Northstream™

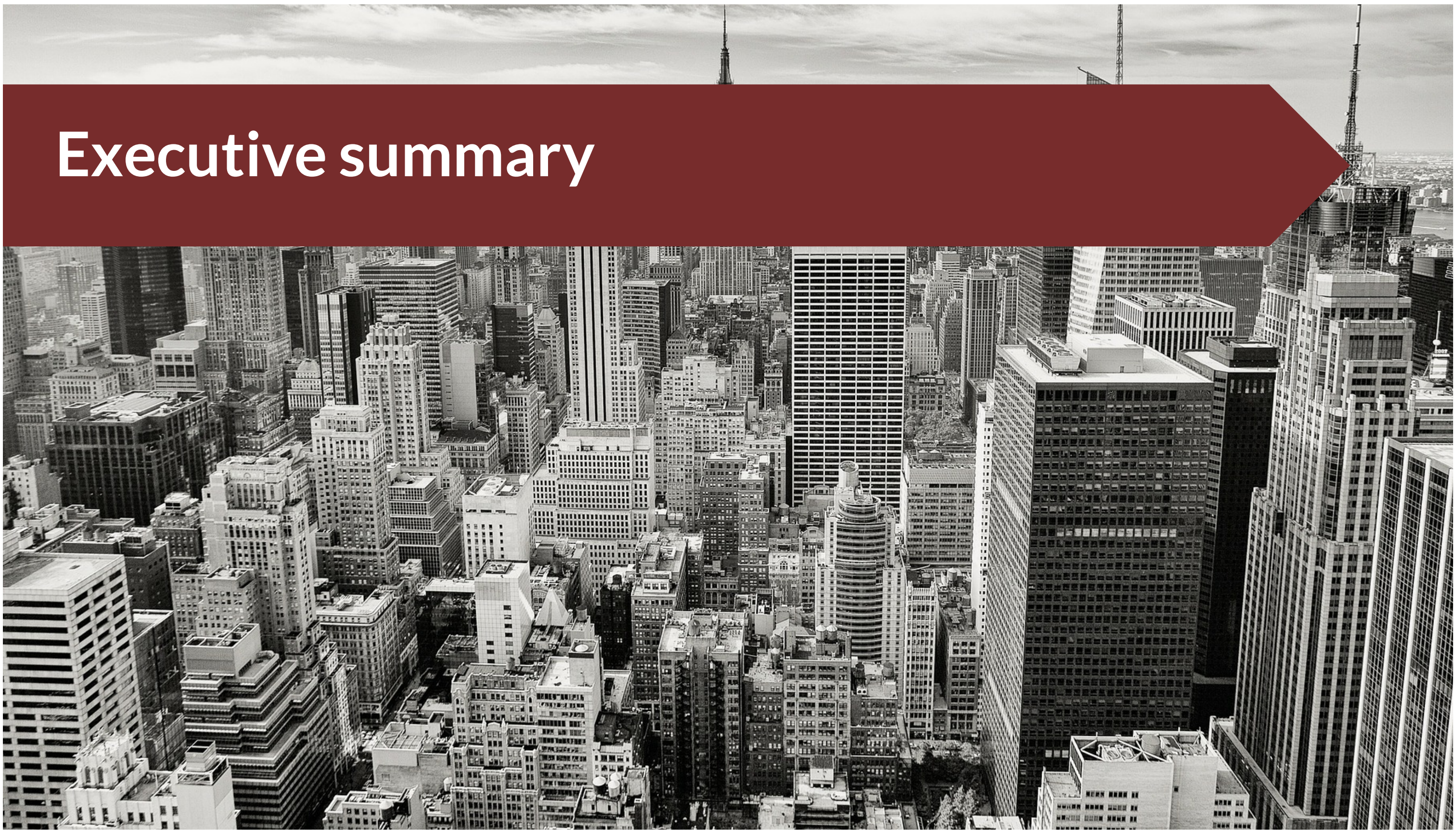
Massive IoT: different technologies for different needs

Northstream White Paper
2017

Commissioned by

WIREPAS

Executive summary



Over the last decade, connectivity in the paradigm of machine-to-machine communication has mostly been concerned with connecting a few high value devices or data gathering points to a centralized monitor and control room. With the advent of the IoT era, “things” no longer just send and pull information from the data centre, but are also beginning to talk to each other. The number of connectivity links is growing exponentially, as new applications continue to emerge and more industry verticals begin to transform their business with the Internet of Things (IoT). As a result, massive IoT is emerging as a new focal point for IoT connectivity technologies.

The sheer number of devices and the scope of massive IoT deployments set stringent requirements on the network coverage, battery life and cost of the device, as well as the cost of connectivity. Several new technologies such as NB-IoT and Sigfox are emerging as cheaper connectivity options optimized for range and energy efficiency, and therefore can be well suited for large scale deployments spread across wide areas.

One of the prominent candidates for addressing the upcoming density challenge is 5G. With a streamlined signaling protocol and a lean air interface, 5G aims to connect millions of devices per square kilometer. In addition, network slicing will provide cellular networks with the much needed flexibility to address specific Quality of Service (QoS) requirements set by enterprises.

Another complementary connectivity option focusing on high density IoT deployments is mesh technology. Originally designed for home/factory automation, mesh technology has expanded its capabilities to cover wider areas thanks to advancements in device capabilities and network protocols. In particular, the scalability of mesh networks can be increased by employing a flat network architecture with autonomous nodes. The reliability and the performance of these networks improves with denser deployments of nodes and gateways, but conversely they lose these advantages if the density is low.

Each of the connectivity technologies on the market today has its own technical advantages and focus. As a result, they are optimally suited to address different segments of massive IoT. Rather than competing with each other, these technologies are highly complementary. The proliferation of long range technologies like NB-IoT or LoRa can provide better backbone connectivity for mesh networks to reach wider areas, and similarly non-cellular technologies like mesh are opening up more industries and enterprises to engage in IoT, which in turn may create more demand for cellular connectivity.

More importantly, different technology options address different business needs for enterprises. Therefore, there is no one-size-fits-all solution. The choice of connectivity technology for massive IoT requires a careful examination of the specific requirements of the use case and the business need of the enterprise, as well as a solid understanding of the relative strengths of each technology option.

1. Introduction

1.1 GROWING RELEVANCE OF IOT TO ENTERPRISES

The number of smart objects or devices worldwide continues to increase at a dramatic pace, with an estimated 8.4 billion connected "things" already in use in 2017, according to Gartner[1]. While consumer IoT accounts for 63% of these connections today, enterprises have also long understood the benefits that IoT can bring to their business, and are implementing different connectivity technologies to capitalize on the opportunity. Selecting the most suitable connectivity technology to meet the enterprise's specific needs is one of the most crucial decisions within an IoT launch strategy, as it can impact the success of the service as well as opportunities for future growth. For instance, choosing a technology which is not easily scalable, or which is not future-proof, can lead to high costs down the line.

There are many benefits that IoT can bring to enterprises; from increasing revenues by enabling new business models (e.g. from a product to a service) and new services, to decreasing costs in internal processes. These benefits apply to a range of different industries, each with unique applications and requirements. Due to the diverse nature of these use cases, there is no one-size-fits-all technology solution. Many factors, both technical and non technical, will dictate the best choice of technology.

1.2 EMERGING MASSIVE IOT APPLICATIONS

As the landscape takes shape, two main categories for IoT applications are beginning to emerge. These can be defined as critical IoT and massive IoT[2], based on the technical and commercial requirements they prioritize. Critical IoT applications are those which require very low latency levels on ultra-reliable networks, often combined with very high throughput. For example, autonomous driving or healthcare use cases such as remote surgery.

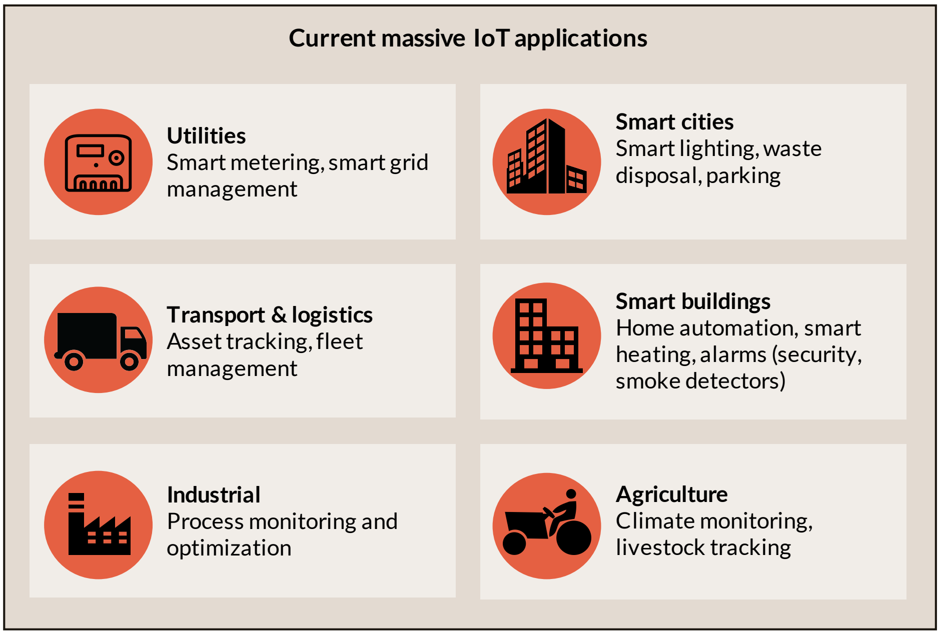
Massive IoT, on the other hand, refers to those applications which are less latency-sensitive and have lower throughput requirements, but require a huge volume of low-cost, low-energy consumption devices on a network with excellent coverage. Figure 1 illustrates some examples of massive IoT applications. The growing popularity of IoT use cases in domains that rely on connectivity spanning large areas, and able to handle a huge number of connections, has driven up the demand for massive IoT technologies.

[1] Gartner report, "Forecast: Internet of Things – Endpoints and Associated Services, Worldwide, 2016"

[2] Ericsson white paper" Cellular Networks for Massive IoT"

Enterprises across a range of verticals are leveraging the benefits of IoT to improve their business and processes. They are poised to experience considerable economic impact from IoT services, as processes can be optimized, information can circulate more quickly and, in some cases, labour costs will be reduced. Critical and massive IoT are only starting to clearly emerge as categories, and there will be different connectivity technologies designed to address their specific requirements.

The following chapters further expand on the requirements for massive IoT applications, and discuss several connectivity technologies in terms of their core focus and suitability for addressing massive IoT.



Current massive IoT applications

Utilities
Smart metering, smart grid management

Smart cities
Smart lighting, waste disposal, parking

Transport & logistics
Asset tracking, fleet management

Smart buildings
Home automation, smart heating, alarms (security, smoke detectors)

Industrial
Process monitoring and optimization

Agriculture
Climate monitoring, livestock tracking

Figure 1 Applications requiring massive IoT

2. Connectivity requirements and options

2.1 CONNECTIVITY REQUIREMENT FOR MASSIVE IOT

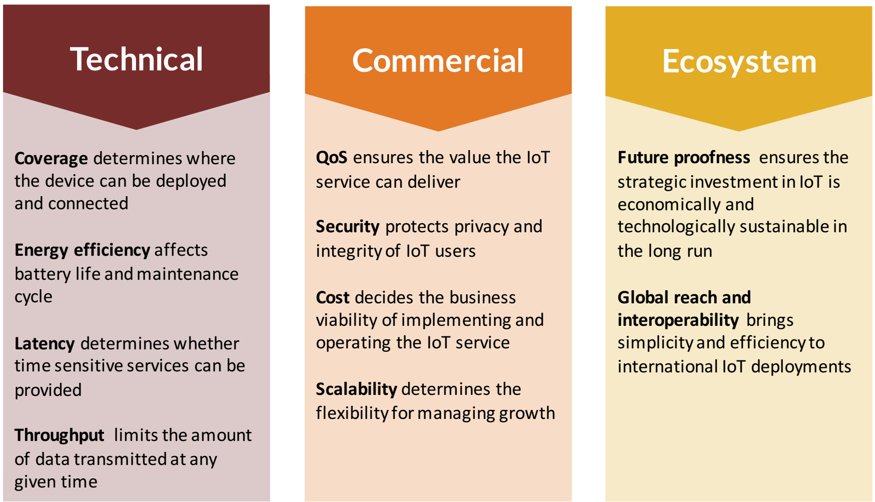
Northstream has presented a framework for IoT connectivity requirements in a previously published white paper, "Connectivity Technologies for IoT"[3], as illustrated in Figure 2 below. Cross examining the Massive IoT use cases described in the previous section against this framework, it becomes clear that these applications share the same requirements for many dimensions.

2.1.1 TECHNICAL CONSIDERATIONS

On a technical level, massive IoT applications typically consist of many devices spread out in a wide area, ranging from large manufacturing plants to cities or even whole countries. Some of the devices are stationary and can be located in challenging radio environments, such as inside a basement or a factory. To accommodate such environments, the connectivity technology used for massive IoT applications needs to not only provide wide coverage, but also a robust signal able to penetrate deep indoors.

Due to the sheer number of devices and the scale of deployments, the technology used for these applications needs to be energy efficient, to enable long battery life and limit the costs for device or battery replacement.

Massive IoT applications often have low to moderate requirements on throughput and latency levels, as they mostly involve data collection and non-critical control functions. Nevertheless, the requirements can still vary from anything as low as several bits per second to hundreds of kilobits per second on throughput, or from seconds to hours of delay tolerance depending on the application.



Technical

Coverage determines where the device can be deployed and connected

Energy efficiency affects battery life and maintenance cycle

Latency determines whether time sensitive services can be provided

Throughput limits the amount of data transmitted at any given time

Commercial

QoS ensures the value the IoT service can deliver

Security protects privacy and integrity of IoT users

Cost decides the business viability of implementing and operating the IoT service

Scalability determines the flexibility for managing growth

Ecosystem

Future proofness ensures the strategic investment in IoT is economically and technologically sustainable in the long run

Global reach and interoperability brings simplicity and efficiency to international IoT deployments

Figure 3 Main considerations for selecting an IoT technology

[3] Northstream white paper "Connectivity Technologies for IoT"

2.1.2 COMMERCIAL CONSIDERATIONS

From a commercial perspective, the requirements on QoS and Security, while relevant, may not be equally crucial for all applications. In fact, it is perhaps more important for the technology to be flexible enough to handle different QoS and security requirements, as they are unlikely to be fully homogeneous within such a large scale deployment.

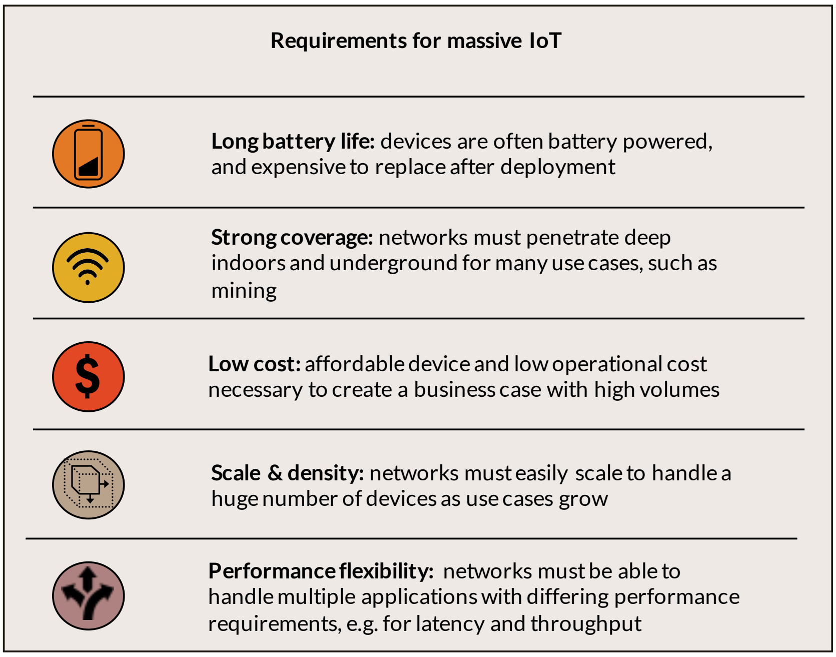
Scalability is a key requirement for massive IoT. These applications will evolve and grow over time and the connectivity technology addressing them must be able to easily scale to meet new capacity demands, without disrupting existing services. Furthermore, scalability is closely linked to cost, as the ability to connect densely deployed devices in large numbers also depends on the viability of the business case. In the absence of affordable devices and low connectivity cost, the business validity of a massive IoT solution would be jeopardized by the total cost of ownership for the implementation and operation of the service.

2.1.3 ECOSYSTEM CONSIDERATIONS

Lastly, turning to the ecosystem dimension, it is perhaps more pertinent for Massive IoT than for any other application to choose a future proof technology, as the volume of devices would render it prohibitively expensive to migrate them to a different technology down the line. One way to ensure this sustainability is to enable OTA (over the air) post-installation software provisioning in order to adapt to any new needs or configurations that may arise.

While massive IoT is certainly deployed in large scale, it can still be contained to regional or national operations. Therefore global reach and interoperability are not necessary requirements for all Massive IoT applications, but may become relevant in certain cases. For example, if an international enterprise is seeking to deploy a solution on a global scale.

Figure 3 below summarizes the key requirements on connectivity technology for massive IoT.



Requirements for massive IoT

Long battery life: devices are often battery powered, and expensive to replace after deployment

Strong coverage: networks must penetrate deep indoors and underground for many use cases, such as mining

Low cost: affordable device and low operational cost necessary to create a business case with high volumes

Scale & density: networks must easily scale to handle a huge number of devices as use cases grow

Performance flexibility: networks must be able to handle multiple applications with differing performance requirements, e.g. for latency and throughput

Figure 3 Key requirements for massive IoT networks

2.2 TECHNOLOGY OPTIONS FOR MASSIVE IOT

2.2.1 MASSIVE IOT: WIDE, DENSE OR BOTH

Traditionally, IoT use cases with a large number of connections have been primarily addressed by cellular M2M technology. While traditional cellular M2M networks provide high quality and secure connectivity solutions for enterprises to connect their high value equipment or data collection points, enterprises have been seeking out cheaper and more efficient alternatives to connect a wider set of less critical devices. This has led to the emergence of new technologies in the last few years, such as Sigfox, LoRa and NB-IoT.

These new technologies have been optimized to provide excellent range while lowering power consumption. They are able to connect tens of thousands of (mostly dormant) devices, covering hundreds of square kilometers, using just one base station or gateway. As a result, they provide a highly cost efficient solution for connecting a large number of devices, deployed with moderate density (up to a few hundred nodes per square kilometer), in a very wide area, using a small number of base stations/gateways.

While these technologies are well suited for many existing IoT applications with devices deployed over a wide area, there is also a growing need to address use cases with even higher densities. As the available technologies allow for increasing numbers of devices to become connected, we will see more and more dense applications appearing across all verticals. These will evolve towards massive IoT, with increased communication between devices and higher density levels than we have ever seen before. For instance, the continuous proliferation of connected devices in smart cities, or the massive concentration of connected bikes at a festival event in Shenzhen[4] would require the connectivity technology in use to handle an ultra-high density of IoT devices.

It is possible to support a higher device density with the technologies mentioned above by densifying the network infrastructure, but this would increase the cost, and to some extent contradicts their value proposition of being able to provide wider connectivity for less. Besides, while NB-IoT and other cellular solutions have the possibility of dedicating more licensed spectrum to provide the necessary capacity for IoT applications, Sigfox and LoRa, relying on the limited spectrum available in the unlicensed bands, will have constraints due to interference from both internal and external sources.

New technologies are being developed to specifically address this need for high density connections. Most notably, 5G has defined Massive MTC (machine type communication) as one of its three pillar use cases (alongside enhanced mobile broadband and ultra-reliable low latency communication). 5G will utilize streamlined signalling protocols and a lean but flexible air interface to facilitate the deployment of massive IoT in ultra-wide areas with ultra-high density. 5G is currently under development in the 3GPP standardization. Commercial deployments of 5G networks are expected to start from around 2020, but it will probably take another 2-3 years before we see mass adoption in developed markets.

Another alternative to connect densely deployed nodes is to use wireless mesh technologies. Wireless mesh is not a specific technology but a family of technologies, including standardized, open source as well as proprietary ones. As the next chapter will describe in more detail, the principle of mesh networks is to rely on peer-to-peer communication between nodes to exchange information or forward data to and from a gateway.

While mesh networks may not have been as widely discussed as some of the other technologies mentioned earlier in the context of massive IoT, they have already been extensively utilized in many industry verticals. For instance, WirelessHART, a mesh protocol for industrial sensor networks, is commonly used to connect sensors densely deployed in manufacturing plants with challenging radio environments.

In the past, wireless mesh technologies have been primarily focused on addressing dense, albeit local, deployment challenges. But recent advancements in networking protocols and the reduced cost of nodes that can support routing functions and long range transmission have greatly enhanced the ability of wireless mesh networks to cover wider areas. By using cellular or other wide area technologies such as LoRa as the backbone that connects the gateways, a mesh network can provide geographical reach for regional or even national deployments with the end nodes extending hundreds of kilometres from the gateway through multi-hop.

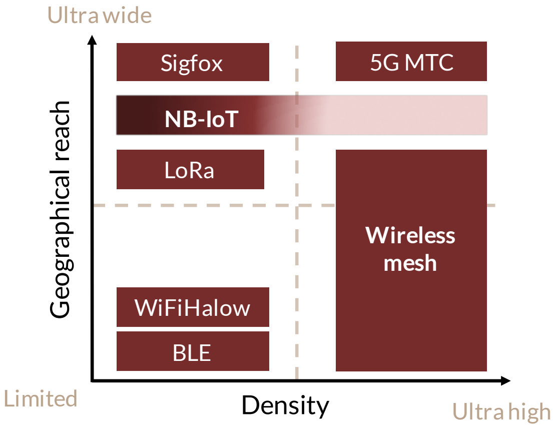


Figure 4 Geographical reach vs. density matrix for massive IoT technologies

[4] Shanghaiist, 2017

Figure 4 illustrates the two main dimensions of massive IoT deployment: geographical reach and node density. The connectivity technologies discussed above are mapped onto this diagram. Their position on the diagram does not indicate the only scenarios in which they can operate, but rather highlights the deployments for which they are optimized, in terms of both performance and cost efficiency.

2.2.2 DIFFERENT OPTIONS FOR DIFFERENT BUSINESS NEEDS

In addition to having a different technical focus, each of these connectivity technologies is also best suited to address different business needs. In particular, the following four aspects are highlighted as the most relevant considerations for massive IoT use cases: global interoperability, adaptability to local requirements, cost and QoS assurance. Figure 5 illustrates how different technologies are best suited to address these dimensions.

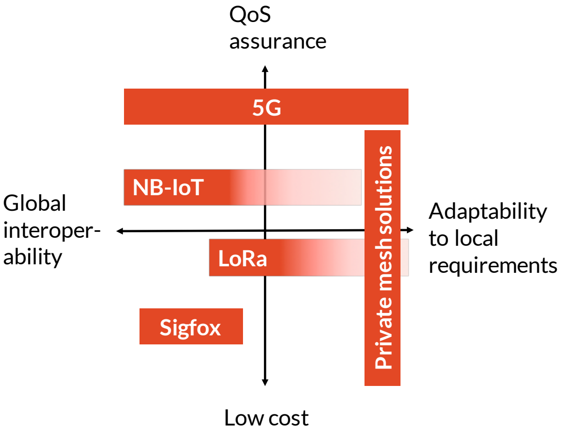


Figure 5 Business consideration trade-offs for selecting massive IoT technologies

From a global interoperability perspective, 3GPP based technologies, such as NB-IoT and 5G, undoubtedly have the clearest advantage, being the output of extensive global standardization processes. Sigfox, as the sole service provider globally (through partnership with local operators), is also able to ensure that all Sigfox devices work on its networks in any country. While only 20% of the global population is covered by these types of networks today, they are predicted to reach 100% population coverage as early as 2022[5].

In addition to the interoperability of these technologies, their operators are often experienced in supporting international business, providing a highly valuable advantage for many enterprises, especially those deploying connected devices on a global scale.

On the other hand, there are limitations regarding the extent to which an enterprise can influence the public network operator to make specific adaptations to its unique requirements, for instance, to improve coverage in a basement or to meet specific service level agreements (SLAs). 5G, however, promises to overcome this limitation and provide flexibility in the service provisioning of cellular networks. This will be achieved through the modernization of core networks and the use of network slicing, which will allocate dedicated network resources into slices, each addressing a specific use case for a specific enterprise. It is expected that this concept will encompass multiple radio access technologies, including NB-IoT.

At the other end of the spectrum, wireless mesh technologies have been mostly deployed as private networks for specific solutions. Though there are a few standardized and open source options, it is a fragmented space with no dominant global solution. This has not been a major hindrance for the use of wireless mesh technologies, as most deployments have been either local or regional. However, the interoperability issue may become a challenge for mesh technologies to gain more traction in larger scale deployments.

LoRa employs an open standard for its network layer, and can therefore be deployed as either a private or a public network. But due to its highly customizable nature, the interoperability between different network implementations is not guaranteed.

On the vertical axis, the enterprise often has to make a tradeoff between QoS assurance and lower cost. From the total cost of ownership perspective, one needs to take into account the device cost, connectivity/subscription cost and network operation cost, if employing a private network solution. The QoS assurance is not only about the throughput and latency of the connectivity, but also the responsiveness to any outage or interruption in the network.

Cellular solutions typically provide the best QoS assurance, by leveraging their extensive experience in providing enterprise solutions, internal support to handle billing and resources for on-site maintenance. In addition, cellular technologies are also capable of delivering higher throughput with lower latency. This premium service comes at a higher subscription cost (even though NB-IoT promises a lower price point than traditional cellular M2M connectivity), and this is one of the main drivers which leads to the emergence of other low cost options like Sigfox and LoRa.

The low cost options, especially Sigfox, have reduced the device complexity as much as possible to limit its cost, but this is achieved at the expense of much lower throughput and higher latency. It is nevertheless a tradeoff that is attractive for certain massive IoT applications.

[5] McKinsey article, “What’s new with the Internet of Things?” 2017

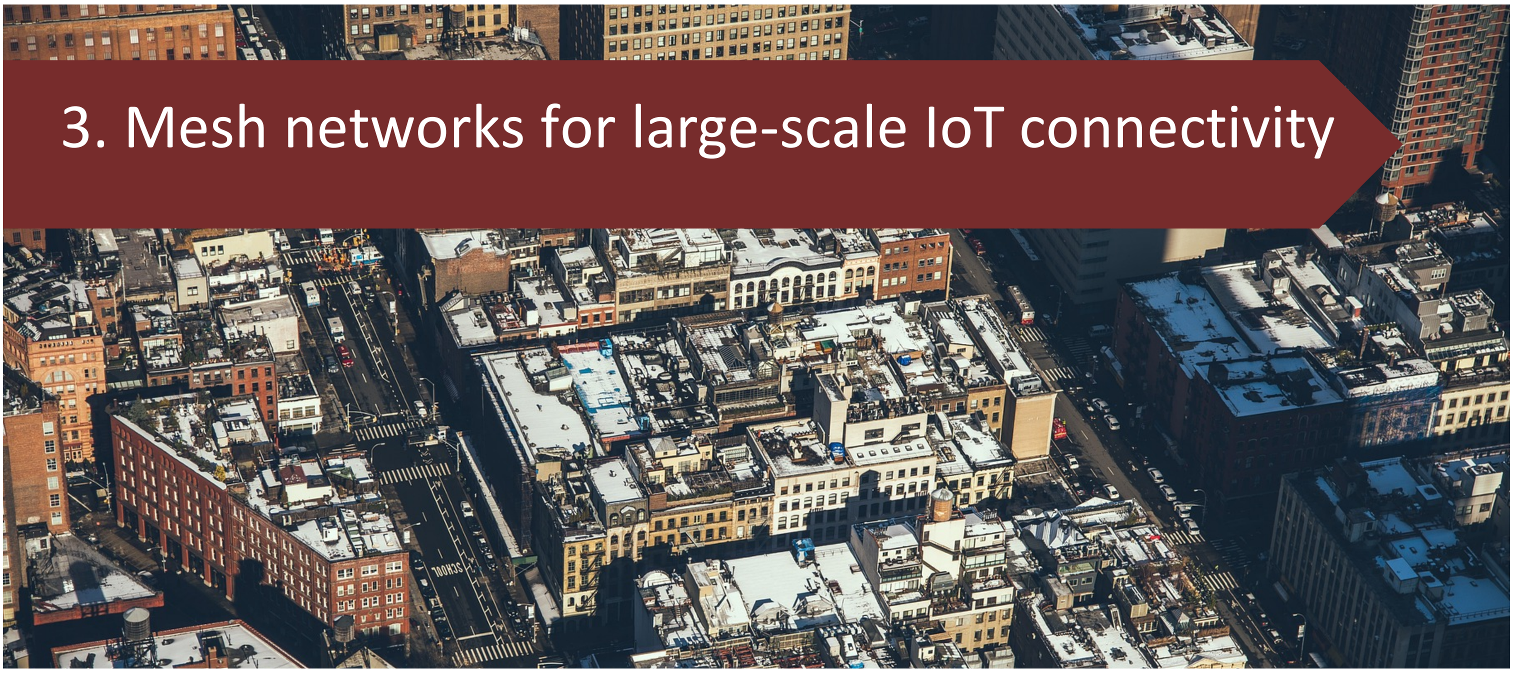
Private solutions, on the other hand, are built based on the specific requirements of each deployment. Multitudes of options exist in the technology, equipment and implementation approach, ranging from complex high quality solutions with expensive devices to cost efficient ones with basic functions. Since most private solutions are implemented by companies that are much smaller than a typical cellular operator, they may lack the necessary manpower in the organization to support the operation and maintenance of the network.

Overall, as illustrated in Figure 5, these technologies are each best suited to address a specific combination of needs for enterprises entering into the massive IoT space. Rather than competing, these technologies are highly complementary to each other. For instance, wireless mesh can leverage LoRa or cellular technologies as long range backbone for gateway access.

It is clear that there is are many different technology options to address a variety of needs. The choice of connectivity technology for massive IoT requires a careful examination of the specific requirements of the use case and the business needs of the enterprise, as well as a good understanding of the relative strengths of each technology option.

So far, many industry analyses have focused on wide area technologies like Sigfox, LoRa and NB-IoT, including Northstream's previous whitepaper. However, little has been discussed on the development of mesh technology. We will therefore describe its key features and how it will meet the requirements of massive IoT in the next chapter.

3. Mesh networks for large-scale IoT connectivity



3.1 DIFFERENT ARCHITECTURES FOR MESH NETWORKS

3.1.1 SEMI-HIERARCHICAL MESH NETWORKS

The origins of mesh networks date back to military research in the early 1990s, resulting from the need for a reliable network which was not dependent on any single node. Today, military forces use wireless mesh networks to connect ruggedized laptops in field operations. About a decade after military research began, mesh networks grew popular within the wireless industry and they continue to be a topic of considerable interest.

One of the early mesh protocols, IEEE 802.11s, was developed in the early days of Wi-Fi as a way to connect Wi-Fi nodes for metro coverage. This ultimately failed due to scalability limitations. Since then, the most popular standards for mesh networks have primarily evolved from IEEE 802.15.4, which was developed with low data rate, low power consumption applications in mind. Notable examples of technologies using the 802.15.4 family of standards include ZigBee, Thread and WirelessHART.

In a similar fashion to the server-client structure which dominates the IP world, IEEE 802.15.4 adopted a semi-hierarchical architecture consisting of dedicated nodes for gateways, routers and end devices. This approach reduces the cost and complexity of end devices, and is well suited for local area deployments, such as home or factory automation. But it also requires some infrastructure planning and installation for network deployments or expansion, which can increase costs and deployment lead time.

One recent development gaining in popularity is to leverage the physical layer enhancement, as introduced in IEEE 802.15.4g, to support longer range and larger scale mesh network deployments – specifically with smart utility networks in mind. Nevertheless, in order to be backwards compatible with legacy devices from the 802.15.4 family, mesh network based on 802.15.4g[6] kept the same semi-hierarchical architecture, and as a result inherited the same network planning complexities.

3.1.2 FLAT MESH NETWORKS

Another approach for supporting longer range, larger scale mesh network deployments is to adopt a fully decentralized or flat architecture, consisting of homogenous nodes, all capable of acting as routers[7] as well as end nodes. This flat, decentralized approach allows the network to be set-up autonomously, with minimum pre-planning to meet capacity requirements. This approach also results in a robust network, as there are multiple possible connection paths from each node to the gateway. The de-centralized architecture moves the intelligence of the network to the very edge, enabling local decision-making for frequency channel and time domain allocation, resulting in better adaptability in a dynamic radio environment. Figure 6 on the next page illustrates the different configurations for connecting the same end nodes using a semi-hierarchical network architecture and a flat network architecture approach.

Enabling each node to act as a router would have led to significant extra device costs when legacy mesh networks were designed, but with the advancement of processing power, efficient software stacks can now be deployed on simple devices, tackling the cost constraints. As a result, flat mesh networks are emerging as an option for a range of massive IoT applications. The sections below illustrate how such a network can be optimized to be a suitable option for large-scale IoT deployment.

[6] E.g. Silver spring network

[7] E.g. Wirepas, TMesh

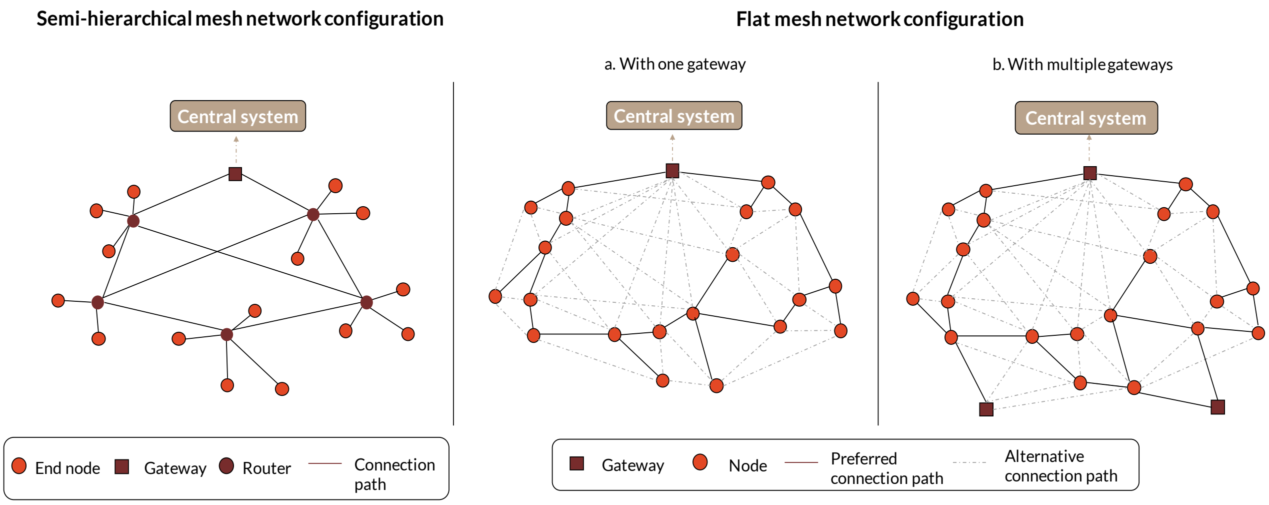

Semi-hierarchical mesh network configuration
Flat mesh network configuration
a. With one gateway
b. With multiple gateways
Central system
Central system
Central system
End node
Gateway
Router
Connection path
Gateway
Node
Preferred connection path
Alternative connection path

Figure 6 Semi hierarchical wireless mesh network configuration vs. flat mesh network configuration

3.2 FLAT MESH NETWORKS CAN MEET THE REQUIREMENTS FOR LARGE-SCALE IOT

3.2.1 SCALABILITY, DENSITY AND COVERAGE

These requirements are usually discussed separately for wireless technologies, but in flat mesh networks they go hand-in-hand. Adding additional nodes further away from the gateway extends the coverage of a mesh network spanning over a large distance. The downside is that relaying messages through too many hops (point-to-point transmissions) along a large distance also limits the capacity of the network.

However, capacity can be scaled up by distributing multiple gateways across the network and configuring the nodes to dynamically choose the best route to a gateway through distributed decision-making. As all the nodes are capable of automatically connecting to new peers and acting as routers, the possibilities for information flow expand compared to a semi-hierarchical architecture, where only certain nodes are routers. The result is a flat mesh network with a self-forming and self-healing architecture, ensuring the scalability and reliability of the network while keeping the cost and logistic complexity of operating the network minimal.

The performance of the network improves as it scales and increases in density, since more neighboring nodes creates more possible connection paths to gateways. On the flip side, as mesh network nodes are typically not equipped with high transmission power or high gain antennas, they would not be able to reach many neighboring nodes in a sparse deployment, limiting the number of possible paths through the network. Consequently, the network may encounter bottlenecks or long chains consisting of too many hops, reducing its overall capacity and reliability.

As a result, flat mesh networks are suited for massive IoT applications, where networks feature many, densely deployed devices.

3.2.2 THROUGHPUT, POWER CONSUMPTION AND FLEXIBILITY

Massive IoT applications typically require very low power consumption to enable long battery life for devices, while the throughput and latency requirements are less onerous. In some mesh networks, nodes can be optimized in terms of operating run time to address specific latency, throughput or energy efficiency needs. For example, a node could be configured to a stand-by power consumption mode if a very long battery life is required, but can also be configured to a high-throughput mode if large packages need to be sent. As another example, CSMA-based transmission could be used instead of a fixed time slotted approach If latency is a high priority for specific nodes.

Network flexibility may be further improved through hardware and software decoupling. An independent software layer may be updated over-the-air to adapt to the new requirements of evolving IoT use cases, without the need to alter the installed hardware infrastructure. This approach would not only improve flexibility, but also reduce running costs of the network over time.

Mesh networks can be energy efficient due to the relatively short transmission distances between nodes compared to star topologies. These nodes generally have a simple processor to further save on power consumption and increase life span. Although the latency of these network tends to be relatively high due to the number of nodes information may have to pass through, they can address massive IoT use cases which are not latency sensitive but require many low-power devices.

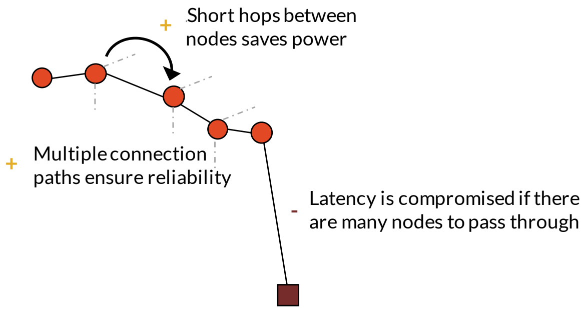

+ Short hops between nodes saves power
+ Multiple connection paths ensure reliability
- Latency is compromised if there are many nodes to pass through

Figure 7 Mesh networks provide reliable and energy efficient networks at the expense of latency

3.2.3 NETWORK RELIABILITY AND SECURITY

As discussed previously, flat mesh networks create multiple pathways to the gateway, allowing the network to self-heal and re-route messages in the event that any one node encounters issues, and thus avoiding any single point of failure in the network.

However, despite these self-healing and re-routing capabilities, the decentralized nature of flat mesh networks also adds a responsibility to oversee the network and monitor its health, as there is no centralized unit to gather this information. This may be done through the application layer, providing the network owner with visibility on the status and performance of the network to ensure reliability.

Although security for IoT services encompasses multiple layers and connectivity is only one link in the chain, security breaches nevertheless pose a serious threat to wireless networks, particularly for networks comprised of millions of distributed devices. Most mesh networks today have employed standard approaches, such as AES128, to ensure the network is secure. Nodes may also be required to have an encryption and authentication key pair to join a network.

While these standard approaches may not be as robust as the SIM card based security system employed in cellular networks, more sophisticated measures can be employed at the network owner's discretion – although not without increasing the cost of hardware. Depending on the application, this trade-off between high network security and low cost needs to be balanced. Over-the-air update capabilities also play a key role in ensuring a network remains secure over time and capable of fixing any breaches quickly.

In the future, as the processing power to device cost ratio continues to improve, flat mesh networks can leverage their decentralized architecture to use distributed ledger technologies such as blockchain for increased security.

3.3 ADVANTAGES AND LIMITATIONS OF NEW PROPRIETARY SOLUTIONS

New proprietary solutions for mesh network connectivity are able to build an innovative network architectures from scratch,. As a result, companies developing these new, lean mesh protocols are able to create simple solutions which are easy to install and have a quick time to market. The speed of development cycles with these new mesh protocols allows them to quickly adapt to the changing needs of the industries they serve, further aided by OTA updates in the field.

These features are well suited to address newly emerging IoT use cases. However, there are also some limitations to the clean-slate approach employed by new proprietary solutions. They lack interoperability with other mesh solutions, and due to their smaller ecosystem, their sustainability is less certain. However, building an ecosystem of partners working with IoT platforms, modules, gateways and chipsets will allow creators of new mesh network protocols to accelerate business development and product creation. In addition, certain mesh solutions have decoupled the software layer from the hardware and thus enable the protocol to benefit from the economies of scale of any hardware platform, solving the interoperability issues new technologies usually encounter in the process.

As this chapter has shown, flat mesh networks possess many attributes for connecting IoT devices, though they are not without their drawbacks. Table 1 summarizes the characteristics of flat mesh networks, and demonstrates that they do indeed meet the requirements for large-scale massive IoT, as set out in section 2.1.

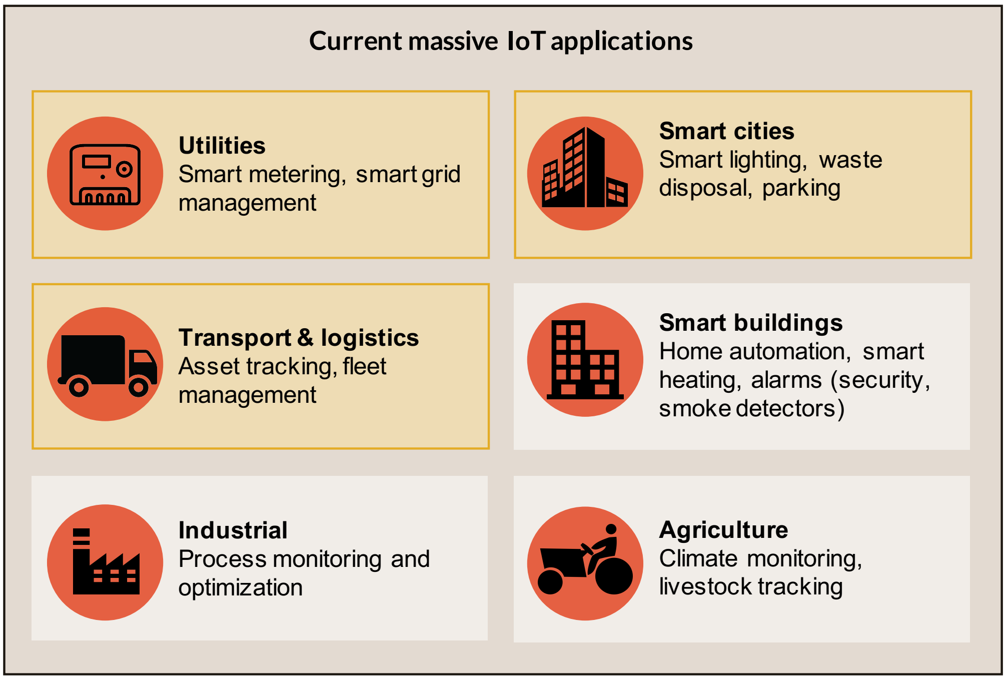
Strengths	Weaknesses
+ Performance flexibility	- Not optimized for sparse deployments
+ Highly scalable	- Lack of interoperability
+ Support for dense networks	- Less mature ecosystem

Table 1 Strengths and weaknesses of flat mesh networks for IoT

4. Use cases

Massive IoT spans a range of applications, from utilities monitoring to industrial process optimization. This chapter discusses three specific application areas within massive IoT: asset management, lighting infrastructures for smart cities, and smart metering. It outlines the benefits of deploying IoT solutions in these three areas, as well as the technology requirements for each one.

The application areas discussed in this chapter are also illustrated through specific use cases, which were provided by Wirepas, a provider of proprietary mesh network connectivity. Each enterprise deploying an IoT solution chooses a specific connectivity technology based on the IoT challenges it faces and its key connectivity needs. For each of the following use cases, Wirepas discusses the IoT challenges the company faced, along with their choice of technology and the results so far of their IoT deployments using wireless mesh technology. Figure 8 highlights the three IoT areas discussed in this chapter.



Current massive IoT applications

Utilities
Smart metering, smart grid management

Smart cities
Smart lighting, waste disposal, parking

Transport & logistics
Asset tracking, fleet management

Smart buildings
Home automation, smart heating, alarms (security, smoke detectors)

Industrial
Process monitoring and optimization

Agriculture
Climate monitoring, livestock tracking

Figure 8 Selection of IoT use cases

ASSET MANAGEMENT

This application area covers the management of both fixed and mobile assets. For fixed assets, such as water pumps, vending machines, etc. connectivity offers an enterprise better visibility of their assets, including condition and usage. This allows them to improve their efficiency by optimizing usage, and to reduce costs and down time through predictive maintenance. For the asset manufacturers, connectivity provides data on how they are being used, which allows them to improve their products and offerings, and also provides an opportunity for them to transform their business models, for example turning their product into a pay-per-use service. For mobile assets, these benefits expand to include remote tracking. Enterprises can better manage and optimize the use of mobile assets if they have real time information regarding their whereabouts.

Typically, the assets would send small amounts of data at set intervals, so high data rates are not always necessary. However, as this application can span countless devices in both urban and rural areas and, in the case of mobile assets, in changing environments, it requires reliable coverage at a low cost. Due to the mobile nature of devices in asset tracking applications, the networks supporting them may become very dense at times. For instance, connected bicycles in a city bike-sharing scheme would usually operate in a relatively sparse network, even in huge cities. However, if a big event occurs in one part of the city, all of the bikes may congregate there, drastically increasing the density of the network.

CASE STUDY: EUROPEAN POSTAL COMPANIES

This case study is provided by Wirepas

About the use case and its IoT challenges

Several leading European national postal services decided to implement an IoT solution for asset management to tackle the challenge of underused trolleys in circulation. By monitoring the trolleys, their target is to optimize trolley use and reduce the overall number of trolley fleets by 20-25%.

Key connectivity needs

The post offices required a connectivity technology which could create a reliable network in a challenging environment for radio propagation. Several different technologies were tried, but network reliability remained an issue.

Technology choice and deployment results

Wirepas connectivity was chosen, and is providing reliable coverage in the postal services' operating environments. The solution offers bi-directional communication and location information without a fixed infrastructure, reducing the deployment costs.

The most advanced organization is currently in the third phase of their asset management pilot, with 100 trolleys currently connected, and the commercial phase is about to kick-off.

WIREPAS

SMART CITY - STREET LIGHTING

Governments are implementing smart city initiatives to improve public services and the quality of life of residents, to optimize the use of resources and to monitor the city's infrastructures. There are many different use cases within this application, such as street lighting, smart parking and waste management. With street lighting, smart lighting infrastructures can adapt to street traffic by dimming when no activity is detected and brightening when movement occurs. This set-up considerably reduces energy usage, improves road safety and can minimize maintenance costs through remote monitoring and management of the lighting infrastructure.

This application requires a long battery life and a low cost connectivity solution, especially as it is generally a government-run initiative using public funds. As part of the broader smart city application, which includes many use cases each with tens of thousands of devices, a connectivity solution for street lighting must be able to handle a very dense network, and must be highly scalable, as new devices are constantly added to the network.

Today, there are approximately 304 million streetlights worldwide, expected to grow to 352 million by 2025[8]. Once every street light, meter, traffic light, parking structure, waste disposal unit and more become connected, these 304 million street lights will become part of smart networks which count millions of connected devices inside each city.

CASE STUDY: HAVELLS

This cast study is provided by Wirepas

About the company and its IoT challenges

Havells is one of the largest electrical equipment companies in India. They were seeking a reliable wireless connectivity solution for their street lighting application.

Key connectivity needs

The lighting manufacturer was looking for a connectivity solution that would scale to large numbers of nodes given the size of many Indian cities. Reliability in the face of changing RF conditions was also a must. Having evaluated alternative connectivity approaches, none of them met the demanding KPIs required to meet the challenge of bringing smart street lighting to India's cities.

Technology choice and deployment results

Havells deployed Wirepas connectivity operating in the sub-gigahertz frequency band. Currently in field trial, the initial performance is in line with the demanding KPIs established by the customer. Automatic configuration and self-healing properties of the network have been extensively tested to ensure that the lighting installations can quickly recover in the event of a power loss, which can happen from time to time.

Havells has been able to run luminaire control in low latency mode while smart city sensor applications (e.g. parking, air quality) operate in the same network on energy efficiency mode to prolong battery life. By using a single lighting infrastructure for multiple applications, Havells benefitted from CAPEX savings and easy scalability.

WIREPAS

[8] Northeast Group, "Global LED and Smart Street Lighting Market Forecast 2016-2022"

SMART METERING

Smart metering applies to water, gas and electricity meters. By connecting their meters, companies are able to receive regular and automatic reader updates. This significantly reduces costs compared to traditional meters, which require monthly estimates or visits from meter readers. The regular data they provide also makes it possible to use resources more efficiently, and for companies to employ dynamic pricing models based on demand. As meters have long life spans, they require a connectivity technology which guarantees longevity. They may be placed underground (e.g. sensors in sewers) or in other hostile environments, and as a result require strong coverage capabilities. Additionally, if the meters do not have access to an electricity supply, as is often the case for gas and water meters, they require a long battery life.

Smart meter rollouts are increasing across Europe, as the European Union has requested that all member governments consider deploying them to upgrade ageing systems and tackle climate change. In the UK, the government's aim is to have 53 million smart electricity meters installed by 2020[9]. When water and gas meters are also included, the UK will have a dense network of connected meters, especially in urban areas with many households, like London.

CASE STUDY: AIDON

This case study is provided by Wirepas

About the company and its IoT challenges

Aidon is a leading smart meter manufacturer and solution provider. The company has contracts in place to implement electricity smart metering solutions with many Scandinavian utilities companies and was seeking an IoT technology to provide the connectivity for their smart metering solutions.

Key connectivity needs

Aidon required a technology that was reliable and cost effective, and which would allow them to build a solution where a cellular subscription was not required for every meter deployed.

Technology choice and deployment results

Aidon chose to implement Wirepas connectivity and has secured contracts for over 1.2 million metering points in Scandinavia. The largest single installation of their RF mesh topology powered by Wirepas is with the utility company Hafslund in Norway, with 700,000 metering points in a single mesh network. Roll-out is on-going. When completed it will be the largest mesh network ever deployed.

With their IoT solution, Hafslund and Aidon have been able to reduce the number of meters requiring cellular connectivity down to one meter per several hundred, reducing the total connectivity costs over the lifetime of the meter deployments. Aidon has also been able to offer their customers decreased communication costs and installation times for the smart meters.

WIREPAS

[9] Smart Energy GB

5. Future outlook

IoT is already well established across many industries, and more and more devices are being connected as new industry verticals join the journey of business transformation through IoT. However, the connections and applications we are witnessing today are just the tip of the iceberg. The number of IoT devices deployed is expected to grow exponentially, and we can expect to see an increasing amount of direct communication between devices as well. In the future, many new applications will join the ranks of massive IoT, and the number and density of connections will far outpace any deployment today.

As discussed in previous chapters, there are several connectivity technologies addressing large-scale IoT deployments, from traditional cellular, to emerging long range solutions like NB-IoT and Sigfox, and to mesh networks for high density deployments. These technologies have different technical characteristics, each with its own advantages and focus best suited to different segments within massive IoT applications.

In fact, rather than competing with each other, these technologies can be highly complementary. For instance, the proliferation of long range technologies like NB-IoT or LoRa can provide better backbone connectivity for mesh networks to reach wider areas (akin to the concept of capillary networks coined by Ericsson[10]). Similarly, non-cellular technologies like mesh networks are opening up more industries and enterprises to engage in IoT, and these would otherwise be difficult for cellular operators to serve. This, in turn, may create more opportunities for cellular connectivity as the overall demand for IoT continues to grow.

In the long run, 5G aims to provide the technical capabilities necessary to meet the key requirements of massive IoT for extensive coverage and ultra-high density, and to provide the business flexibility for operators to offer customized SLAs for different enterprises and use cases. 5G is expected to become commercially available sometime after 2020, and in the meantime enterprises seeking a massive IoT solution may consider employing a combination of connectivity technologies, leveraging their complementary strengths to meet the challenging requirements. Correspondingly, cellular operators could also benefit from embracing multiple technologies in order to be able to offer a comprehensive massive IoT solution package for their enterprise customers.

[10] Ericsson, "Capillarty Networks – Bridging the Cellular and IoT Worlds"

Northstream™

ABOUT THIS PAPER

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

While Wirepas commissioned the white paper and provided the use cases in chapter 4, all opinions expressed in the rest of the text are entirely Northstream's and do not necessarily represent the opinions of Wirepas.

ABOUT WIREPAS

Wirepas is focused on providing reliable, optimized, scalable and easy to use device connectivity for its customers. Wirepas Connectivity is a de-centralized radio communications protocol that can be used in any device, with any radio chip and on any radio band. With Wirepas Connectivity there is no need for traditional repeaters because every wireless device is a smart router of the network. The connected devices form the network – easy as that. Wirepas has its headquarters in Tampere, Finland and offices in Australia, France, Germany, South Korea, the UK and the United States.

www.wirepas.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 analyses, 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