SELECTING A WIRELESS TECHNOLOGY FOR

New Industrial Internet of Things Products

A Guide for Engineers and Decision Makers

Wireless Connectivity is Exploding

WITH EXPLOSIVE INTEREST IN THE INTERNET OF THINGS (IOT), MANY ENTERPRISES AND ENGINEERS ARE FOCUSING ON WIRELESS CONNECTIVITY OPTIONS.

This paper briefly outlines some options available on the market today and describes the advantages and disadvantages of each. The trade-offs between range vs. data throughput or battery life vs. latency will be discussed.

Selecting a wireless option for IoT devices is a difficult proposition, and only after considering all parts of the go-to-market strategy can the full picture of advantages and disadvantages be appreciated.

First, a few definitions to make reading this paper easier:

Endpoint:

This is the "thing." It could be a connected thermostat, a door lock, a GPS tracker, or a dishwasher. It is the device which is creating business value through its sensor data, its ability to be remotely controlled, or both.

Access Point:

This is the radio that is receiving data from one or more endpoints and is usually connected to the Internet. For Bluetooth, it is often a cell phone. For cellular-based or M2M IoT devices, the access point is on the cell tower. For WiFi, the access point is the router. With Link Labs' technology, access points are called gateways, and they function similarly to a WiFi router.

Back End:

Once wireless data gets to the access point, it is generally sent to a server on the Internet—for example, "The Cloud"—where a program is running to "do" something. This could be anything from storing data in a database so an iPhone app can query it to deciding to send a text message because a smart refrigerator is above its normal temperature.

Key Questions When Reviewing Connectivity Options

1 HOW WILL IDENTITY AND PROVISIONING BE HANDLED?

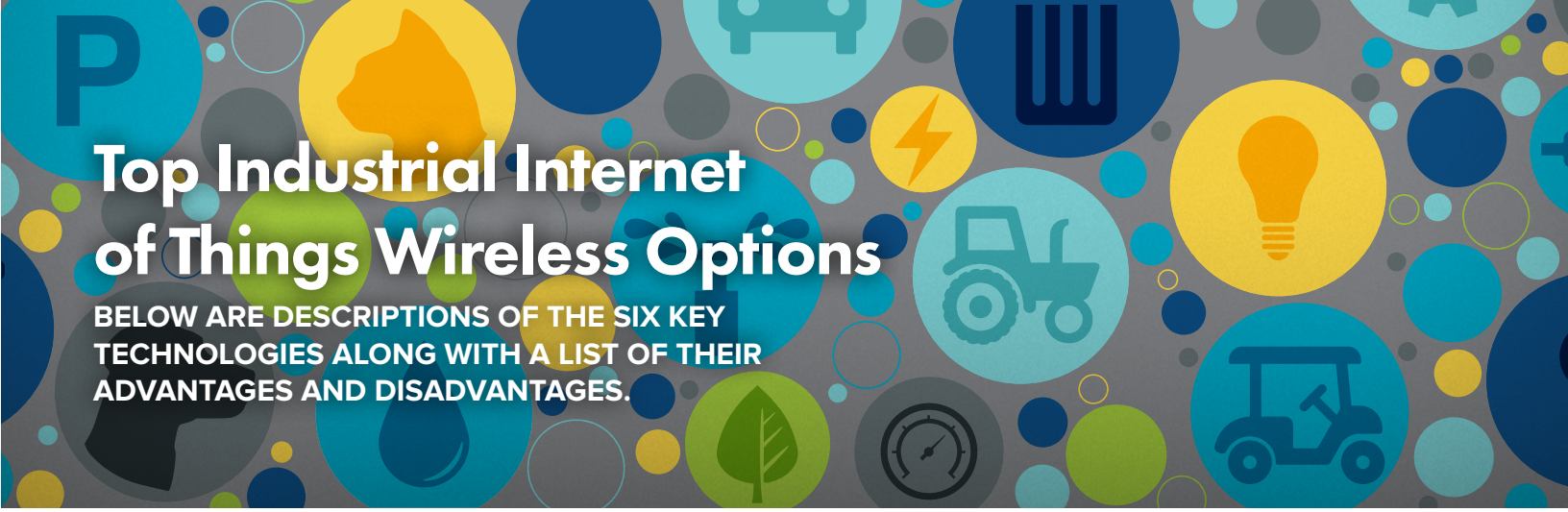
Figuring out how an endpoint device sold into a sales channel can be associated with a specific customer is a significant issue in industrial IoT applications. Often just as challenging is how the customers' various devices can be further segmented into the location, role, or configuration required.

2 WHAT ARE THE COSTS AND FRICTION POINTS ASSOCIATED WITH THE ACCESS POINT TECHNOLOGY?

For instance, with cellular, someone will have to pay a mobile operator for network access and manage SIMS and connection at the device level. For WiFi, your system can operate only where the end devices "know" how to join a network. Convincing industrial or enterprise customers to allow your WiFi-enabled endpoint on their network might not be possible, as this is a perceived security risk. For a mesh technology, the challenge is guaranteeing that node density is high enough to ensure reliable performance.

3 HOW WILL OVER-THE-AIR SECURITY BE MANAGED?

Since radio waves are available for anyone to receive, encrypting over-the-air transmission is usually a must. Encryption requires that some "secret" is known by both sides at the beginning. This secret is then often used to create a "session" secret, so each endpoint's data is encrypted in a different way. In a WiFi system, the secret is often the AES passphrase. In a cellular endpoint it can be on the SIM card. For Bluetooth, it can be a passcode or a preshared application key.



Top Industrial Internet of Things Wireless Options

BELOW ARE DESCRIPTIONS OF THE SIX KEY TECHNOLOGIES ALONG WITH A LIST OF THEIR ADVANTAGES AND DISADVANTAGES.

WiFi

WiFi needs virtually no introduction. Chances are, almost everyone reading this paper is very familiar with WiFi. WiFi standardization is one of the crowning achievements of IEEE, which standardized WiFi as 802.11. There have been many advances in WiFi, with "b" progressing over time to higher performance "ac". (Note that there are many WiFi standards that were never adopted.)

The foundational premise of WiFi is interoperability. An access point from one vendor will nearly always work with a WiFi endpoint from another vendor. Using the brand name "WiFi" often denotes that the device has been certified as compliant to the standard and interoperable.

Because WiFi is a full TCP/IP-based protocol, devices communicating via WiFi are known as "on the Internet." This means any WiFi-enabled host is by definition part of the local area network (LAN) it joins. This can create security concerns, as IT departments may not be able to secure and manage IoT-connected WiFi endpoints the same way they can secure a Windows laptop.

There is a strong perception across many enterprises that WiFi-connected third party devices pose an enormous security risk. The infamous Target hack of 2014[1] was caused by HVAC devices, which were provisioned on the corporate WiFi network.

Therefore, the most successful WiFi-based IoT products will be those with a high degree of ownership and control by the owner of the WiFi LAN. Asking to connect your third party system to the LAN via WiFi is likely to be met with increasing resistance.

Even if you successfully sell your WiFi-connected device into an enterprise where the use of WiFi is permitted, you still face a huge uphill battle in terms of provisioning. Paying someone to program a password into every connected light is very expensive. If credentials change, the entire process might have to be repeated. Even using DMZ or Guest WiFi networks can be difficult, as these systems are often designed to challenge human users via a landing page, and MAC/IP leases often time out after a few hours.

IDEAL INDUSTRIAL WIFI USE CASES

- Barcode scanners in factories
- Connected machines

BENEFITS

- Near ubiquitous network coverage in enterprises
- Inexpensive chipsets and modules
- Can be power efficient, if application and polling rate is designed well

CONSIDERATIONS

- Friction for 3rd party devices joining WiFi networks
- Provisioning of credentials is difficult

1. http://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/

Bluetooth

Like WiFi, Bluetooth is something most designers are familiar with. While Bluetooth is very popular in the consumer electronics space, we have witnessed a growth in interest in using Bluetooth in the industrial setting. This is primarily because Bluetooth is the least costly wireless technology on the market.

However, Bluetooth is a **short range** technology. It is reliable only when endpoints are used within the same room (or within a few dozen meters) of an access point. Therefore, many customers we see are now pairing Bluetooth (no pun intended) with another wireless technology in the following way: Dozens of endpoints in an area are connected back to one master device, which acts as the Bluetooth access point. Then, that device uses another form of connectivity to communicate to the back end. For example, there might be a cellular-to-Bluetooth bridge in a factory for lighting control. We call this **Bluetooth bridging**. Then, a large number of endpoints can have inexpensive connectivity using Bluetooth, while only a small number of devices in the system require more expensive connectivity options (like cellular).

Obviously, Bluetooth can be used to connect to phones as well, though this is less common in an industrial setting. Hybrid architectures—where Bluetooth endpoints use phones when available and then use bridging when they are not—are possible.

IDEAL BLUETOOTH USE CASES

- Light control
- Proximity monitors
- Disposable asset trackers (Active RFID)

BENEFITS

- Low Cost: disposable or competitive product lines.
- High datarates
- Long battery life

CONSIDERATIONS

- Very short range
- Requires key coordination at both endpoint and access Point
- Needs access point (phone or application specific device)

Mesh Networks

The number of mesh technologies has exploded over the last 10 years. There are many mesh network options, each with strengths and weaknesses. **ZigBee**, **Z-Wave**, **Thread**, **802.15.4**, and **6LoWPAN** are all variations on a theme; they use short-range, high data rate wireless to build networks that depend on relaying data between nodes. Data is either trying to get to the endpoint or the access point. Configuring and optimizing mesh networks is a major undertaking.

Because mesh technologies are short range, if you want to cover a large area, you need a fairly even distribution of closely spaced nodes. It is very common in mesh HVAC sensing systems to put "dummy" thermostats down a long corridor, just to ensure that the network can propagate properly. This often requires installation by experts.

When done well, mesh networks can be a good way to get wide-area, power efficient coverage. However, low density, ad hoc mesh networks cannot provide reliable connectivity.

IDEAL MESH NETWORK USE CASES

- HVAC sensing and control
- Lighting control (high density)

BENEFITS

- Resilient physical system architecture
- Modification or expansion can happen without system disruption
- Good power budget if designed correctly

CONSIDERATIONS

- Short range
- Link performance problems
- Deployment difficult
- Interoperability is often not possible due to configuration differences and key management

Cellular Machine-to-Machine (M2M)

Using cellular networks to connect industrial IoT devices is an attractive option for many companies. Cellular networks exist in most (but not all) places, and network management is someone else's problem—but these advantages come at a cost.

Until advances like LTE-M1 or NB-IoT come onto the market, an M2M endpoint is often taking more than its share of network resources—resources that could be more profitably used for iPhones. The lowest price-per-month we've seen for 750kB of data is $0.75 per device, which is great if it fits your business model. If not, cellular could be very expensive.

The cost of cellular end device certification is an important consideration. Cellular device certification is a confusing and frustrating field. A new chip down cellular endpoint will cost well over $100,000 in certification and testing to bring to market. Even a module-based design could cost $20,000 or more.

Another consideration is that cellular devices (as protocols exist today) require a fairly large power budget to maintain network connection. This is one of the primary reasons (with chip cost being the other) that 3GPP is focusing on improving cellular standards for IoT.

IDEAL CELLULAR M2M USE CASES
- GPS telematic trackers
- Smart meters
- Connected cars

BENEFITS
- Ubiquitous network coverage

CONSIDERATIONS
- Recurring cost
- Expensive chipsets
- Short battery life
- Expensive certification

Sigfox / LoRaWAN / Ingenu

We have written extensively on low power, wide-area network (LPWAN) technology. Please see our white paper for more details. (http://info.link-labs.com/lpwan) These are the three primary players to building large-scale, cellular-like networks, specifically for IoT. Sigfox and LoRaWAN are focused on uplink sensor data with small payloads. Ingenu is building a national network for machine communication. In areas with ubiquitous network coverage, these technologies offer reliable solutions for smart cities, smart metering, and related applications.

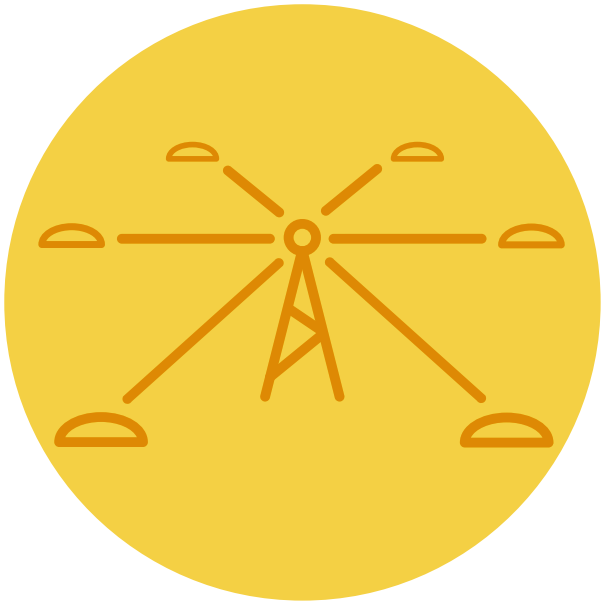
The biggest drawback of these networks is that they do not exist everywhere. Therefore, they are appropriate only for solutions sold in a defined geographic area. Companies wanting to deploy IoT solutions quickly in a variety of locations may have to wait on the buildout of network coverage.

These networks also have some work to do to make device provisioning and identity easy. Without a SIM card-like concept, keys and unique ID numbers for each endpoint need to move between network operators and device manufacturers.

IDEAL USE CASES
- Automatic meter reading
- GPS tracking devices (in a defined area)

POSITIVES
- Power efficient
- Inexpensive chipsets
- Low certification costs

CONSIDERATIONS
- Low data throughput
- Networks do not exist everywhere
- Quality of Service not guaranteed in unlicensed spectrum.
- Current provisioning and key management schemes make large scale manufacturing difficult.



Symphony Link

Symphony Link is Link Labs' primary product. It is a highly integrated wireless system for industrial sensor and controller networks. It uses the same type of technologies as some LPWAN providers, but it adds features to make the system useful for customer deployed scenarios.

Symphony Link customers place access points in the areas where they need coverage, generally one per building or factory. End nodes can join and transact on this network securely, without further provisioning.

IDEAL SYMPHONY LINK USE CASES

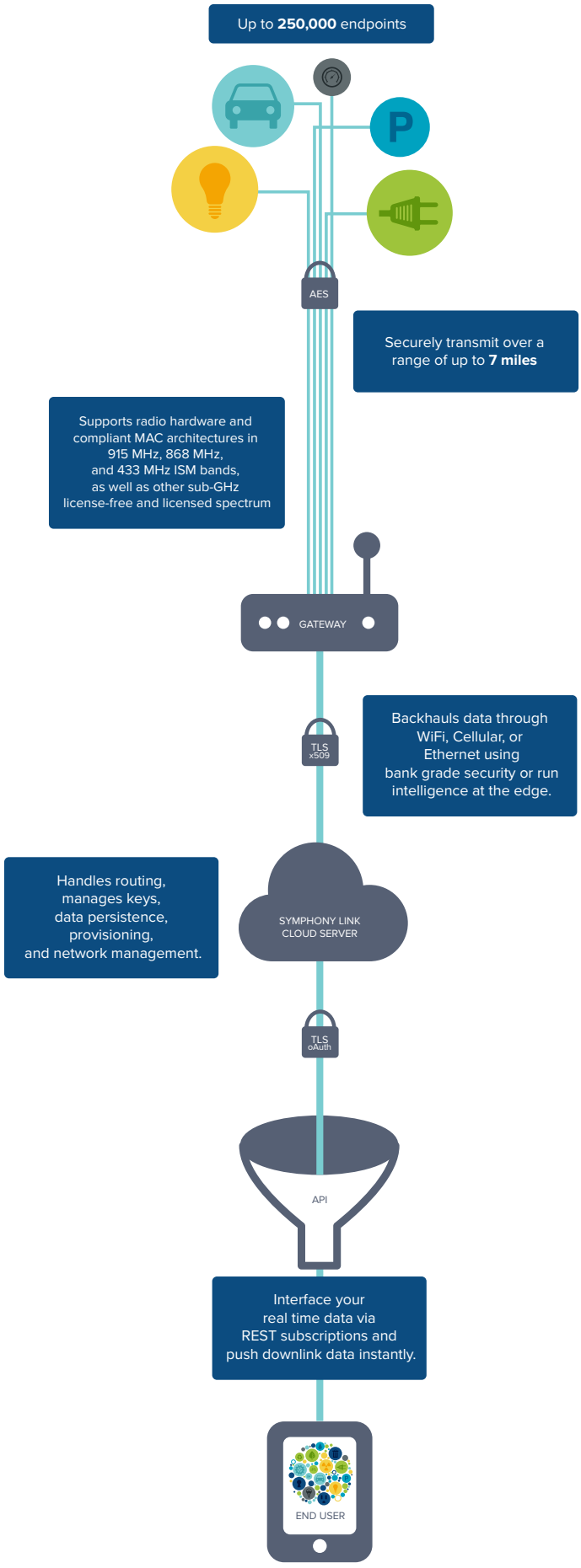
- Building controls
- Lock controllers
- Occupancy sensors
- Safety sensors
- Alarm devices
- Environmental sensors

BENEFITS

- Automatic device provisioning and discovery
- Long range
- Long battery life
- Low latency
- High capacity

CONSIDERATIONS

- Low data throughput
- Proprietary technology (full licensing available)



In Conclusion

There are several players in the wireless connectivity market, but there's room for all of them. WiFi, Bluetooth, Cellular, ZigBee, Z-Wave, Thread, 802.15.4, 6LoWPAN, Sigfox, LoRaWAN, Ingenu, and Symphony Link all have strengths and weaknesses. If you can understand and identify potential issues with provisioning, security, costs, access, and the considerations outlined above before choosing a wireless technology, you'll be able to make the best choice for your application.

Want to learn more about Symphony Link?

LET'S TALK.

For additional questions:
info.link-labs.com/contact
+1 (202) 524-1390
Learn about our other products:
link-labs.com/

LinkLabs