The Value of Carrier-Grade Network Service for the Delivery of LoRaWAN® IoT Solutions

The Best Path to Avoiding the Suboptimal Performance and Pitfalls of Decentralized Hotspot and Developer IoT Networks

A Senet Business White Paper

senet
Connecting the IoT Revolution

Abstract

This white paper addresses the need for clarity on the viability of LoRaWAN® networks for critical infrastructure and essential business Internet of Things (IoT) applications in utility, municipal and enterprise markets. It spells out the requirements for the carrier-grade level of performance such applications require. It also explains how those requirements are being met by the LoRaWAN cloud-based operations platform supplied by Senet, Inc. and in contrast to other approaches which fail to meet those requirements.

Benefits from low-power IoT applications can and should be realized without compromising on Quality of Service (QoS) requirements, project-based Service Level Agreements (SLA's), and technical flexibility. As IoT deployments continue to scale and solution requirements become more predictable, the distinction between carrier-grade Low Power Wide Area Networks (LPWANs) and those that fail to meet carrier-grade specifications is becoming more apparent. This distinction has drawn clear lines between what are defined as commercial and consumer grade networks, with commercial applications for critical infrastructure and essential business needs trending toward utilizing carrier-grade networks throughout their evolution from development to massively-scaled deployments.

Table of Contents

Introduction

Amid surging demand for Internet of Things connectivity delivered by Long-Range Wide Area Networks there's one overarching principle stakeholders cannot afford to ignore:

Critical infrastructure and essential business IoT applications require the support of a carrier-grade network services.

LoRaWAN technology, as defined by the LoRa Alliance, is a version of the IoT communications category known as Low Power WAN (LPWAN), which refers to modes of wireless connectivity where only a limited amount of spectrum is needed to support sensor-based applications generating small amounts of data. Representing what is estimated to be over half the world's IoT connections, the LPWAN device count is projected by one study to jump from about 1.8 billion in 2019 to over 2.7 billion by 2025, at least 1 billion of which will be linked via LoRaWAN technology.[i]

One of the great advantages of LoRaWAN is its adaptability to multiple business models, ranging from supporting a single local application to providing network connectivity for many applications and millions of connected devices on a public network deployed nationally.

Once a LoRaWAN network has been deployed for a particular application, it can easily be densified and made available to support additional applications and a significantly larger ecosystem of participants. There is also great flexibility in terms of the provisioning and management of the gateways (hardware devices that provide wireless access for end devices and relay data to and from the network server) that are employed across that infrastructure to communicate with low-power signal-emitting sensors at distances far beyond the reach of local area and cellular networks. Offering significant ease of deployment advantages, gateways under the control of one or more organizations, can be mounted on buildings, cell towers, light poles and other elevated outdoor structures, or inside commercial or residential buildings, to support one or more IoT applications.

No matter what the gateway configurations and operational engagements might be, when it comes to water and energy utility meter readings, gas leak detection, temperature-sensitive storage monitoring or any myriad of other applications that depend on persistent performance and accuracy, there is very little margin for error. Entities executing those applications do not want to run the risk of being hit by unexpected outages, downtimes for repairs, arbitrary gateway disconnections or any other disruptions common to "best effort" hotspot, shared, and developer LoRaWAN network operation.

If the goal of IoT is to improve systems and processes by connecting real-time data to decision making, the underlying means of doing that has to be predictable and reliable, meaning the LoRaWAN network connecting devices to "smart" applications must support all the communications and functionalities at the performance levels we associate with the term "carrier-grade." Much as traditional telephone networks had to meet lifeline service requirements, IoT networks serving critical infrastructure and business essential goals must be equipped to operate with the end-to-end fault awareness, self-healing redundancy and other quality control mechanisms that are essential to five 9s or better availability, with 24/7 support from customer service and technical teams. Further, networks must be backed by Service Level Agreements (SLA's) that underpin the requirements for the application being deployed, which in most cases are not available from consumer and developer networks.

This is not an out-of-reach aspiration. It's an established fact of Senet's worldwide commercial operations and characterizes all the implementations of IoT applications running worldwide on LoRaWAN networks supported by Senet's cloud-based platform.

In the remainder of this document, we will detail how Senet's turnkey solutions enable rapid, scalable deployment of LoRaWAN networks by integrating all back-end support needed to securely connect, activate, monitor and manage IoT devices. Senet's platform delivers carrier-grade performance in conjunction with any of the business models common to LoRaWAN network operations, whether they're implemented as independently managed networks or via Senet's patented global Low Power Wide Area Virtual Network (LVN™), offering coverage or connectivity readiness in over 80 countries.

Whatever the type of engagement, Senet provides web-based portal access, optimized for network operators, applications providers and standalone Radio Access Network (RAN) businesses of every description, delivering access to the elements of network planning and management unique to their respective market positions. In all cases, users benefit from the full range of monitoring, diagnostic and other functions essential to maintaining carrier-grade operations.

The following discussion begins with an explanation of LPWAN and LoRaWAN technologies in the context of IoT market trends, followed by an in-depth look at the requirements essential to fulfilling the carrier-grade networking mandate.

The focus then turns to an exploration of various QoS-deficient approaches to LoRaWAN services and how they compare to a carrier-grade LoRaWAN infrastructure. This is followed by a deep dive into the Senet cloud services architecture and all the components that go into providing support for carrier-grade operations at minimum costs with reliable ROI across all go-to-market models.

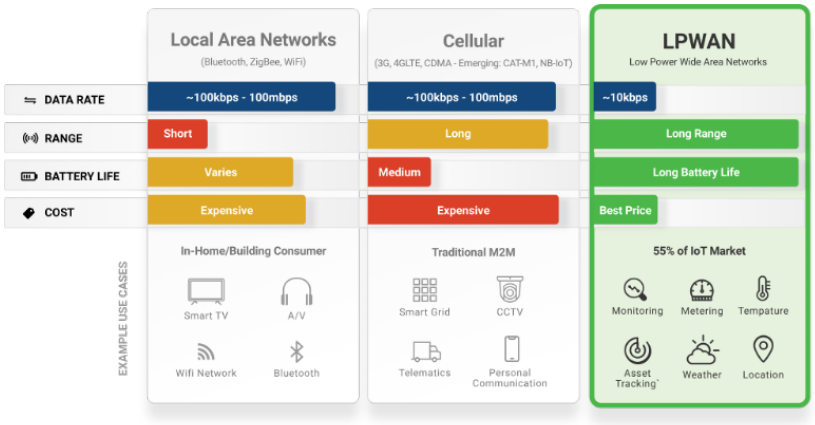
The Explosion in LoRaWAN Market Opportunities

LPWANs and LoRaWAN Technology

Accelerating reliance on Internet of Things applications is driving demand for affordable network support across utility, industrial, enterprise and government market segments worldwide. As a result, Low-Power Wide Area Networks, the class of wireless networks best suited to these needs, are capturing the lion's share of IoT device connectivity at an annual growth rate topping 100%.

The installed base of LPWAN devices, representing over 70% market share of IoT connections, totaled 231 million at YE 2019, a gain of 110% over the previous year, according to researcher IoT Analytics.[ii] LPWAN market value, calculated at about $1.5 billion in 2018, is on course to hit $65 billion in 2025, according to a recent report from Global Market Insights.[iii]

Figure 1.



LPWAN, a term that came into vogue around 2013, applies to wireless networks that use small slices of spectrum to support communications in the 3-375 Kbps range between clusters of usually stationary but sometimes nomadic and even mobile battery-powered sensors and backhaul network gateways. The resulting network, device, and other cost efficiencies help to ensure that benefits derived from IoT applications live up to their billing as net-positive contributions to bottom lines. Figure 1 depicts where LPWAN fits in the pantheon of major network categories.

Four approaches to connectivity comprise 92% of the LPWAN market, according to IoT Analytics. These include:

- Two versions of mobile network technology, Narrowband-IoT (NB-IoT) and LTE for Machines (LTE-M), which leverage unused guard bands from allocated spectrum channels.
- Sigfox, a proprietary multi-national network utilizing unlicensed Industrial, Scientific and Medical (ISM) spectrum.
- Long-Range WAN (LoRaWAN), a protocol under management of the LoRa Alliance® that relies on a spread-spectrum technology, also utilizing ISM, developed by Cycleo, a company now owned by Semtech, a founding member of the LoRa Alliance.

In just five years since release of the protocol, LoRaWAN has become the most widely deployed LPWAN technology, now representing over 50% of the market base, according to IoT Analytics. With over 500 members, the LoRa Alliance counts LoRaWAN deployments in 142 countries with more than 180 million end devices, or "nodes" in LoRaWAN parlance, connecting to over one million gateways as of mid-2020, as tabulated by Semtech.

LoRaWAN gateways, linking to core servers in star topologies over IP backhaul networks, enable bi-directional communications with end devices in multiple application scenarios. There are now hundreds, if not thousands, of unique devices certified to serve as LoRaWAN end devices which typically consist of several sensors, a microcontroller and LoRa radio. A single high-capacity LoRaWAN gateway can support hundreds of thousands of sensor connections.

Unusually low total cost of ownership (TCO) in LoRaWAN deployments rests in part on significant CapEx and OpEx savings stemming from mass production of standards-based devices with low-power consumption that extends battery lifecycles to ten years or more. The long reach of gateway coverage is also critical to lowering TCO through superior economies of scale.

As with any wireless technology, coverage distances vary greatly depending on terrain, tower elevation, presence of buildings and other obstacles, weather conditions and the spectrum tier in use (915 MHz in North America, 868 MHz in Europe). Transmission distances in urban settings extend

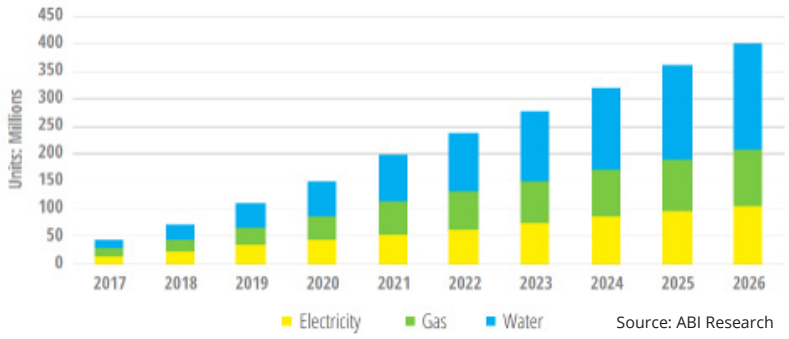
to five miles or more. while distances in exurban and rural deployments routinely reach 15 miles and often run to 35 miles or better.

LoRaWAN Business Flexibility

TCO is also mitigated by the low incremental costs of driving new revenue on a deployed LoRaWAN network. It's possible to continually add end devices and new applications to a gateway coverage area over time, owing to the size of areas served by gateways, the expandable device density per gateway and built-in protocol support for global provisioning of gateways and multiple applications.

The aggregated revenues and business benefits from all the applications tied to a given gateway can add up quickly. This is a big reason why businesses, communications service providers (CSPs) and IoT service specialists have been drawn to LoRaWAN operations with coverage areas ranging from single localities to entire countries, continents and multiple continents.

Figure 2. Non-Cellular LPWA Connections by Smart Meter Type



The fact that every LoRaWAN network is a potential seedbed for ever wider use of IoT technology is especially important when it comes to spawning applications that are beneficial to budget-limited local government operations. Often an IoT initiative mounted by one municipal agency will lead to development of initiatives by other agencies once they see how easy it is to add new applications and end devices to the existing LoRaWAN infrastructure.

Senet's RAN Provider tools and services extend the company's expertise to operators, tower and infrastructure companies, and solution providers, allowing them to perform high-quality RAN designs and deliver carrier-grade coverage and capacity for massive IoT opportunities. Through a unique business model, supported by the economics of the growing IoT market, Senet RAN Provider partners receive up to 50 percent of Senet's monthly contracted revenue generated by the end devices connecting to the Radio Access Network they have deployed. This is a great benefit, but, as shall be seen in Part 2, like everything else related to building successful LoRaWAN business models, individual participation must be managed in accord with the best interests of application users and gateway owners alike.

Another element contributing to LoRaWAN success is support for security rigorous enough to meet the requirements of infrastructures like water, gas and electric metering and monitoring networks that are regulated as critical to national interests. All LoRaWAN networks are accorded protection through end-to-end encryption utilizing 128-bit Advanced Encryption Standard (AES) algorithms with distribution of two types of keys, one related to protecting payload content, the other for authenticating users, devices and other aspects of network operations. More and detailed information on LoRaWAN security has been published by the LoRa Alliance and is maintained on their LoRaWAN Security pages.

The LoRaWAN IoT Applications Landscape

The range of opportunities open to LoRaWAN is vast and growing, fed by ongoing inventions of new ways to put IoT connectivity to use.

A major force driving LoRaWAN proliferation to date has been the utility sector. As noted by the LoRa Alliance, the North American water metering market was one of the first markets to deploy LoRaWAN devices at scale, with hundreds of thousands of connected meters in use by 2019. At the same time, the networking technology has been playing a major role in growing reliance of all types of utilities on LPWAN for their monitoring needs.

As of the end of 2019, utilities comprised the leading LPWAN market segment, accounting for 39% of installed LPWAN devices and on track to maintain that market share through 2025, according to the previously cited IoT Analytics study. Water and gas metering are the leading utility use cases, with water projected to gain an ever-larger share (Figure 2).

ABI Research projects that by 2023, nearly half of the 1.34 billion smart meters installed worldwide on LPWANs will

be used for the water utilities market.[iv] Smart metering in electricity, well-entrenched on other network platforms before the emergence of LoRaWAN technology, is moving to LPWANs, and LoRaWAN for micro-grid management in particular. In all, nearly 20% of smart meters deployed by energy and water utilities worldwide will be connected to LoRaWAN and other noncellular LPWANs by 2026, ABI predicts.

There are many reasons LoRaWAN has become an attractive alternative to utilities' traditional networking approaches for metering and to monitoring their grids, starting with the fact that it is the networking option with the lowest TCO, whether they choose to deploy a private LoRaWAN network or connect to a public network. In addition, utilities, like many other types of entities drawn to LoRaWAN technology, are benefitting from strong OEM support for devices optimized for their use cases. Utilities can easily deploy new applications on the infrastructure, knowing that LoRa Alliance certified devices coming onto the market will interoperate with existing network components out of the box.

Along with measuring usage, a smart metering infrastructure allows utilities to reduce loss and improve safety through leak detection, streamline billing through enhanced flow monitoring, and implement new rate structures to incentivize resource conservation. The two-way communication between a utility and AMI-enabled metering endpoints also delivers additional actionable data to Supervisory Control and Data Acquisition (SCADA) systems, allowing for improved infrastructure diagnostics, advanced data analytics, and the ability to enhance field operations. Further, consumers benefit from behind-the-meter leak detection solutions and detailed information about their consumption which can lead to more efficient resource use and lower consumer bills.

Briefly, here are some of the other market sectors that are contributing to rapid growth in LoRaWAN networking across the globe:

Smart Cities – LoRaWAN-connected sensors are assisting in multiple aspects of municipal operations, including:

- parking and traffic management,
- smart street lighting,
- environmental monitoring,
- road weather information,
- automated irrigation control,
- building safety and security applications such as detection of fire code violations and overlooked locking of doors and windows.

Industrial Production and Manufacturing – LoRaWAN-connected sensors are providing manufacturers visibility into:

- production flow,
- resource utilization,
- machine health and other facets of operations, providing data that is not only specific to each category but that can also be used in the aggregate to analyze overall operational efficiency.

Smart Agriculture – LoRaWAN has made IoT automation affordable to farms and ranches of every description, enabling:

- better control over crop yields through monitoring of soil moisture and pest infestation,
- improved dairy and livestock sales performance through visibility into herd conditions,
- flood and fire risk mitigation by keeping close tabs on points of vulnerability.

Smart Buildings – This is a market with 67% CAGR growth potential for LPWANs through 2025, according to the previously cited Global Market Insights report. LoRaWAN networks are supporting sensors engaged with monitoring of everything that defines modern building operations, including:

- air quality monitoring for occupant safety,
- space usage-based control over HVAC resources and light intensity,
- alerts pertaining to leaks, spoilage, cleaning needs, waste collection and security,
- space usage management using room sensors to help with assignments of conference rooms and offices.

Asset Tracking – LoRaWAN devices play a big role in keeping track of usage and performance of interior and outdoor assets supporting supply chains and other aspects of operations, from storage locations to forklifts, conveyor belts and other location-based equipment, to many aspects of fleet management and the transportation of goods from manufacturing to retail and all points in between. Global Market Insights projects 60% LPWAN CAGR for this category.

Health Care – Another sector with high LPWAN CAGR expectations over 65%, health care requires monitoring of high-risk patients and the systems serving them that often is best served via LoRaWAN connectivity.

Supporting Critical Infrastructure and Essential Business Applications

The Carrier Grade Mandate

These commercial IoT use cases can be served either by private LoRaWAN networks dedicated to in-house needs, through connection to LoRaWAN networks operated by public network operators devoted to serving one or multiple market segments, or a hybrid of both as uniquely offered by Senet. But whatever path to network support any entity might choose, the choice must consider the fact that nearly all applications enumerated above, as well as most others used in commercial operations, are critical to operations.

That means operators of private and public LoRaWAN networks supporting applications for utilities, industries, municipalities or any other segments in the commercial IoT markets must be able to assure network users that they'll experience the quality of performance essential to their needs. In other words, users and providers alike need to be certain they're engaging with a platform that can deliver carrier-grade services.

Following published best practices, it is not all that hard to deploy a LoRaWAN network and connect small quantities of end devices. These steps are all mapped out and supported by LoRa Alliance protocols that can be implemented in the cloud in conjunction with LoRaWAN-optimized end devices, gateways and other physical components and applications that can be readily deployed on LoRaWAN infrastructure.

Developing a platform that facilitates network design, end device configurations, application instantiations, link testing and other steps in a scaled LoRaWAN deployment however, is significantly more complex. The requirements that must be met to ensure carrier-grade performance with the ability to maximize all the benefits of deploying LoRaWAN introduce another order of challenges. As a result, there are many things to look for beyond basic adherence to the standard when it comes to assessing the suitability of a LoRaWAN platform for commercial IoT operations.

The assessment starts with gauging whether the service provider will be able to deliver 5 9s or better performance. This traditional measure of carrier-grade status refers to a provider's ability to guarantee that the network will be available to deliver any user's services 99.999% of the time, which translates to no more than 5 minutes and 15 seconds of downtime per year.

Of course, it's not enough to claim 5 9s reliability. The provider must be able to back it up with enforceable Service Level Agreements (SLAs).

Optimizing Network Configuration and Scalability

At the same time, LoRaWAN service providers need to have the flexibility to take advantage of QoS parameters suited to specific application requirements. While 5 9s availability on the fixed network backhaul portions of the LoRaWAN means all signals will get through with that level of reliability, 5 9s availability on the wireless links doesn't mean that every signal needs to get through whenever an end device generates one. One of the great benefits of LoRaWAN technology is the combination of transmission range and the methodology in which communications from end devices can be "heard" by multiple gateways within range to maximize data collection.

This capability, which maximizes densification of end devices per gateway at minimal TCO, depends on whether users have access to network planning tools that can support mapping of resource allocations with high levels of precision. These tools are essential for use not only with initial coverage modeling but also in future scenarios to enable maximum utilization of the network as new opportunities arise. For example, in the case of a smart city, a LoRaWAN deployment that might begin with support for one area of operations like street lighting, should be available for use in other areas as administrators see opportunities for applications in smart parking, pest control, trash collection, etc.

Network design tools available on the LoRaWAN platform must also provide support for determining optimal placement locations for gateways based on available options such as exterior building surfaces, utility poles, cell towers and other structures.

The LoRaWAN platform should also support both methods of onboarding devices, which can be performed individually or en masse, as defined by the LoRa Alliance's Over-the-Air Activation (OTAA) and Activation-by-Personalization (ABP) join specifications. OTAA bulk onboarding greatly simplifies set-up by pre-provisioning devices and the join controller with address identifiers.

A Comprehensive Operational Framework Accessible to All Stakeholders

Beyond support for setting up LoRaWAN connections and operations, there are many other functions the LoRaWAN platform should make available to those responsible for network operations. For example, network operators should have direct web portal access to tools that can be used to engineer the network to all application requirements, administer and operate gateways and applications, facilitate management of developers, create application provider accounts and populate the network with applications.

Similarly, the platform should provide applications providers access to resources they need, such as tools for mapping applications on the network, controls over end device authorization, activation and de-authorization, and reports on network and device consumption.

And in cases where the LoRaWAN is operated as a public network for use by multiple Radio Access Network (RAN) providers, the platform should enable each to execute provisioning and other management controls relevant to their domains.

Tools Essential to Maintaining Carrier-Grade Performance

The ability to maintain carrier-grade performance across the LoRaWAN infrastructure begins with platform support for automated monitoring and analytics that can trigger switches to redundant paths and other self-healing mechanisms. At the same time, the LoRaWAN platform should provide all stakeholders direct web portal-based access to management tools that allow them to contribute to the steps essential to maintaining carrier-grade performance. Toward that end the system should be able to generate alerts with analysis that can facilitate pre-emptive manual action against emerging outage threats and reduce mean time to repair when outages do occur.

Operations personnel who are responsible for overall network performance should have persistent visibility into everything impacting the health of the network. In cases involving participation of multiple RAN providers delivering LoRaWAN connectivity, each one should be able to monitor their network performance and receive alerts pertinent to their operations with access through customer service portals and reps to backup support from the platform's operations team.

When gateway owners are on the network, they need to have support from tools that generate alerts and trouble ticketing specific to those gateways. And application providers should have access to tools that help them maintain the health of applications and end devices. In these cases, as in all the others, access to such tools needs to be supplemented by recourse to help from customer service personnel.

Multi-Layered Security

Protection from disruption through security breaches is another vital component of a carrier-grade caliber LoRaWAN operation. As noted in Part 1, high level key-based AES encryption security is incorporated into LoRa Alliance specifications and is fully supported by Senet's Join Servers, which serve as the access control authority responsible for authenticating end devices and generating network and application keys.

Access to additional security layers on top of the LoRaWAN security protocol may be required by entities relying on mission critical IoT applications. Consequently, the LoRaWAN support platform should support additional layers of security such as protection against distributed denial-of-service (DDoS) attacks and IoT application-specific security mechanisms from best-of-breed ecosystem suppliers.

Senet combines security inherent in the LoRaWAN protocol with industry best practices for securing IP links on the backbone and additional mechanisms provided by vendor partners. For example, Senet supports applications-layer security through its integration with the IoT security suites supplied by Atos and Thales, both global leaders in digital transformation technology.

Examples of QoS-Deficient LoRaWAN Platforms

In the search for a LoRaWAN platform adequate of supporting the carrier-grade performance required by commercial IoT operations, it is helpful to be able to immediately identify and eliminate from consideration the types of approaches to LoRaWAN networking that fail to meet these requirements. Two approaches in particular stand out as the types of platforms that are best avoided when it comes to supporting critical infrastructure and essential business applications.

Both approaches referenced below employ cloud-based backend support to enabling users of any description, typically an individual, to become "providers" of network service. Anyone can purchase one or more LoRaWAN gateways or hotspots and leverage the platform's set-up mechanisms to link the gateways to end devices supporting targeted applications, either as part of an existing IoT operation or to begin a new one.

The Decentralized Hotspot Approach to Building a LoRaWAN Ecosystem

In one case, in addition to enabling set up of networked applications, devices and gateways, the platform utilizes proprietary iterations of blockchain technology to support transactions covering costs of network usage and payments to gateway owners. All devices and gateways, in addition to being LoRaWAN compliant, must be equipped to support the proprietary mechanisms that facilitate communications and processes related to the platform's blockchain-based accounting system.

The communications between gateways and end devices, along with adhering to LoRaWAN specifications, have a proprietary component that's required to transmit traffic accounting data used in the blockchain payment system. The platform operators make money from charges on traffic generated by the end devices and from the sales of the specialized gateways.

Payments to gateway owners are based on each gateway's tabulation of the volume of data flowing from the connected devices it has been assigned to interact with through the set-up processes. The platform assigns value to those traffic tabulations in cryptocurrency, logging tokens for each gateway owner that can be converted to cash through an exchange that supports the platform's cryptocurrency, the value of which, like any cryptocurrency, fluctuates based on supply and demand.

The platform adheres to basic security and other LoRaWAN specifications for authenticating users and devices. And it provides the provisioning mechanisms along with the cloud connectors that guide alignment of end devices with gateways, backbone routing and linking of specific applications traffic to their associated IoT support systems.

But service providers (typically individuals with no networking experience deploying a single gateway) on the network are left to their own devices when it comes to controlling QoS. The only assistance provided in that regard is a "debug tool," which they can open when something goes wrong to try to decipher what's at issue with traffic linked to a single gateway.

The only way to gain insight into performance across all the gateways under a provider's control is through reference to a mobile app. There's no resource for discovering sources of problems that might be caused by malfunctions farther up in the network.

Once a provider discovers there's a problem on a specific gateway, the effort to find the cause is impeded by the fact that, once the tool is open, it only tracks current messages plus the last ten that were sent prior to use of the tool. Troubleshooting intermittent end devices or gateway malfunctions is a hit-or-miss proposition with a high miss probability.

Such decentralized network architectures may be suited for personal or consumer applications such as pet location tracking, tracking bikes, and in-home DIY solutions, but they do not provide the professional network design and deployment tools or the centralized network management capabilities required for critical IoT infrastructure and essential business solutions.

The DIY Approach Geared for App Developers

Another type of platform takes an alternative DIY approach to drawing participation by individuals and organizations in a public LoRaWAN infrastructure. The heart of the strategy is a network server software consisting of the stack of standardized mechanisms that allow IoT application

developers to set up and operate their own LoRaWAN services.

Users can subscribe to dedicated virtual machine instantiations of the network server that are offered as a service or pay a license fee to set up the server software in their own private or public clouds. There are no fees relating to messaging traffic. It's up to users to set up market-facing business models and back-office support for settlements and other aspects of those business relationships.

Decentralized DIY participation in the community infrastructure through the network server is supported by routing, network discovery, mapping of applications to network components, data management and other functions that are activated in the cloud through open source protocols. Once developers learn the ropes through platform educational resources, they can tap all these elements to set up and manage networked IoT applications utilizing already deployed gateways as well as any off-the-shelf LoRaWAN-compliant gateways they purchase for connection to the network.

Every network "provider" is responsible for locating and troubleshooting problems. The only assistance provided by the platform is an online set of instructions for gateway troubleshooting. Providers are also invited to "reach out to the community" for insight on issues through a network forum set up by the platform provider.

Similar to the hotspot crowdsourcing approach noted above, developer networks are not deployed based on professional propagation studies and network designs with consideration for carrier-grade service delivery at scale. Rather, a single or small number of gateways are deployed by individuals or organizations for application development purposes and lack the centralized network management capabilities required to deliver predictable network coverage and QoS.

Factors Undermining Carrier-Grade QoS

Because these LoRaWAN infrastructures are not purposefully designed to support critical infrastructure and essential business IoT applications, users should be aware of the challenges they may experience.

Beyond the lack of support for remedying device- and network-induced QoS issues, these platforms are vulnerable to issues caused by network upgrades mandated by new releases of platform software or newly discovered bugs in existing iterations, resulting in many hours of network downtime. Further, local network outages may be caused by individual gateway owners who, for one reason or another, may remove the power source from (unplug) their gateways.

In each case, application providers and end users of services connected to these networks lack any guarantee of timely recourse to resolve their network connectivity issues.

Clearly, neither of these types of platforms is suited to providing the carrier-grade QoS that is essential to entities who can't afford to risk anything less. Major requirements to achieving carrier-grade performance as listed in Part 2 are missing, including platform support for:

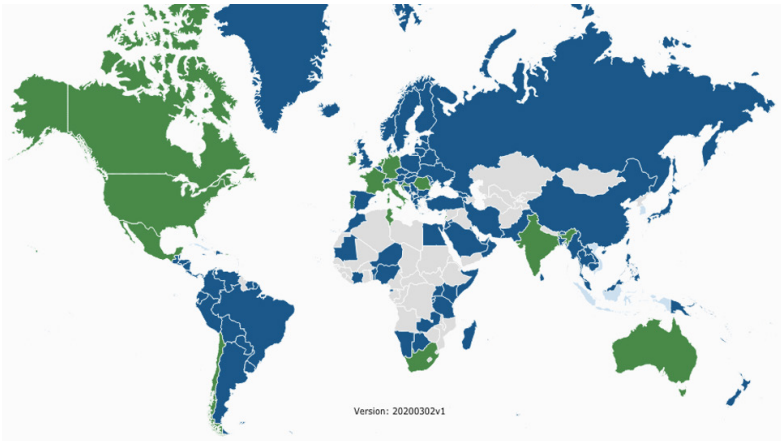
- Set-up processes that minimize chances things will go wrong, including tools for optimizing outdoor and indoor gateway placement and mapping applications and end devices.
- Automated performance monitoring across all points of the network from end devices to gateways to backbone connections to core cloud components.
- Network health analytics that can trigger preventive actions in advance of outages and switchover to redundant paths and devices when outages occur.
- Tools that facilitate troubleshooting by correlating alarms with specific causes.
- Stakeholder visibility into everything impacting network health pertaining to their operations, whether they be LoRaWAN infrastructure operators, service providers in a multi-provider LoRaWAN environment, providers of the applications running on those services or RAN providers lending support to one or more LoRaWAN services.
- Customer service with fully staffed help desks and 24/7 backup assistance from a team of NOC professionals.
- Issuance of project-based SLAs with documentation of performance on all contractual commitments.
- Processes that enable execution of infrastructure-wide upgrades with downtimes lasting seconds, or minutes at most, rather than hours.

Senet's Approach to Carrier-Grade Performance

These carrier-grade performance parameters are intrinsic to LoRaWAN networks supported by Senet. From its founding in 2009 as a full stack IoT solution provider, to its current leadership position as a provider of cloud-based software and services for the on-demand build-out and management of global IoT networks, Senet has focused on creating a LoRaWAN operating environment suited to meeting the QoS requirements of critical infrastructure and essential business IoT applications serving the needs of utilities, municipalities, manufacturers, agrobusinesses and other industry segments. As a founding member of the LoRa Alliance, Senet has taken a leadership role on its board and in committees devoted to formulating specifications and best-practice recommendations.

Senet's cloud-based LoRaWAN operations platform provides turnkey back-end support for everything that is needed to securely connect, activate and manage IoT applications with unlimited scalability and carrier-grade persistence that delivers 5 9s reliability. As shown in Figure 3, the Senet platform is supporting instantiations of LoRaWAN networks all over the world.

Figure 3.



This success is a reflection of the reliability and predictability of performance, the versatility of business models and the efficiencies in network expansion that a growing legion of private and public LoRaWAN network operators and applications service providers have come to expect from the Senet platform. Whatever the anchor application or applications might be with an initial instantiation of network resources, stakeholders know they will have the support they need to continually add new devices and applications to the network at minimal costs.

Solution providers that deliver metering applications on the Senet platform, for example, have activated more IoT devices on their gateways for other applications as well, building new revenue streams and serving other entities' needs. Similarly, city governments that have built out networks to address a specific need find it easy to expand into full smart-city operations as they identify needs to deploy additional applications.

Flexibility in Go-to-Market Models

The Senet platform supports three go-to-market models:

- Senet as a LoRaWAN Network Operator offering Network-as-a-Service (NaaS) connectivity
- RAN Provider Services for network operators, tower companies, municipalities, building owners, and solution providers who desire to deploy their own LoRaWAN gateways
- Managed Network Services for IoT (MNSi™) for network operators offering their own branded LoRaWAN network service

For solution providers, connecting to Senet's Network-as-a-Service (NaaS) is the easiest way to deliver data from IoT end devices to their applications. Senet NaaS provides solution providers with industry leading security, data streaming and device and application management through an intuitive management portal. Carrier-grade service delivery ensures high-availability network connectivity and device operation, and traffic policy service agreements can be customized through individual commercial agreements.

Senet's RAN Provider tools provide network operators, tower companies, municipalities, building owners, and solution providers with everything needed to rapidly design, deploy, and manage carrier-grade LoRaWAN networks (both indoor and outdoor), directly from a dedicated RAN Provider Portal. Alternatively, RAN Providers can contract RAN deployment services from Senet on an as-needed basis, leveraging

Senet's expertise to accelerate time to market and scale operational excellence.

Senet's Managed Network Services for IoT (MNSi) combines all aspects of the Senet LoRaWAN platform into a service that can be utilized anywhere in the world by any type of communications service provider who wants to offer a LoRaWAN network service, whether they be a mobile operator, cable MSOs or other connectivity provider who want to add support for IoT applications to their service portfolios.

Patented Cloud-Based IoT Network Architecture

All models noted above support participation in Senet's patented Low Power Wide Area Virtual Network (LVN), a multinational LoRaWAN infrastructure that enables a wide range of approaches to participating in the IoT marketplace. The LVN leverages Senet's operations platform to support services now available in over 80 countries, including the U.S., where Senet operates the largest public carrier-grade LoRaWAN network.

Providing advantages over historically antiquated connectivity business models, the Senet LVN creates opportunities for organizations across the IoT ecosystem to contribute to the rapid build out of LoRaWAN networks and benefit from revenue sharing based on their level of participation. Under this cooperative model, the Senet LVN delivers pervasive and unified connectivity with standardized global device activation and deployment processes, along with single billing for global device connectivity. Further, any application service connecting to an LVN gateway is fully supported by Senet's network management services without the need for traditional and costly roaming contracts.

The LVN supports new entrants in the LoRaWAN services market, including network operators, municipalities, building owners, and application providers who join through gateways deployed on their assets. Entities joining the LVN have the support of Senet's RAN Provider Services, which supply everything they need to install, register and professionally manage the vast majority of commercially available LoRaWAN gateways.

Unique to the LoRaWAN network market, gateway owners participating in the Senet LVN get a share of the revenue generated from all connected end devices. Those who deploy gateways on the LVN to support a specific application can draw additional revenue from other parties' applications running through their gateways. Revenue shares of up to 50 percent of the fees payed Senet on traffic passing through deployed gateways, depending on level of participation, are paid in cash. This incentive-based model provides extremely efficient, scalable and secure options to connect and manage low power, low-cost sensors at massive scale and simplifies historically complex operations related to application and device registration, message accounting and settlements.

Equally important, from the gateway owner's perspective, the Senet platform allows those who have deployed the gateways for private LoRaWAN networking purposes to prevent access to their gateways from applications running on other public networks. Or they can choose to support some but not all applications in semi-private iterations of engagement.

Being able to securely connect, activate and monitor IoT devices at massive scale, in a multi-tenant and multi-vendor environment, across a broad range of applications, is the new standard for network operators. Operators need to be able to manage the OSS/BSS features of the network server, packet core, data streaming, security, performance of the Radio Access Network and end device adaptive data rates (RF tuning). In addition, the IoT application management environment provided by the network operator must efficiently enable gateway deployment and provide scalable, secure, end-device onboarding, application service provisioning and visualization tools.

Crowdsourced hotspot and developer networks fall well short of these capabilities.

Carrier-Grade Operations Support

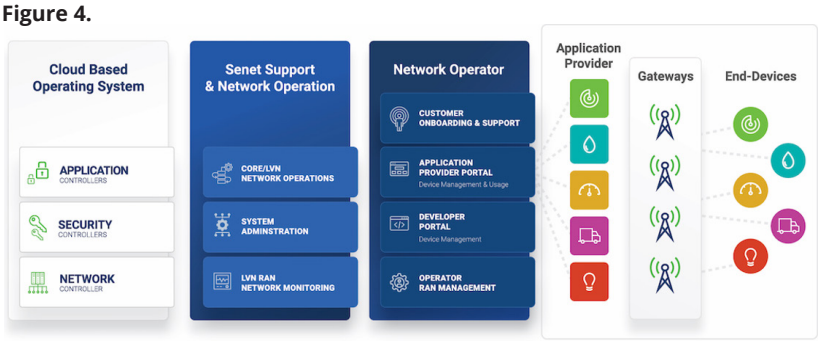
All Senet platform users benefit from Senet's commitment to carrier-grade performance extending to every end device, gateway and link end to end. All elements are continuously monitored with intelligent cross referencing of performance data and alerts to pinpoint causes of emerging as well as immediately disruptive issues.

Automated analytics-generated responses, utilize redundant service paths as needed and convey real-time information used by customer service staff to elevate issues for trouble shooting. Summary reports with alerts are delivered for viewing on user-specific service portals dedicated to network operators, application providers and entities who participate as contributors of gateway connectivity to service providers.

Senet customer service and NOC teams are on call 24/7 with visibility into all networks operating on the platform. With the support of automated analytics, NOC response times and mean times to repair are always fast enough to ensure that every service running on a Senet-supported network maintains better than 5 9s availability over any given timeframe as stipulated in providers' customer SLAs. Reports generated by the platform provide a record of performance associated with each SLA.

This level of performance is made possible by the robustness of Senet's cloud-based global LoRaWAN connectivity architecture and the rigorous analysis applied to configurations of end devices and gateways from the point of initial instantiation through all phases of network expansion. The architecture is designed to enable the ecosystem of connections supported by Senet's Managed Network Services for IoT (MNSi) and Low Power Wide Area Virtual Network (LVN) service models to scale to billions of devices worldwide with no diminution in carrier-grade performance (see Figure 4).

Figure 4.



Comprehensive Support for Planning Network Set-Up and Migration

The management and control point for all Senet-supported LoRaWAN networks is the cloud-based Network Server, which provides the suite of features and task-oriented tools comprising comprehensive OSS and BSS support for all go-to-market models. This is the source for all the functionalities used to monitor and maintain network status, health and performance across all links, devices and applications, including execution of alerts, issue escalations and ticketing.

The Network Server also provides the tools and mechanisms used in network planning, gateway configurations and device provisioning. As a fundamental condition for enabling carrier-grade performance, the Senet platform's network planning tools optimize positioning of elevated high-grade gateways on buildings, towers, utility poles and whatever other structures might be available to platform users for maximizing signal quality and reach of their services. Interior placement of gateways is supported as well, under rigorous stipulations designed to maximize reliability.

Senet platform users also have access to planning assistance that is part of a full suite of planning, deployment and management services provided by Senet operations personnel. The Network Design service component covers all aspects of site selection, RF propagation planning and spectrum analysis.

Precision placement of end devices and gateways based on signal propagation and spectrum analysis makes it possible to build and expand connectivity with maximum efficiency in the utilization of resources. In addition, planning tools aid in the design of networks that deliver LoRaWAN connectivity based on application requirements. With the ability to define coverage areas based on propagation distances supported by externally placed gateways, network planners avoid reliance on small coverage areas and gaps between them that result from depending exclusively on in-home gateways.

Conclusion

LoRaWAN technology has paved the way for long-awaited pervasive use of IoT applications across the commercial marketplace. LoRaWAN networks are providing low-cost connectivity for low-power sensors used in water, gas and electrical power metering and management as well as devices supporting a vast range of IoT applications for municipalities and enterprises worldwide.

A major force behind this expansion is the support for carrier-grade performance provided by Senet's cloud-based LoRaWAN operations platform. Unlike other platforms designed to drive LoRaWAN connectivity, Senet has implemented all the components essential to ensuring critical infrastructure and essential business applications are delivered with 5 9s availability.

These QoS policies apply to all providers, whether they're leveraging the network design, implementation and operations support provided by Senet's Managed Network Services for IoT (MNSi) or delivering applications on Senet's Low Power Wide Area Virtual Network (LVN).

In both cases, Senet's planning tools ensure optimum placement of all gateways and end devices for maximum reach and densification. Once they're up and running, all stakeholders can deliver project-based SLA performance enabled by Senet's support for automated service redundancy, trouble-shooting analytics and 24/7 customer service and NOC technical support.

Entities aspiring to benefit from low-power IoT applications don't need to wonder whether they can exploit the low TCO afforded by LoRaWAN networks without risking sub-optimal performance. The capabilities embodied in the Senet LoRaWAN operations platform make clear they shouldn't expect anything less.

---

i. IoT Analytics, LPWAN Market Report 2019-2025, January 2020

ii. Ibid

iii. Global Market Insights, Low Power Wide Area Network Market to Hit $65bn by 2025, May 2019

iv. LoRa Alliance, Connecting Utility Assets Using LoRaWAN, November 2018

---

senet
Connecting the IoT Revolution

100 Market Street, Suite 302
Portsmouth, NH 03801

Phone
+1 877-807-5755

Website
www.senetco.com