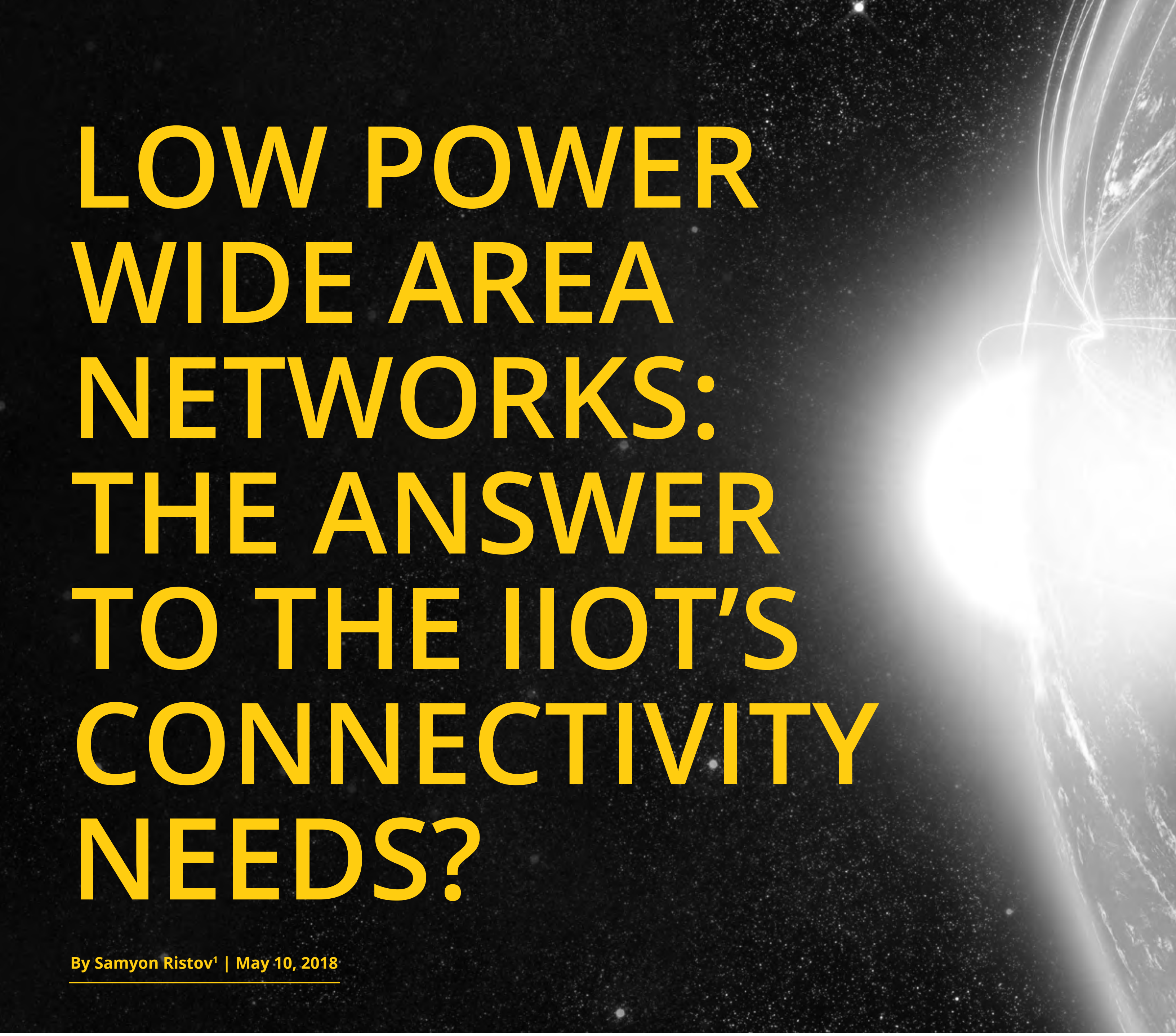

LOW POWER WIDE AREA NETWORKS: THE ANSWER TO THE IIOT'S CONNECTIVITY NEEDS?

By Samyon Ristov[1] | May 10, 2018

Low Power Wide Area Networks (LPWANs) are a family of wireless telecommunication networks designed to facilitate low power, low bitrate communications between network endpoints and servers.

In the industrial variant of the IoT, the IIoT, this emerging class of communications networks has generated widespread excitement for its ability to affordably connect large networks of 'things' (such as battery-operated sensors) to systems used to monitor and control industrial processes (such as Supervisory Control and Data Acquisition, or SCADA, systems).

More importantly, LPWAN networks have enabled industrial operators to begin leveraging the benefits of IoT systems before commercial rollouts of telco-operated cellular IoT networks such as NB-IoT have become widely available. By doing so, they have become more than a stop-gap on the journey towards cellular IoT and have emerged, instead, as viable IoT communication technologies in their own right - now vying with NB-IoT for supremacy as the world's preeminent IoT communication technology.

LOW POWER WIDE AREA NETWORKS: THE CONCEPT

LPWAN technologies have been designed to serve the needs of operators requiring ultra low volume data transmissions (typically those not exceeding 1MB per month). As wide area network (WAN) technologies, they are expected to be capable of sending information over long distances, even within urban environments, which are more challenging than rural landscapes for non line-of-sight radio transmissions to transverse.

Due to high receiver sensitivities, LPWAN networks are theoretically capable of broadcasting over long ranges in open environments and shorter ones in the dense 'concrete jungle' landscapes that characterize most urban areas.

When operated in optimal line-of-sight conditions, the signals of some LPWAN networks can theoretically extend for dozens of yards. Given more realistic, real-world conditions of environment and landscape, however, base stations need to be installed every few hundred metres to ensure that adequate network connectivity is achieved.

'LPWAN networks' – at least when the classification is being used to distinguish them from cellular ones[2] – refer to those communication protocols that transmit over frequencies on the unregulated part of the radio spectrum. These are frequencies the allocation procedure of which is not overseen by communications agencies. Nevertheless, so long as they adhere to basic communication regulations and best practices their existence is generally not actively contested by regulatory authorities.

In the United States, for example, frequency distribution is supervised by the Federal Communications Commission (FCC). Worldwide, agencies such as the FCC work to ensure optimal network conditions by stipulating operational requirements such as maximum transmissions durations, spacing allocated frequencies on the spectrum at intervals that avoid interference, and limiting output power. While these limitations are necessary to ensure the operation of a busy multi-tenant network, they also create somewhat restrictive operating conditions which may be difficult for those using them for both established and emergent IoT use cases to work with.

The unlicensed frequency bands in which LPWAN networks operate include the ISM (industrial, scientific, medical) RF bands and are clustered in ranges not in use by other radio operators, including telecommunications providers, emergency services, and broadcasters. Other LPWAN technologies, such as Weightless, operate their frequencies in TV whitespace (TVWS), the range of frequencies formerly reserved for analog television broadcasts. In contrast, cellular IoT networks, such as NB-IoT, are fully licensed and operate 'in band' within regulated radio spectrum.

Irrespective of the technical nuances of the particular implementation, LPWANs have quickly emerged as powerful forces in the race to connect as many 'things' as possible in the burgeoning global IoT ecosystem.

> ***Irrespective of the nuances of the implementation, LPWANs have emerged as powerful forces in the race to connect as many 'things' as possible in the burgeoning global IoT ecosystem.***

LPWAN technologies have done this by offering a cost proposal that often exceeds what the slower-moving cellular IoT ecosystem is capable of offering. While cellular networks must adhere to internationally agreed-upon telecommunications regulations and the fixed standards development process of the 3rd Generation Partnership Project 3GPP consortium, LPWAN networks can sprout anywhere that a prospective network operator chooses to install a

LPWAN networks transmit over unlicensed radio spectrum, including the TV whitespace left over after the transition from analog to digital television broadcasts.

base station - provided, of course, that they have the necessary technology to ensure reliable communication between control center and endpoint. The overall development of the cellular ecosystem has therefore been slower than that of LPWAN, led by the more agile startup-heavy list of technology providers that dominate the space and its various sub-ecosystems.

Despite some of their limitations and the comparatively meager financial resources at their main proponents' disposal, the global appetite for LPWAN connectivity has remained impressively robust and can be expected to remain so over the short to medium term. Some market forecasters, such as Machina Research, have estimated that by just 2022, 1.4 billion smart devices will be connected through its family of protocols alone[3].

The following overview of the LPWAN IoT connectivity market and its main technologies seeks to empower those responsible for evaluating IoT communication technologies by offering a perspective from a company supplying operators in the industrial segment as to how the LPWAN technology family can be expected to continue to grow and evolve over the coming years.

Specifically, this white paper seeks to provide answers to the following questions, among others:

Which LPWAN networks are leading the ecosystem in its race against the many alternatives it is pitted against (including cellular and mesh networks as well as other platforms in the LPWAN ecosystem)?

Why, at this early stage, while the technologies remains unstable, fragmented, and unpredictable in their future trajectory, are non-regulated LPWAN networks already being adopted by operators instead of cellular offerings, such as NB-IoT?

Is the battle between non-regulated LPWAN networks and NB-IoT a binary duel at all or can the two coexist in a future in which operators' choice of network is largely determined by use-case and deployment size?

CELLULAR IOT OPTIONS: NB-IOT AND CAT-M

Before describing the leading LPWAN connectivity technologies and their respective merits, it is important to understand the state of play in the regulated cellular IoT world whose market share these networks are hoping to capture.

Narrowband IoT (NB-IoT, also Cat-M2 and Cat-NB) and LTE Cat-M1 (often now referred to simply as 'Cat M') are two IoT-specific networks that are based on release 13 of the 3rd Generation Partnership Project (3GPP) evolution of network protocols.

NB-IoT has been described as the "clean sheet" 3GPP initiative to create an IoT-specific network that economizes on data throughput in order to deliver maximum battery life performance for field devices. It is delivered 'in band' within a spectrum block that was initially reserved for Long Term Evolution (LTE) use.

After a period of uncertainty, it has emerged as the cellular network best primed to power IoT devices on a global scale.

Compared to previous cellular 3GPP networks, narrowband IoT's focus is on delivering optimum battery life, connecting a large number of endpoints, and achieving reliable indoor coverage. To achieve this, it has dispensed with many of the functionalities of traditional cellular networks - such as voice and mobility support - that non-IoT "endpoints", such as cellphones, require in order to be useful.

Ironically, the IoT branch of the cellular network family (familiar to most as the 2G, 3G, and 4G/LTE evolution of networks), therefore represents a progressive reduction in functionality of sorts which simultaneously has the stated goal of facilitating some of the most advanced use-cases in wireless network connectivity. This is understandable. Whether cellular or LPWAN-based, IoT-specific networks are the first communications networks designed *ab initio* to facilitate the transmission of information between machines rather than between humans.

When the 3GPP codified its thirteenth release, two IoT-specific networks were proposed: NB-IoT and Cat-M1, (often simply denoted as 'Cat-M'[5]). Cat-M has a higher peak data rate[6] in addition to full mobility support (although the latter is not required in the majority of Industrial IoT use-cases). The two also have different bandwidth (1.4MHz for Cat-M, 200KHz for NB-IoT). Voice over LTE (VoLTE) is supported in Cat-M but not in NB-IoT. NB-IoT/Cat-M2 therefore represents the more pared down of the two variants while Cat-M1 retains some functionalities that certain IoT applications, particularly those in the consumer realm, may require.

Both extant cellular IoT technologies hold substantial promise for those that wish to hitch their deployment hopes on the back of a network family with a proven track-record, not to mention the stability that comes with the deep pockets of the major telecom providers. However, these networks' deployment schedules have lagged behind those of providers in the LPWAN ecosystem and continue to do so in much of the world.

EXISTING LPWAN TECHNOLOGIES: AN OVERVIEW

With total spending on IoT technologies this year expected to amount to billions of dollars[7], there is a striking incentive for private networking technology developers to work towards trumping cellular IoT to become the dominant choice for IoT connectivity – and thereby capture the lion's share of the sizable market revenue at stake.

Industrial network operators have long been clamoring for solutions that will allow them to reliably and immediately connect their dispersed assets to control centers - creating smart cities, among other projects, and tapping into the benefits of these, such as improved operation, reduced operating cost, and better service to customers. Until the advent of LPWAN networks and alternative power sources to keep endpoints running, such assets were often located in areas where neither reliable communications nor stable power supplies were readily available.

Cellular-based networks include both ‘traditional’ varieties, such as 2G/3G/4G-LTE as well as those optimized for the needs of IoT endpoints, such as NB-IoT.

On the other hand, the slow-moving development process of the 3GPP, as well as the need for telecommunications operators to deploy the necessary infrastructure to roll out the technology over stretches of territory that serve entire populations rather than individual deployment sites, have together created a vacuum of unmet demand which an entire legion of companies hoping to develop their own IoT-suitable low-power networking protocols have stepped in to fill.

For these companies, the comparative ‘WIld West’ of the unregulated radio bands have afforded them the ability to quickly develop solutions to meet the needs of those with smart city projects ready to deploy.

In the interest of brevity, this white paper will limit its treatment of the currently available LPWAN technologies to three of the most well-known protocols in common use today: Sigfox, LoRa, and Ingenu.

SIGFOX

Sigfox is a networking technology developed by a French startup that operates over the sub-GHz frequency bands (868MHz in Europe, 902MHz in the US). It is a lightweight data transmission protocol that is heavily optimized for transmitting only the smallest of transmissions and uses Differential Binary Phase Shift-Keying (DBPSK) and Gaussian frequency shift keying (GFSK) modulation technologies to ensure the encoding of transmitted data. It is used to operate IoT networks in more than 60 countries around the world.

Sigfox’s key limitation is that it is effectively an uplink-only technology. This is a crucial limitation for use-cases in which frequent endpoint software modulation is a requirement. Although a limited form of downlink is technically possible, in reality Sigfox is not a suitable choice for network operators that need to frequently change the configuration of their IoT devices on an ongoing basis. This means that Sigfox is not a viable network technology for operators that need to regularly alter transmission frequencies, push hardware and firmware upgrades over the air (OTA), and configure logic-based rules that may need to be frequently changed (for example, once per day). A wastewater operator wishing to change the sampling interval of their devices on an ongoing basis – perhaps in response to the emergence of unpredictable and fast-changing meteorological phenomena such as flash foods – may find that a Sigfox-powered solution cannot meet their technical requirements. Sigfox is, however, a viable option for those with extremely minimal data requirements that do not require a reliable downlink. This group includes many industrial operators, particularly those deploying simple to manage devices such as usage meters.

A second key limitation of the Sigfox ecosystem is that the protocol itself is closed-source. Vital elements of the network’s operation have been monopolized by the parent company. If Sigfox were to go out of business, for instance, projects that leverage its technology would be left without a viable means of achieving network connectivity - theoretically with immediate effect. Although Sigfox reaches commercial agreements with manufacturers to develop chipsets for endpoints, the critical parts of its technology stack remain proprietary. Finally, its closed-source nature mean that achieving sufficient scale to displace NB-IoT once the latter reaches probable future deployment levels will be highly unlikely.

LORAWAN

LoRaWAN (wide area, low-powered IoT-suitable networks based on the LoRa protocol) is also a natural choice for projects with a significant open component. LoRaWAN networks are currently being operated in over one hundred countries[8], making it - alongside Sigfox - the LPWAN ecosystem’s leading technology cluster.

The LoRa Alliance, a collection of more than 500 companies working towards enabling and developing IoT projects based on the LoRaWAN open standard, is a heterogenous group of startups and established technology companies implementing the LoRa protocol (transmitted at 868MHz in Europe, 915MHz in the US). It is based upon a patented Chirp Spread Spectrum (CSS) modulation technology.

LoRaWAN facilitates higher data throughput rates than Sigfox, allowing transfers of up to 300-50,000 bits per second over the sub-gigahertz frequency bands it transmits over (Sigfox, by comparison, only allows 100-600bps). But it suffers from the same drawback on the downlink.

The key limitation, scale-wise, for companies developing solutions using the LoRa protocol, is that only one manufacturer, Semtech, is currently authorized to manufacture the radio component of the network[9]. An operator hoping to provision a truly holistic LoRa-based network therefore has no choice but to work with what LoRa has made available.

Relative to Sigfox, LoRa includes far more robust security features. At the protocol level, it features both network and application security keys. Network security ensures authenticity of the node in the network and application security ensures that the network operator does not have access to end users' application data. To achieve this, LoRa uses AES-128 (Advanced Encryption Standard) security keys and encrypts a unique key to ensure security on the network level. A unique application key is also used to ensure end to end security as well as a device-specific key. Despite these features, some vulnerabilities in the protocol have been exposed[10 11 12]. Given the iterative nature of protocol security development, it can be expected that these will be addressed in future protocol releases.

The open-source nature of the LoRa protocol gives it a clear-cut advantage over Sigfox. Given the multiplicity of companies already offering LoRa-based networks, as well as the fact that it is fully documented online, LoRa can be considered both an open-source and distributed technology. Operators have both a variety of networks to choose from as well as redundancy to rely upon should a particular carrier cease to exist. The door is also aways open to new entrants hoping to develop new LoRa-based networks for use by operators.

INGENU

A lesser-known competitor to the technologies offered by Sigfox and the members of the LoRa Alliance is Ingenu, formerly known as On-Ramp Wireless.

The San Diego-based company offers a proprietary solution that uses a Random Phase Multiple Access (RPMA) technology developed in-house. It operates in the 2.4GHz band, giving it a significantly shorter range than either Sigfox or LoRa but a higher data throughput (and thus shorter battery life). For industrial operators, sensors that support RPMA are significantly more expensive than those designed to work with other LPWAN technologies.

While Ingenu is making headway in supporting various smart city projects, primarily in the US, it lacks first adopter status as well as clear-cut advantages over either Sigfox or LPWAN. The higher battery consumption rate also puts it at a significant disadvantage compared to Sigfox and LoRa.

THE ADVANTAGES OF UNREGULATED LPWAN NETWORKS

The reasons for non-cellular, unregulated LPWAN networks' surge in popularity can, in large part, be attributed to several basic facets of their operation.

Unlike cellular networks such as Cat-NB/NB-IoT that operate 'in band' using commercial cellular networks (whether dedicated IoT versions of those or mainstream offerings such as 4G/LTE leveraged for IoT use-cases without a significant low-power requirement) it is generally free to operate on these unlicensed ranges given the fact that there is no need to pay subscription fees to a licensing authority to ensure connectivity to the network. Naturally, for very large scale implementations, such as those encountered in the industrial domain, this helps create significant economies of scale.

In addition, to incentivize operators to use their technology rather than cellular-based alternatives, chipsets and modules for LPWAN networks are often cheaper than their cellular counterparts. Whereas latest generation cellular IoT modules frequently cost more than $10[13], LPWAN chipsets can often be acquired for a fraction of that.

AN INHERENTLY AGILE ECOSYSTEM

The wide nature of manufacturer partnerships such as the Sigfox Partner Network and the agile philosophy that underpins the LPWAN concept of transmitting over unlicensed radio networks as a whole have also made it the perfect technology to incubate a broad base of manufacturing partners giving rise to platforms that are suitable for very specific use-cases.

Smart water meters, for instance, which require little periodic updating of endpoints via downlink, might be ideal use-cases for a Sigfox-based connectivity architecture. On the other hand, those that want to run an entirely self-operated network without any subscription fees might be better advised to select a LoRa-based networking scheme for their deployment, notwithstanding the limitation that a Semtech radio must be used.

The agile, open nature of the LPWAN ecosystem has also had the effect of encouraging many smaller chipset makers to take a first foray into the IoT market through championing networks that exist outside of the cellular telecommunication networks framework. This, in turn, leads to further diversity in the LPWAN market as protocols are developed to optimize for new hardware. A rapidly iterative development process is thereby initiated: as (I)IoT use-cases continue to expand and emerge, LPWAN connectivity technologies are developed to hone in on and optimize for operators' precise needs. Such a process is simply not possible in the cellular world, where the need to develop standardized networks for cross-continental roll-outs necessarily trumps the desire to develop networks that cater to the connectivity nuances of emergent IoT use-cases.

SUITABILITY FOR THE INDUSTRIAL IOT

The affordability of both the hardware components themselves, as well as the ability to connect a large number of nodes to the network without having to worry about generating a spiralling network subscription budget, also make LPWAN systems particularly well-suited for use in the Industrial Internet of Things (IIoT). The

LPWAN networks can be independently operated and provisioned in locations where cellular coverage does not exist. Smart sewers and oil rigs are two use cases that can take advantage of this fact.

IIoT is a rapidly growing subsystem of the IoT which involves installations that utilize exponentially larger numbers of endpoints than would be encountered in consumer applications.

Deploying adequate monitoring technology to help a wastewater operator remain vigilant enough to prevent Combined Sewer Overflow (CSO) events, or to feed big data algorithms with enough information to pick up on the very first indications of an abnormal operating state, could involve provisioning a far-reaching network consisting of hundreds of water level and wastewater quality sensors.

> ***Deploying monitoring technology to help a wastewater operator remain vigilant enough to prevent Combined Sewer Overflow (CSO) events ... could involve provisioning a network consisting of hundreds of water level and wastewater quality sensors.***

By comparison, a typical use-case in the consumer realm, such as connecting a refrigerator to the internet to deliver periodic updates to homemakers about stock levels, would involve installing and maintaining just a single endpoint connection.

Quantitative forecasts for the growth of the IIoT show that it is expected to emerge as a significant driver of the IoT's overall growth. McKinsey predicts that it will deliver up to $11.1tn. on an annual basis by 2025[14] and touch 43% of the global economy[15]. This means that, for the foreseeable future, operators will continue to afford a high priority to network deployments whose financial overheads are congruous with their scalability objectives.

THE SELF-DEPLOYMENT ADVANTAGE

A second important advantage for operators of non-cellular IoT networks is that provisioning LPWAN-based networks does not depend upon the existence of commercially deployed (and motivated) roll-outs of emerging networks such as NB-IoT. These often involve bureaucratic and administrative difficulties that private operators simply do not have to take into consideration. Together, these can extend their deployment timeframe to as long as two years or more[16]. Additionally, because LPWAN networks can be independently created and operated to various degrees, additional base stations and endpoints can be configured on an *ad-hoc* or as-needed basis. By contrast, an operator hoping to run an NB-IoT-powered project in a location where the network does not exist could not reasonably expect a national telecommunications provider to accede to a request to install a base station solely to facilitate the needs of their particular installation.

For operators rolling out non-licensed LPWAN networks, owing to the large number of nodes that can be connected to each individual base station and the long range of sub-GHz transmissions under typical operating conditions, a vast network of end-points and base stations can be affordably and expeditiously set up without having to involve external stakeholders in the deployment process. No prior telecommunications infrastructure, such as cellular towers, needs to be in place to green-light new deployments. This generally makes the total cost of operating such a network within the budgetary reach of all but the very smallest of operators.

LOW POWER, LONG SERVICE LIFE

Like other IoT-specific networks (and in contrast to protocols such as GSM, GPRS, UMTS, LTE, and 5G that were designed with data-intensive applications such as VOIP and video streaming in mind) LPWAN networks are specifically optimised to facilitate minimum data throughput and offer maximum battery life. This is an ideal set of features to facilitate the connection of endpoints in Industrial IoT networks. Owing to the variety of difficult-to-access places within which they are often installed, such endpoints can only rarely avail of fixed or solar power sources. The advent of edge analytics, in which autonomous logic is placed onboard devices along the network endpoints, synergizes with low bandwidth networks such as LPWANs to provide optimal battery performance.

Unlike those connecting devices through cellular IoT networks, many LPWAN network administrators enjoy the further luxury of controlling the frequency with which they make network updates that also require the updating of modems aboard endpoints.

The prospect of network blackouts due to the sunsetting of commercially-operated legacy communications networks (as is currently happening with 2G and CDMA in the United States) is a threat that those using LPWAN networks largely do not have to countenance – particularly those managing deployments based upon more open source technologies such as LoRaWAN.

> ***The prospect of network blackouts due to the sunsetting of commercially-operated legacy communications networks is a threat those using LPWAN networks largely do not have to countenance.***

The expediencies of the individual remote monitoring project (and when it will be both practical and convenient to spend the money and manpower required to update hardware) is all that needs be of concern to an operator that manages both the infrastructure and the communication network connecting it to the SCADA room. This both increases endpoints' service lifetimes and reduces the lifetime ownership cost of LPWAN devices compared to their cellular-based counterparts, particularly when the reduced subscription budget is considered.

Compared to mesh topology networks such as ZigBee and Z-Wave, LPWANs' benefits are also clearcut.

Mesh networks do not scale well beyond medium distances. High data rates and limited received sensitivities also greatly impairs their available link budgets. In addition, they are heavily inefficient users of battery resources given the requirement to replicate transmissions through other nodes on the network[17].

INTERFERENCE, DUTY CYCLE LIMITS: AMONG LPWANS' DISADVANTAGES

Because LPWAN transmissions occur over the unlicensed parts of the radio spectrum, interference from both other devices and ISM transmissions over the same frequencies are impossible threats to fully obviate against.

Despite the fact that many LPWAN technologies, such as Sigfox, use only a tiny fraction of available radio spectrum, as both LPWAN deployments and network operators continue to grow in number, this may emerge as a significant problem in years ahead. LPWAN networks such as Sigfox allow anybody to create a radio network on a scale that would have been impossible in unregulated spectra just a few years ago.

Unlike MNOs broadcasting on licensed radio frequencies (or VMNOs transmitting aboard their infrastructure) there is no regulatory framework dictating frequency allocation or scrutinizing network plans for conflicts with other operators before approving deployments. In Europe, LPWAN networks are also limited to a 1% duty cycle[18]. Duty cycle limits, which cap the length during which a signal can be active to certain durations or percentages of the day, also exist in other geographies. Quality of Service (QoS) is therefore impossible to guarantee so long as the possibility of network overlap exists both at present and in the future.

Crucially, no major LPWAN network has to date succeeded in achieving significant scale of coverage. Continuing to the present, the LPWAN ecosystem has been largely focused on creating solutions for individual customers. Sigfox, LoraWAN, and Ingenu have struggled to achieve significant adoption beyond localities in which early adopters and startups tend to cluster, such as the San Francisco Bay Area, and places of industry such as important oil and gas sites in the Southern US. Consequently, their deployment levels in localities beyond these areas remains negligible.

By contrast, telecommunications companies typically focus on bringing networks online to entire countries - or at least to the swathes of them that are the most populated. Once NB-IoT rollouts pick up traction, the deployment levels can be expected to dwarf the patchwork adoption levels that have characterized all of the LPWAN ecosystems to date - both major and minor.

CELLULAR AND NB-IOT'S ADVANTAGES

Many commentators are forecasting that the evolution of the IoT connectivity ecosystem will proceed in the opposite direction and are placing their bets instead that cellular IoT networks, primarily NB-IoT, will become the preeminent connectivity technology for the IIoT.

Early deployments have begun to become available at terminal costs of mere dollars. This fact alone makes them a viable option for those seeking to deploy networks in territories covered by their reach. While the cost savings of LPWAN networks over NB-IoT and high-speed cellular networks can be substantial, compared to legacy 3GPP iterations such as 2G, the financial outlay required to provision NB-IoT networks will not likely prove a major deterrent for operators hoping to support use-cases with the more modest end-point requirements encountered in the consumer realm.

Compared to LPWAN, cellular IoT technologies offer support for both the Internet Protocol (IP) layer and the UDP and TCP transport layer protocols. Additionally, NB-IoT (but not Cat-M) supports non-IP traffic. This allows operators to transition between their 2G/3G/4G devices currently in use and NB-IoT devices planned to be used for NB-IoT deployments with relative ease. By comparison, devices using cellular-based technologies that wish to transition to LPWAN networks would need both hardware and firmware modifications in order to remain operational.

Several important concerns with LPWAN networks also remain unaddressed but ripe for solving by cellular IoT entrants. These include latency concerns (owing to their long capable ranges and low power operation, LPWAN networks tend to deliver low data rate and higher latency); security concerns related to operating over unlicensed radio network; and issues surrounding the ability to reliably deliver upgrades to device firmware among the fragmented cluster of current providers supporting the technology. Finally, duty cycling is generally not necessary on most cellular networks, allowing operators to rest assured that transmissions from their devices will be received any time they are sent.

Despite the fact that it requires licensed telecommunications infrastructure to operate, cellular IoT networks also have an important advantage over LPWAN systems in that regard. For telecom providers, cellular IoT networks usually merely represent a software upgrade to LTE that can simply be turned on at existing base stations[19]. By contrast, LPWAN networks must generally have their infrastructure, such as base stations and repeaters, provisioned afresh for each planned deployment.

An often overlooked part of NB-IoT's appeal is the standardization that it offers operators thanks to its codification into a formal standard by a universally recognized telecommunications governing body, the 3GPP.

Finally, the fragmentation that continues to pervade the LPWAN ecosystem will continue to be regarded negatively by many operators that continue to clamor for a universalized technology that 'just works'.

CELLULAR AND NB-IOT: CRITICISMS AND DISADVANTAGES

Some have regarded cellular operators' promise to deliver multi-year battery life through licensed, cellular-based networks as a mere marketing tactic designed to appease the desire of analysts to point to a solution that addresses the deficiencies of the convoluted, fragmented LPWAN ecosystem rather than a substantive answer to IoT users' needs. Or, as a hastily conceived reaction to the realization that 2G networks - now being sunset in many countries - are insufficient to meet the needs of modern IoT network operators.

For others, the fact that cellular IoT (which enjoys the goliath engineering and marketing resources of the global telecom monoliths), appears to have been outrun in the race to develop the first IoT-specific networks to receive large-scale adoption by a loosely formed conglomerate of alternative, largely open-source network providers was something of an embarrassment to the major telecommunications companies and their financial backers. For those that subscribe to such a view, this resulted in the development of IoT-specific networks that are arriving years after the first LPWAN networks became operational and which have therefore failed to adequately cater to their emerging preferences (such as the ability to deliver self-managed networks).

The deployment of narrowband IoT networks, at least at the time of writing, also remains extremely limited on a worldwide scale. Vodafone, for example, only deployed its first NB-IoT network in Spain at the beginning of last year (despite being a vocal proponent of the network and its earliest commercial proponent) while other European countries, such as Ireland, only had their rollouts in early fall[20]. More peripheral geographies, such as New Zealand, are still waiting to be brought online[21].

Given the financial clout of the major telecommunication operators, however, this is a limitation that can be expected to be quickly overcome as demand for the networks continues to grow among operators.

Because LTE forms the base of the NB-IoT protocol stack, in addition to requiring a software update required to make an existing cellular base station operable for NB-IoT, advanced telecommunication networks, namely LTE, need to already be in place before NB-IoT connectivity is even possible. In some, older, base stations, hardware also needs to be updated. This is an impediment to would-be operators in many emerging economies with a strong appetite for IoT growth but limited infrastructural resources with which to deploy a network. Nationwide LTE penetration levels in many countries, among them many potential IoT leaders, remain far from complete.

WHICH WAY IS FORWARD?

Despite the uncertainty among technologists, reasonably probable speculation about the likely direction the

The choice between cellular and LPWAN depends largely on the use case and planned network size. Both, however, can be expected to make significant contributions towards enabling smart city projects the world over.

market will take can already be advanced.

The true answer to the multi-billion device question as to whether cellular IoT or a LPWAN variant will come to dominate the connectivity market is likely that everything depends upon the use-case and the requirements of individual remote monitoring projects. Both will continue to vary widely, particularly during the technologies' early days.

Those use-cases with more demanding connectivity requirements – such as for ongoing two-way communications via uplink and downlink – are unlikely to find any of the currently available LPWAN solutions sufficiently well-developed and tested to satisfy their requirements.

In addition, the bias on the part of many current and would-be operators that networks managed by global telcos are inherently more reliable than those deployed by comparatively smaller organizations will likely prove stubbornly difficult to refute, particularly when the merits of cellular IoT solutions are considered against a backdrop of unstandardized consortia working towards disparate objectives.

However, failing significant modulation to cellular IoT's standards, the most ambitious IoT projects involving the largest number of end-points (which includes, particularly, use-cases drawn from the industrial world) are likely to find LPWAN the more attractive of the two major ecosystems currently in existence. Furthermore, as NB-IoT deployment rates continue to lag, LPWAN networks continue to enjoy a period of artificial market primacy during which they can assert their advantages over cellular relatively unhindered by competing solutions.

Perhaps for this reason, and in an attempt to satisfy as many customers as it is immediately possible to please, many major telecom operators, including notable players such as Orange and Swisscom, have announced plans to roll out cellular and LPWAN offerings in unison. Doing so hedges in the short term against either's long-term succession and caters for as broad a swathe as possible of the often diverging preferences of those hoping to deploy IoT networks as is currently possible.

Irrespective of whether LPWAN or cellular IoT leads the charge into the multi-billion dollar IoT connectivity boom anticipated to occur in the short to medium term, it looks likely that there will be plenty of volatility in store in the market to bring as many industrial resources as possible online.

GLOSSARY

3GPP	3rd Generation Partnership Project. The consortium responsible for the standardization of GSM-based networks.
LoRa	An abbreviation for Long Range. A long range low power wireless platform being promoted by Semtech.
LoRaWAN	LoRa Wide Area Network: the LoRA protocol with both MAC and physical layers.
LPWAN	Low Power Wide Area Network.
LTE	Long Term Evolution a 4G high-speed mobile communications standard.
NB-IoT	Narrowband IoT. An ultra low power iteration of the GSM network family.
TCP/IP	Transmission Control Protocol/Internet Protocol. The basic communications protocol of the Internet.

FOOTNOTES

[1] Senior Engineer, Ayyeka. Ayyeka is a technology company providing ultra low power remote monitoring solutions to companies in the industrial sector.

[2] Cellular IoT networks, such as NB-IoT, are also technically low-power WANs, but are not usually considered under the LPWAN rubric.

[3] https://smartcitiesworld.net/news/news/lpwa-networks-to-lead-iot-connections-by-2022-1348

[4] https://www.link-labs.com/blog/nb-iot-vs-lora-vs-sigfox

[5] a consideration of the previous releases, Cat-1 and Cat-0, is beyond the scope of this white paper

[6] https://www.iot-now.com/2016/06/21/48833-cat-m1-vs-nb-iot-examining-the-real-differences/

[7] https://www.idc.com/getdoc.jsp?containerId=prUS43295217

[8] https://docbox.etsi.org/Workshop/2017/201710_IoTWEEK/WORKSHOP/S04_CONNECTING_IoT/LoRaAlliance_THUBERT.pdf

[9] https://www.iotforall.com/iot-connectivity-comparison-lora-sigfox-rpma-lpwan-technologies/

[10] https://www.elektormagazine.com/news/lorawan

[11] Emerkan, A., Ramachandran, G., Lawrence, P., & Hughes, D. (n.d.). Exploring the Security Vulnerabilities of LoRa. Retrieved from https://lirias.kuleuven.be/bitstream/123456789/587540/1/camera_ready.pdf

[12] Aras, E., Small, N., Ramachandran, G., Delbruel, S., Joosen, W., & Hughes, D. (2018). Selective Jamming of LoRaWAN using Commodity Hardware. Proceedings of the 14th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services. doi:10.4108/eai.7-11-2017.2273515. Available online: https://arxiv.org/pdf/1712.02141.pdf. Also: https://www.elektormagazine.com/news/lorawan,

[13] http://iot.t-mobile.com/telit-announces-cat-1-iot-module-certified-for-t-mobile/

[14] https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/The%20Internet%20of%20Things%20The%20value%20of%20digitizing%20the%20physical%20world/The-Internet-of-things-Mapping-the-value-beyond-the-hype.ashx

[15] https://s3.amazonaws.com/dsg.files.app.content.prod/gereports/wp-content/uploads/2015/09/29153350/Annunziata_Moment-for-industry_Final1.pdf, p3

[16] http://www.vodafone.com/content/index/what/technology-blog/nbiot-commercial-launch-spain.html

[17] http://cdn2.hubspot.net/hubfs/427771/LPWAN-Brochure-Interactive.pdf

[18] https://www.link-labs.com/blog/nb-iot-vs-lora-vs-sigfox

[19] This is true for Cat-M, but NB-IoT is not backward compatible. See: Wang, Y., Lin, X., Adhikary, A., Grövlen, A., Sui, Y., Bergman, J., & Razaghi, H. (n.d.). A Primer on 3GPP Narrowband Internet of Things (NB-IoT). Retrieved from https://arxiv.org/pdf/1606.04171.pdf

[20] https://www.siliconrepublic.com/machines/vodafone-ireland-nb-iot

[21] http://www.zdnet.com/article/vodafone-nz-to-deploy-nb-iot-network-in-2018/