | $5                | $5        | $5           |
| **Connectivity cost**   | Medium               | High          | Very high        | High        | Medium   | Medium | Very low | Low   | Medium  | Medium            | Medium    | Medium       |
| **Scalability**         | High                 | High          | High             | Very high   | Very high | Very high | High   | High  | Low    | Low               | Very low  | Low          |
| **Future proofness**    | Medium               | Medium        | Very high        | High        | Medium   | Very high | Low    | High  | Low    | Medium            | High      | High         |
| **Global reach & interoperability** | Very high           | Very high     | Very high        | High        | High     | High   | Medium | Low   | Very low | Low               | Medium    | High         |

Table 1. Main technologies for IoT

---

2 The data points in this table are collected from official reference sources, including 3GPP standards for cellular technologies, company websites for proprietary LPWA technologies, IEEE 802 standards for Wi-Fi, ZigBee and Bluetooth. “n/a” is used in the table where official information was not available.
This section discusses the needs of some example application areas with respect to the technical, commercial and ecosystem considerations introduced in the previous section to illustrate how these needs determine the choice of connectivity technology for each area (or use case within). A summary is provided in Table 2.

An application area is usually not homogenous and there can be differences in development stage across markets. As a result the discussion on needs may differ to some extent. Markets that are new to IoT have the advantage of being able to learn from best practices in more developed regions and benefit especially from partners that provide both technology and experience. Developing markets typically start with the more basic applications and therefore may not have as high initial requirements but can develop fast to more advanced applications.

Table 2. Application areas, typical needs and suitable connectivity technologies

| Application area          | Need for: | Suitable connectivity technologies |
|---------------------------|------------|-----------------------------------|
|                           | Indoor coverage | Wide area coverage | Energy efficiency | High data rate | Bidirectional comm. | Mobility | Localization | QoS & security | Low cost | Scalability | Future proofness | Global reach & interoperability | |
| Automotive                | L M H L H H L H | Cellular |
| Smart cities              | M M L L L H L H | LPWA, Wi-Fi |
| Safety and security       | H M L H M L L L | Cellular, LPWA |
| Industrial manufacturing  | H L L H M L M H M L | Wi-Fi, Cellular |
| Fleet and logistics       | M M H H M L M L | Cellular, LPWA |
| Asset management          | H H L L M L M L M | Cellular, LPWA |
| Agriculture and environment | L H L H L L L L | LPWA |
| Smart meters              | H H H L M L L M H | Cellular, LPWA |
| Wearables                 | H L L L L L M H L L | Bluetooth, ZigBee |

L = Low, M = Medium, H = High
The connected car is already a reality, providing vehicle owners and car manufacturers with great amounts of data about driving behavior, car performance, need for maintenance and more. The connected car market is set for fast growth in the next decade, as in-vehicle wireless connectivity is rapidly expanding from luxury brands and models to the mid-market segment. Gartner Research has forecast that about one in five vehicles on the road worldwide will have some form of wireless network connection by 2020, amounting to more than 250 million connected vehicles in service.

For a connected car with embedded connectivity (where both the connectivity and intelligence are built directly into the vehicle), there is a wide range of requirements that have determined cellular as the most suitable technology. To begin with, a key feature of vehicles is mobility, which translates into the need for reliable coverage while in motion and regardless of location – both national coverage in urban and rural areas, as well as global reach (roaming capability) to provide continuous connectivity when driving across borders.

Connected cars have a need for high QoS – both in terms of reliability of the network to ensure the faultless operation of features such as voice calls, remote access to car functions, real-time navigation, automatic crash notification and roadside assistance, as well as low latency to be able to in the future enable the vision for self-driving cars. In addition, security is a major consideration given the nature of personal data collected, and unauthorized access to the car’s main systems can have life-threatening implications for the driver and passengers. Connected cars have also demands for high data rate in order to support infotainment services for streaming of music and video.

From a commercial perspective, the cost of connectivity is important as the auto makers are trying to find the best business models and build ecosystems with services that create value and willingness to pay. From a technology ecosystem perspective, another major requirement is longevity – the product development cycles for new vehicles can be three to five years, followed by a lifespan of seven to ten years. These long lifecycles mean that it is necessary to rely on a connectivity technology and solutions that have long-term commitment by technology vendors and operators and support over the air software updates. With the GSMA embedded SIM Specification, automakers will be able to remotely provision connectivity over the air to vehicles with an operator of their choice and connect vehicles with local operators, regardless of where the cars are manufactured.

Currently, no other technology apart from cellular can fulfill all the above mentioned key requirements, which is why connected cars by Volvo, GM, Tesla etc. are today typically using HSPA+ or LTE technology and will likely continue to rely on cellular standards for the foreseeable future.

The objective of smart cities is to improve the quality of life and public services, traffic and safety as well as conserve limited resources and monitor the condition of vital infrastructure. Therefore, there is a wide variety of use cases within this area, some of the most discussed being smart parking, waste management, street lighting, noise monitoring and many more.

What many of these use cases have in common are the key needs for good coverage in urban areas, long battery life (10+ years) and low cost of the solution and connectivity, which can enable cities to justify the investment of public funds. In addition, although each of the connected devices may be sending little amounts of data, the magnitude of smart cities means that tens of thousands of devices may be connecting to a single access point/ base station and will need to often transmit data simultaneously, thus placing demands for network scalability, especially as new devices are constantly added.

The combination of above requirements is best satisfied by LPWA technologies. Proprietary LPWA technologies such as LoRa and Sigfox have the advantage of being first to market and are offering good cost efficiency. Since these proprietary technologies are using unlicensed spectrum, they may face some potential scalability challenges in the long run as more networks and billions of devices are deployed using the same unlicensed band, but in the short to medium run, they are capable of meeting requirements. With the commercial launch in the near future of cellular LPWA technologies such as NB-IoT and EC-GSM, the technology alternatives will expand, as they bring comparable benefits plus the extra advantages of better quality of service, reliability and security.

Wi-Fi networks are another suitable alternative, especially for use cases like smart parking, which entail connecting sensors within an indoor parking garage.

Connected assets offer benefits both to the businesses that own them and the businesses that manufacture them. In this application area we include a wide range of mostly fixed assets – water pumps, vending machines, elevators, ice cream machines, lawn mowers and similar. If companies have better insights into how their assets are working, they can improve efficiency and avoid downtime through predictive rather than reactive maintenance. If businesses that manufacture such assets can receive data on how their products are used, they can offer better service and maintenance, supply spare parts faster, develop new (value added) services or even entirely transform business models (e.g. from product to service).

Most of these assets are used indoors and can often be in dispersed locations in urban areas (e.g. vending machines) but also in rural areas (e.g. water pumps). Therefore, they have the need for reliable (indoor) coverage at low cost.
For many businesses global reach is also needed so that a single type of device can fit each machine produced to be sold anywhere in the world. Assets would send small amounts of data more or less frequently, but high data rate is not a requirement. Depending on the type of asset, quality of service guaranteed by SLAs can be important.

Cellular 2G networks offer good coverage and telecom operators can provide global reach. LPWA networks can also serve many use cases in this application area, especially when cost is a deciding factor, thus allowing to connect even assets of less value.

**CASE STUDY: CARPIGIANI GROUP**

*This case study is provided by Telenor Connexion*

**About the company and its IoT challenges**

Carpigiani is a market-leader in the production of machines for gourmet gelato, better known as Italian-style ice cream. Carpigiani was founded in 1946 by the Carpigiani brothers, and quickly established itself as the market leader in the production of machines for gourmet gelato. During the 1960s and 1970s, Carpigiani began to expand globally.

The Italy-based company manufactures over 10,000 ice cream machines per year, of which over 80% are being exported around the world. Customers span from small ice cream shops to large global fast-food brands and the installed base of machines exceeds hundreds of thousands.

The company was early in seeing the benefits of connecting its products and started the process in the late 90’s.

**Main reasons for being connected**

- **Cut cost of aftermarket service within the warranty period.**
- **Long lifespan of machines calls for an efficient way to do upgrades and maintenance.** By monitoring the lifecycle of the machine based on actual use, not time, customers reduce the risk of downtime. The system schedules the substitution of critical parts only when necessary and based on the quantity of ice cream produced.
- **Increase the efficiency of machines.** Connectivity enabled the company to offer a remote monitoring system, Teorema, by which the efficiency of each machine is improved. The data generated is used to comprehensively examine the state of the equipment and to provide the customer with a diverse range of service options, including predictive maintenance and cost reductions such as decreased downtime, less waste, compliance with hygiene & safety regulation, energy savings.
- **Allow to perform field tests for improvement and new machines.**

All the above became especially important when the company started to expand worldwide with machines installed in many countries.

**Key connectivity needs and technology choice**

The first steps of the project were undertaken in the late ’90s, when only few technologies were available. Carpigiani started with the powerline technology, but faced challenges such as difficulties to access firewalls where the machines were installed.

The company then switched to cellular technology and the first big deployment of the system took place in early 2008. At first the connectivity was provided via a local network provider, but when the company started expanding out of Italy it was no longer possible to work with a local operator. At that time (2010) the cooperation with Telenor Connexion started.

The machines were not mobile and only needed to transmit small data volumes. Therefore, the critical requirements on connectivity were:

- Global reach and standard connectivity
- Reliability and accessibility

Carpigiani tried several different technologies but cellular technology has proven most suitable to meet the company’s requirements.
INDUSTRIAL MANUFACTURING

Industry 4.0 is a collective term that in recent years has come to signify the transformation that IoT brings to the world of industrial production. Sensor technology and connectivity make it possible to create smart factories in which machines can connect and self-organize, optimizing the production process based on real-time data. Smart factories can even be connected into one production network to form a global factory. Companies such as General Electric and Harley Davidson have already reaped benefits from transforming their manufacturing process through IoT.

Industrial manufacturing use cases need connectivity that offers good indoor coverage, often in industrial regions, and high reliability since every interruption of service can be very costly. In addition, many of the machines are in close proximity to each other and multiple sensors send frequently data, thus requiring high bandwidth at low cost. In many factories, machines were not initially designed to be connected and thus need to be retrofitted with sensors and connectivity, which means that the network fabric must be adaptable to a mix of both legacy and new machines and be able to scale up easily as new machines are being connected.

Wi-Fi networks have a lot of advantages in meeting the needs above, offering good indoor coverage and high capacity at low connectivity cost (after the initial investment in setting-up the network). It is also relatively easy to retrofit legacy machines with sensor nodes with Wi-Fi connectivity. Cellular technologies such as 2G/GPRS can also be a suitable alternative for companies within industrial manufacturing, eliminating the need to set-up and maintain private Wi-Fi networks and providing high quality of service through SLAs.

Typically, cellular networks, especially 2G/GPRS have been best suited and most commonly used for tracking large moving assets. As network operators are increasingly shifting traffic to their 3G and 4G networks (and some operators even plan to shut down their 2G networks), the faster networks offer expanded benefits that can enable new services – such as video streaming, new productivity tools etc.

Apart from the large assets, there is a whole category of lower value assets like packages, luggage and other items that are to a great extent still unconnected and tracked only by scanning barcodes. LPWA networks can make it economically feasible to track such a large number of widely dispersed objects through sensors that can send location and other status updates. LPWA networks can also be suitable for creating sophisticated integrated solutions that serve large docksides and warehouses.

WEARABLES

This consumer application area includes devices attached to the human body (also called wearables), such as smart watches, connected shoes and clothing, fitness and healthcare devices. Their purpose is to measure and collect data on human activity – exercise, sleep, heart rate, blood pressure and many more in order to improve wellness, health and productivity.

What these devices have in common is that their use is tightly connected to the use of a smartphone, which is already wirelessly connected, as well as the need to work out of the box and at virtually no extra cost since consumers do not appear willing to pay for separate connectivity for their wearables. Therefore, for a majority of these devices Bluetooth is a natural choice since it provides the necessary short-range connectivity at no cost.

FLEET MANAGEMENT AND LOGISTICS

This application area includes a variety of use cases for tracking and management of moving assets – trucks, shipping containers, construction equipment vehicles etc. Connected solutions in fleet management allow to monitor vehicle location, optimize route planning, perform remote vehicle diagnostics and analyze driving behavior. The resulting benefits are that businesses can improve operations and delivery time, prevent theft and save fuel.

The main connectivity requirements for these type of solutions are about reliable coverage - both in urban and rural areas as well as global reach (roaming capability) to provide continuous connectivity when assets travel across countries. Other requirements include also localization capability for tracking location, quality of service to ensure that assets do not “go dark”, and longevity of the technology as some of the assets (like vehicles) have production and life cycles spanning over a decade. The latter also means that the devices have SIMs and modules that are future proof and support bidirectional communication for over-the-air updates to avoid the need for costly swapping out in the field.

SMART METERS

Smart meters are used in electricity, water and gas. Smart electricity meters in particular have been the most developed use case to date, because it offers good cost savings and since electricity meters have access to power supply so battery life has not been an issue. For electricity meter deployments traditional cellular technology has been widely used, meeting well the requirements for coverage, reliability and longevity of the technology (meters can have a lifespan of up to 15 years).
Water and gas meters on the other hand are often located underground and in more inaccessible places (e.g. sensors placed in sewers), without access to electricity supply and thus requiring very long battery life.

These use cases are hard to address with traditional cellular systems but LPWA solves both of the above challenges. NB-IoT technology is very suitable for water-metering applications, which have some of the most extreme coverage requirements underground.

CASE STUDY: SMART METER COMPANY

This case study is provided by Telenor Connexion

About the company and its IoT challenges

The company manufactures certified gas, heat and electricity meters on a global scale. Approximately 15 years ago legislation was passed in some countries that invoices for utilities should be based on actual consumption and not on estimates. This created the need for smart meters that can communicate with a central system to deliver automatic meter readings at specific time intervals.

A meter company has two main types of customers:

- Utility companies;
- Meter reading companies (whose business is to collect and secure meter readings from millions of meters and deliver quality assured readings to utility companies).

As the product is standardized, meter companies compete on pricing but are trying to move from a product centric business model (meter equipment) to delivering a service instead.

Main reasons for being connected

- IoT is the only way of accessing readings in a cost efficient way due to many, remote meters
- The long lifespan of meters calls for remote operation and upgrades

Key connectivity needs and technology choice

The main considerations when choosing connectivity technology are:

- Global reach to support global deployments
- Scalability to ensure growth
- Easy plug and play solution
- Reliability and quality of service (ensured by SLAs)
- High security for customer and invoicing data
- Good coverage in remote areas
- Future proofness of the technology and a trusted supplier to match the long lifecycles of meters

Historically the choice of connectivity technology has been among powerline communication, local RF (radio) and cellular. With the first two, a transformer collects the readings, which are sent via fiber or GSM. This provides an easy and cost efficient installation but the operation is complex and expensive. Any disturbance will eliminate data readings, which then have to be carried out manually. These techniques also pose a question of who is the service provider, which makes it hard to change the business model into a service.

Cellular technology, specifically 2G, was selected as most suitable option. It allows the meter company to buy communication as a service from an operator instead of having to set-up own network, which simplifies operation and roll-out of new systems. It also satisfies well the requirements for reliability, security, coverage and global reach. As the cost of cellular connectivity has decreased over time, cellular became increasingly attractive.

LPWA can be an alternative to 2G, especially as 2G may be phased out in some markets. LPWA allows low hardware and operation cost and satisfies well the coverage requirements. LORA and Sigfox can be used but entail trade-offs with respect to reliability and SLA requirements. NB-IoT has interesting potential and when commercially available will be also a very suitable option.
SAFETY AND SECURITY

Connected safety and security includes a wide range of use cases ranging from video surveillance in both public setting and on private properties, security alarms to prevent intruders, as well as safety alarms to signal events such as fire, gas or water leakage.

These use cases can have varying requirements. Video surveillance, for example, has demands for high data rate, coverage and bandwidth as streaming video entails significant data traffic. In addition, quality of service and reliability need to be very high to ensure uninterrupted operation in real time. Security for the data transmission is often highly important, which entails the need for heavy processing for encryption and decryption of data. These requirements are very well served by cellular networks such as 4G LTE (but also 3G) that can provide a high rate of data transmission. Although LTE networks have high capacity, bandwidth consumption can be a challenge for LTE if a large number of cameras need to be served – this challenge though can be mitigated with careful system design for efficient scheduling, camera placement etc. Wi-Fi networks can be another technology option for supporting video surveillance applications and have the benefit of lower cost and ability to support devices that are geographically dispersed and send occasionally small amounts of data. For tracking livestock, reliable localization is also important. Once the devices are deployed across large remote areas, they are expected to need minimum maintenance and operate for long periods of time without access to power supply. Therefore, long battery life but also future-proofness of the technology are essential.

Security and safety alarms send small amounts of data, often infrequently, but have requirements for high reliability, security, indoor coverage and low cost. Cellular 2G/GPRS networks fulfill these conditions and are typically used to provide wireless connection between the on-site control panel and the central monitoring station. The needs of safety and security alarms are also very well served by LPWA networks, especially if the alarms are used for buildings in remote areas. Sigfox has, for example, made deployments in home security, where they provide back-up connectivity to create a more robust system in case the building’s primary broadband connection fails or the burglars use GSM jammers. NB-IoT and EC-GSM are expected to offer very good benefits.

AGRICULTURE AND ENVIRONMENT

Sensors can be used in agriculture to monitor environmental conditions such as solar intensity, the temperature and humidity of soil and air, thus defining the optimum time and location for irrigation, fertilization etc., resulting in more efficient use of agricultural land and resources and improving the quality of produce. Another use case is tracking the location and health of domesticated and wild animals. Environmental agencies can also use sensors to monitor weather conditions.

What these use cases have in common is the need for coverage in rural/remote areas, low cost and ability to support devices that are geographically dispersed and send occasionally small amounts of data. For tracking livestock, reliable localization is also important. Once the devices are deployed across large remote areas, they are expected to need minimum maintenance and operate for long periods of time without access to power supply. Therefore, long battery life but also future-proofness of the technology are essential.

This area is one of the most suitable for LPWA technologies – both proprietary alternatives such as LoRa and Sigfox but also cellular LPWA such as NB-IoT and EC-GSM are expected to offer very good benefits.
As illustrated in the previous section, different application areas and use cases have different needs that determine the most suitable choice of technology. At the same time, these needs may change over time and new use cases will appear. Therefore, what the requirements of future IoT applications will be is not completely clear.

Using a single connectivity technology has advantages but some enterprises will face situations where multiple technologies need to be used in parallel, either because they serve different applications that are part of a larger system, or because they serve the same application but in different environments/geographies where network availability differs. In those cases, cloud platforms as the middle layer of integration can become an important means for navigating complexity and allowing to unify the data collected and present it through the same interface. This may mitigate certain future risks but can present other challenges as it entails considerable transformation and integration efforts. Therefore, the choice of connectivity technology still remains an important decision that can have long-lasting implications.

4.1 5G AND IOT

5G has been garnering increasing attention as a future enabler for critical and massive IoT. 5G as the next generation mobile technology is still primarily focused on mobile broadband evolution, but it will bring architectural changes and new features that give operators better flexibility to address the diverse requirements and massive connections of future IoT applications. More specifically, 5G will support:

- Multi-radio access technology coexistence that integrates devices deployed in different environments, for example in both Wi-Fi and cellular networks into a unified network layer and thus brings better transparency to the end user;
- Network slicing that creates ‘private-like’ networks for different IoT applications with separated billing and service provisions;
- Ultra-low latency (less than 1ms) high reliability communication for mission-critical applications.

With these improvements 5G undoubtedly will provide new opportunities within IoT but it will not become available before 2020. Until then, the latest cellular IoT technology NB-IoT will continue its evolution and eventually become a pillar in future 5G networks. Therefore, enterprises that have identified specific IoT opportunities need not wait for 5G with so many IoT connectivity technologies already or soon-to-be available.
ABOUT THIS PAPER

This white paper was written by Northstream with the aim to provide an objective and independent view on IoT connectivity technologies.

While the white paper was commissioned by Telenor Connexion, all opinions expressed are entirely Northstream’s and do not necessarily represent the opinions of Telenor Connexion.

ABOUT TELENOR CONNEXION

Telenor Connexion designs and operates Internet of Things (IoT) solutions. Building on more than 15 years of experience Telenor Connexion provides reliable IoT solutions to a number of global customers such as Volvo, Nissan, Scania, Hitachi, Verisure Securitas Direct and Telcare. Headquarters and tech centre are located in Sweden and the company has regional offices in UK, Germany, US and Japan. Telenor Connexion is wholly owned by Telenor Group, one of the world’s major mobile operators.

www.telenorconnexion.com

ABOUT NORTHSTREAM

Founded in 1998, Northstream is an experienced management consulting firm providing strategic business and technology advice to the global telecom and media industries. We help our clients through independent and objective analyzes, advice, problem solving and support that are tailor-made to our client’s situation. Our work is based on a well-balanced combination of innovation, industry best practices and in-house methodologies. Northstream typically works with:

- Business strategy development and planning
- Strategic sourcing of systems and services
- Technology & product strategy evaluation
- Operational review, optimization and support
- Investment analysis and due diligences

Clients across the world include mobile operators, network and device suppliers, application providers, investment banks, regulators and industry fora. Contact us to learn more about how we can work together to ensure your success in the mobile voice and broadband business.

Strategy and Sourcing
www.northstream.se