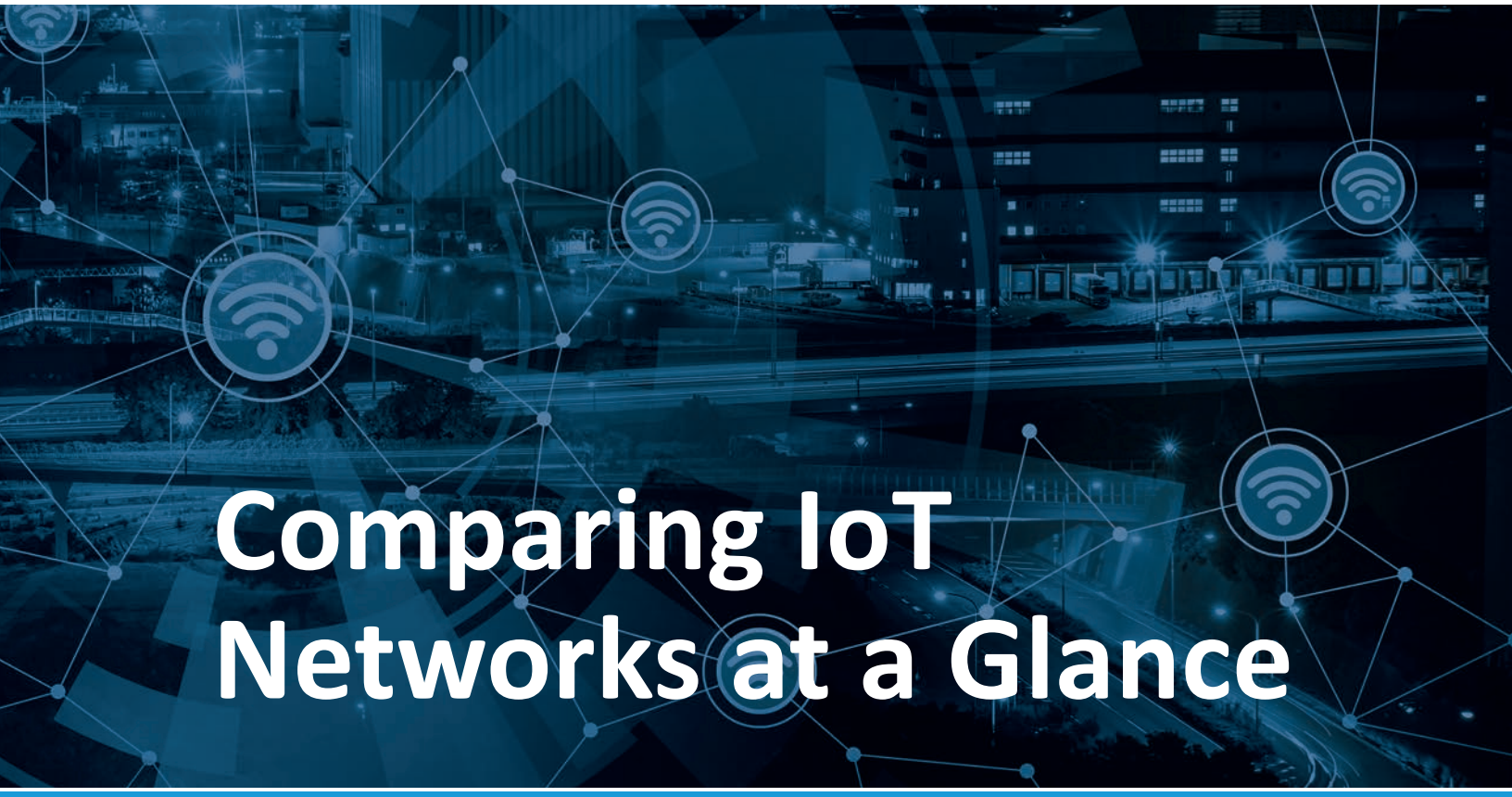

Comparing IoT Networks at a Glance

How Wi-SUN® Compares with LoRaWAN® and NB-IoT

Contents

2 How Wi-SUN Compares with LoRaWAN and NB-IoT
2 Wi-SUN, LoRaWAN and NB-IoT
2 Network Topology and Coverage
3 Communication Performance: Bandwidth, Latency and Bi-Directional Communication
3 Industry Standards
4 Security
4 Provider Ecosystem
5 Power Efficiency
5 Scalability
5 Network and Device Longevity
6 Summary

How Wi-SUN Compares with LoRaWAN and NB-IoT

We live in a world of connected industrial assets, with an unprecedented capability to remotely monitor and control these assets. This is referred to as the Industrial Internet of Things (IIoT). Gartner forecasts that endpoints of the IoT will grow at a 32.9% CAGR from 2015 through 2020, reaching an installed base of 20.4 billion units[1]. The IIoT is not a trend, it is here today and growing rapidly.

If you are planning an Internet of Things initiative then prepare to make a lot of important choices. And in the early planning stages, no choice is more important than the network wireless technology on which you plan to build your IoT environment.

That choice affects everything—from the devices your services rely on to the network architecture that will define your IoT deployment's performance, longevity, reliability, security, interoperability and scalability. When you assess your needs and goals, be certain you make the choice you (and your customers) can live with for years, even decades.

Wi-SUN, LoRaWAN and NB-IoT

In today's marketplace, you can choose from a number of IoT network wireless technologies. Below is a comparison of three major IoT wireless technologies.

Wireless Smart Ubiquitous Network (Wi-SUN) is a technology based on the IEEE 802.15.4g standard. It is backed by the Wi-SUN Alliance™, a global industry alliance that promotes the Wi-SUN specification. Wi-SUN has a 3rd party organization that develops tests to certify that IEEE 802.15.4g based IoT equipment is both conformant to the standard and interoperable with other certified equipment. Wi-SUN networks support star and mesh topologies, as well as hybrid star/mesh deployments, but are typically laid out in a mesh topology where each node relays data for the network to provide network connectivity. Wi-SUN networks are deployed on both powered and battery-operated devices.

LoRaWAN is a Low Power Wide Area Network (LPWAN) specification based on chirp spread spectrum radios from Semtech, a supplier of proprietary semiconductor solutions. LoRaWAN is supported by the LoRa Alliance™, which provides certification for vendor interoperability. LoRaWAN radios are commonly used in low power devices with infrequent data transmissions. LoRaWAN is typically laid out in star topology with gateways relaying messages between end-devices and a central network server.

NB-IoT is a new mobile technology specification by the 3GPP standards body, and is expected to be used for low power and infrequent data transmission devices. NB-IoT can operate in the GSM spectrum or utilize an un-used resource block within a LTE's carrier's guard-band. NB-IoT compliant chipsets are now becoming available in the prototype stage. Most network topologies are star-based. 3GPP has not announced plans for a certification program yet. Certification programs with cellular companies have included high fees in the past, but no details have been announced as of the writing of this paper.

The three wireless networking technologies differ in several key areas. Following is a quick overview of those differences.

Network Topology and Coverage

IoT networks typically are deployed in one of two topologies: star or mesh.

- **Star:** LoRaWAN and NB-IoT networks are usually connected via a tower- or star-based topology. Commonly used in cellular networks, a star topology uses gateways (cellular towers, for example) that must have a direct connection to every device for that device to communicate. However, anything that obstructs the path from device to gateway (weather, construction or temporary obstacles) can impact a device's ability to remain connected to the network, which in turn compromises the reliability of the network and the services it carries. These obstructions are known as "black spots" or "shadows". In urban areas, the emergence of black spots could mean having to install more gateways to ensure a reliable connection for all devices, as many IoT devices are fixed in place and can't be moved to a better coverage location.
- **Mesh:** Wi-SUN networks are usually mesh networks. In a mesh network, IoT devices communicate with neighboring devices on their network, all of which can serve as conduits to the network base station. This allows for multiple, redundant connection paths, so unlike star-based

[1] *Forecast: Internet of Things — Endpoints and Associated Services*, Gartner, Inc., Worldwide, 29 December 2016.

networks, both single points of failure and black spots are dramatically reduced, or even eliminated entirely. In fact, as mesh networks scale, their reliability and performance improves because the possible communication paths multiply. Mesh networks devices tend transmit short distances which enable them to be power efficient, deliver long battery life and have more consistent data rates. A mesh architecture is essential for applications which require distributed computing or some local intelligence. These applications go beyond simple data acquisition and process locally-available information from in field devices to make quick, intelligent decisions. Wi-SUN mesh networks are self-forming (when a new device is added, it automatically finds peers to communicate with) and self-healing (if obstacles emerge, devices will automatically reroute to the nearest available peers). Wi-SUN-based mesh networks have proven themselves for years in an array of harsh and remote environments across the globe. Tens of millions of reliably connected endpoints demonstrate that a Wi-SUN-based IoT mesh network can achieve the ubiquity and scalability many IoT customers demand.

Communication Performance: Bandwidth, Latency and Bi-Directional Communication

The bandwidth, latency and bi-directional communication performance of a technology can have significant impact on the usable lifetime and functionality of the network. IoT applications are rapidly developing with new uses and benefits being discovered and created. Having a network with the capacity to handle new applications and data streams will avoid early obsolescence. Additionally, the ability to update and upgrade deployed devices remotely can significantly extend the working life of those devices, while minimizing the need to conduct expensive field visits. Most of the current IoT applications today require on-demand control. On-demand commands require a network that can listen frequently and respond in a timely manner to on-demand commands. Not all IoT technologies offer the necessary bandwidth, latency and bi-directional communication to ensure long usable life and full-featured functionality.

IoT NETWORK	FEATURE	
	Bandwidth	Latency
Wi SUN Alliance	Up to 300 Kbps	0.02 sec
LoRa™	Up to 50 Kbps[2]	1-2 sec[4]
Advanced Pro LTE	Up to 60 Kbps[3]	2 – 8 sec[5]

- **Wi-SUN** provides high data rates that are consistent throughout the network and low latency. Additionally, Wi-SUN modules use less power for listening (see Power Efficiency section) which enable customers to configure devices to listen frequently and still maintain a long-life.
- **LoRaWAN & NB-IoT** In an attempt to drive down device costs and extend battery life, these devices are designed for low bandwidth (bandwidth also drops the further a device is from the base station) and infrequent communication. This may compromise the ability for the device to do future applications, firmware upgrades, security updates, and receive on-demand commands. Transmissions can be longer, too, because communication speeds can at maximum be only 50-60 Kbps—up to ~5-6 times slower than Wi-SUN—which results in more power consumption.

Industry Standards

When an IoT network adheres to recognized industry standards, you as a network owner or operator will enjoy certain advantages. One of the biggest is that you're not locked in to solutions from one vendor. So how do the three technologies stack up on the standards front?

[2] *LoRa Frequently Asked Questions*, Semtech.
[3] *Standardization of NB-IoT completed*, 3GPP, 22 June 2016.
[4] *Unclear what exactly is possible with LoRaWAN technology*, The Things Network, June 2016.
[5] Ericsson Tech Review of NB-IoT report, LinkLabs, 22 May 2016.

- **Wi-SUN**, established in 2011, leverages IEEE 802.15.4g and IPv6 protocols and is driving innovative wireless Smart Utility and Smart City applications. More than 100 member companies have collectively introduced more than 90 Wi-SUN certified products. Wi-SUN components and Wi-SUN compatible products are currently available from several vendors.
- **NB-IoT** is based on 3GPP, Release 13. 3GPP unites seven telecommunications standard development organizations. Ratified in June of 2016, Release 13 incorporates specific features for use in public emergencies. Though still a nascent network standard, NB-IoT certified products are expected to be available in the market shortly.
- **LoRaWAN** is built around proprietary technology owned by Semtech. As such, it is not an open standard. Implementing LoRaWAN-based solutions requires the use of chips made by Semtech or their licensees, potentially creating vendor lock-in. Further, while a diverse ecosystem of vendors offer LoRa products, these may not be fully interoperable. This could result in stranded assets and customers dropping down to the simplest form of LoRaWAN which could mean the loss of performance and possibly functionality.

Security

Security is a core concern for any network as compromised devices can be used to mount attacks on other networks, result in costly technology replacements or, even worse, disrupt essential services or public safety as would be the case for critical IoT networks. Military-grade security is the gold standard among IoT networks. Only Wi-SUN-based networks have achieved military-grade security by offering the security capabilities described below.

Provider Ecosystem

When an IoT network standard has a broad ecosystem of providers and developers that are interoperable, you have a broader set of product options and features supported by stronger pricing competition. Having access to a wide variety of options enables you to deploy a more cost-effective and optimized IoT network solutions.

- **Wi-SUN –** The Wi-SUN Alliance consists of more than 130 member companies including product vendors, silicon vendors, software companies, utilities, government institutions and universities. Each member company contributes to the Wi-SUN ecosystem as the Wi-SUN Alliance has defined testing and certification programs for multi-vendor interoperability. Wi-SUN networks have been deployed for more than 10 years in mixed-vendor environments, demonstrating ongoing commitments from a wide variety of organizations.
- **LoRaWAN –** The LoRa Alliance™ has more than 400 members, however it is unclear how interoperable each member's provider ecosystem is.
- **NB-IoT –** Because NB-IoT is based on 3GPP, an alliance of multiple standards organizations, NB-IoT has the potential to have a healthy ecosystem of partners. However, due to the developmental nature of NB-IoT, there are no ecosystems built yet and it is unclear how

ELEMENT OF SECURITY	IoT NETWORK		
	Wi-SUN	LoRaWAN	NB-IoT
Authentication Chain of Trust (for mutual authentication of all devices and applications across the platform)	Public key infrastructure with x.509 certificates	Not Specified	Challenge/response authentication using pre-shared secret
Key Exchange and Distribution	Automated, symmetric key exchange and rotation using 802.11i	Static key exchange; no rotation	Static key exchange; no rotation
Key Generation and Storage	Hardware security modules and hardened crypto processors	Not specified	Not specified
Data Transmission	AES, HMAC and certificates	AES, CMAC and pre-shared secret	LTE data transmission encryption: AES
Network Access Control	Authentication via certificate prior to network enrollment	Authentication via pre-shared secret prior to network enrollment	Challenge/response authentication using pre-shared secret

the interoperability programs will work and at what cost. In fact, questions have been raised about the interoperability of two different implementations of NB-IoT.[6]

Power Efficiency

Many IoT devices do not have access to direct power and thus require battery power. As such, low-power devices are required to ensure long service life. But consuming less power can come with trading off functionality. To preserve battery life, some IoT devices will listen less frequently—a problem for applications where on-demand commands are needed, or when it's time to configure and update firmware. As explained below, these trade-offs differ based on the type of network technology that connect those devices.

- **Wi-SUN –** Wi-SUN devices can be designed for frequent (up to 10 seconds), low-latency communication that draws less than 2 µA when resting and, more importantly, only 8 mA when listening.
- **LoRaWAN –** LoRaWaN devices are designed for infrequent communication (up to 128 seconds) and draws 2 µA when resting and 12 mA when listening. The longer latency compromises the ability for the device to receive on-demand commands.
- **NB-IoT –** NB-IoT devices are designed for infrequent communications (up to 600+ seconds). Power consumption during resting and listening have not been published as of this printing.

Scalability

Today's largest IoT networks will look small in five years. The ability to grow a network—while adding new applications —is a crucial consideration when choosing a network platform standard.

- **Wi-SUN –** Wi-SUN-based mesh networks can scale in both capacity and size. Due to the higher bandwidth capabilities noted above, Wi-SUN-based networks provide the ability to add new applications as operational needs require. Due to the mesh topology, the network reliability improves as more devices participate in the network. Additionally, with 10s of millions of endpoints deployed across the world, including several deployments with more than 1 million devices, Wi-SUN-based IoT networks are the most proven in the world today. Successful deployments on five continents demonstrate that Wi-SUN-based networks perform well at scale in urban, suburban and rural environments.
- **LoRaWAN –** LoRaWAN networks require the installation of additional gateways to provide the direct connections needed for adding devices to star-based networks. In real world deployments, LoRaWAN is yet to be proven at very large scale and because LoRaWAN networks do repeated transmissions to ensure reliability. It is unclear if the network will have enough capacity at large scale.
- **NB-IoT –** Scalability is largely undetermined as NB-IoT have not yet been deployed at scale yet.

Network and Device Longevity

A general rule of IoT networks is that longer-lasting devices connected via higher-performing networks require fewer field visits and swap-outs, resulting in lower total cost of ownership (TCO) overall. Another factor influencing device longevity is backward compatibility. When choosing a network, evaluate each platform's ability to accommodate multiple generations of hardware on a single network; this too will lower TCO by allowing you to use older devices longer.

- **Wi-SUN –** To date, higher performing networks and backward compatibility are more prevalent among Wi-SUN-based networks. One leading provider of Wi-SUN-based networks deploys hardware designed to last 15 years, battery included. That same provider has customers who operate multiple different generations of hardware within the same networks, proving both backward and forward compatibility.
- **LoRaWAN –** LoRaWAN Alliance members claim to offer network and devices that will last up to 10 years, however these claims will need to be backed by commercial terms and proof points that the technology will be supported for an extended period of time.
- **NB-IoT –** Since it's too early to assess device and network longevity for NB-IoT devices, we can only evaluate how the infrastructure supporting NB-IoT devices have evolved over the past several years. Cellular carrier networks are primarily designed to support the increasingly data-intensive consumer mobile device market. Addressing

[6] *The NB-IoT Train is Delayed*, Light Reading, Iain Morris, 27 March 2017.

those needs has resulted in an acceleration of changes to generation platforms in carrier networks. Not all of those generations have been supported on the network—a trend that may impact backward-compatibility in the future and potentially leave stranded assets. Additionally, there are a few different bands involved in 3GPP based technologies (e.g. others are pushing Cat-M1). The question becomes for a potential user is how can I guarantee my technology choice will endure for the 10-15 years required for an IoT device.

Summary

Machine to Machine (M2M) communication and IoT is enabling many different and exciting new solutions for cities, utilities, and companies to better manage their assets, operations and environment. Folks using the networks to connect the various sensors and nodes deployed need to understand the various technologies available. This document has compared the three leading technologies to show how they stack up on several key design considerations. For many applications, the security, coverage, ecosystem and scalability assessments favor the characteristics of Wi-SUN technology. For more information on the Wi-SUN Alliance and its role in the future of IoT, visit www.wi-sun.org.