Vol 58, No 2—June 2024

ANALOG DEVICES | ADI Analog Dialogue™

A Complete Guide to Designing Your Smart Wireless Industrial Sensor

Richard Anslow, Senior Manager

Abstract

This article provides an overview of wireless standards and assesses the suitability of Bluetooth® Low Energy (BLE), SmartMesh (6LoWPAN over IEEE 802.15.4e), and Thread/Zigbee (6LoWPAN over IEEE 802.15.4) for use in industrial harsh RF environments. Comparative metrics are provided, including power consumption, reliability, security, and total cost of ownership. SmartMesh time synchronization results in low power, and SmartMesh and BLE channel hopping result in higher reliability. A case study for SmartMesh concludes with 99.999996% reliability. Analog Devices' BLE and SmartMesh wireless condition monitoring sensors are presented, including a new wireless sensor with edge artificial intelligence (AI), which increases battery life for constrained edge sensor nodes.

Introduction

The market for smart sensors for motor driven systems is expected to more than double in sales volume between 2022 and 2024 (growing to $906M USD).[1] Within smart sensors, wireless and portable devices are expected to be the primary growth drivers. Monitoring industrial machines using wireless environmental sensors (temperature, vibration) has one clear goal: to detect when the equipment being monitored deviates from healthy operation.

For industrial wireless sensor applications, low power consumption, reliability, and security are consistently ranked as the most important requirements. Other requirements include low total cost of ownership (minimal gateways, maintenance), short range communication, and a protocol capable of mesh formation for factory environments that include lots of metallic obstacles (meshing networks help to mitigate possible signal path shielding and reflections).

Industrial Applications and Wireless Standards Requirements

Figure 1 provides an overview of wireless standards, and Table 1 ranks selected wireless standards against key industrial requirements. It's clear that BLE and SmartMesh (6LoWPAN over IEEE 802.15.4e) offer the best combination of low power consumption, reliability, and security for industrial applications. Thread and Zigbee offer low power and secure mesh implementations but score lower on reliability.

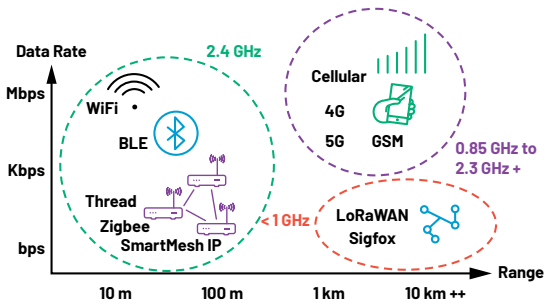

Figure 1. Survey of wireless standards.

Table 1. Mapping Wireless Standards to Industrial Application Requirements.

Standard	Range	Power Consumption	Reliability	Robustness	Total Cost of Ownership	Mesh Capable	Security
Wifi (802.111 b, g)	100 m	High	Low	Low	High	Yes	Yes, WPA
BLE	20 m to 100 m	Low/medium	Medium/high	Low	Medium	Yes	Yes, AES
Zigbee, Thread (6LoWPAN over IEEE 802.15.4)	20 m to 200 m	Low/medium	Low	Low	Medium	Yes	Yes, AES
SmartMesh (6LoWPAN over IEEE 802.15.4e)	20 m to 200 m	Low	High	High	Low	Yes	Yes, AES
LoRaWAN	500 m to 3000 m	Medium to low power nodes, high power gateways	Low	Low	High	No — Star Topology	Yes, AES

Table 2 provides more details for the Zigbee/Thread, SmartMesh, and BLE mesh standards. SmartMesh includes a time synchronized channel hopping (TSCH) protocol, where all nodes in a network are synchronized and communication is orchestrated by a schedule. Time synchronization results in low power and channel hopping results in high reliability. The BLE standard also includes channel hopping, but has some constraints in comparison to SmartMesh, including line powered routing nodes (increased system cost and power), and TSCH is not supported. As previously mentioned, Zigbee/Thread score low on reliability and do not offer many advantages compared to BLE.

Table 2. Key Wireless Standards and Performance for Industrial Applications

Feature	Zigbee, Thread (6LoWPAN over IEEE 802.15.4)	SmartMesh (6LoWPAN over IEEE 802.15.4e)	BLE Mesh
Radio frequency	2.4 GHz	2.4 GHz	2.4 GHz
Data rate	250 kbps	250 kbps	1 Mbps, 2 Mbps
Range	20 m to 200 m	20 m to 200 m	20 m to 150 m
Application throughput	< 0.1 Mbps	< 0.1 Mbps	< 0.2 Mbps
Network topology	Mesh, Star	Mesh, Star	Mesh, Star
Security	AES encryption	AES encryption	AES encryption
Power	Line powered routing nodes	Routing nodes require only average 50 µA	Line powered routing nodes
Total cost of ownership	$$ to $	$	$$ to $
Time synchronized channel hopping	x	✓	x
Robustness (channel allocation)	x Single channel comms	✓	x
Reliability (channel hopping)	x Single channel comms	✓	✓
Standards (interoperability)	Yes	Proprietary	Yes

This article will focus on SmartMesh and BLE mesh as the most suitable wireless standards for industrial condition monitoring sensors.

Analog Devices Wireless Condition Monitoring Sensors

Table 3 provides an overview of Analog Devices' Voyager 3 Wireless Vibration Monitoring Platform and next-generation wireless condition monitoring sensors. Voyager 3 uses a SmartMesh module (LTP5901-IPC). An AI enabled vibration sensor (still in development) uses a BLE microcontroller (MAX32666). Both sensors include temperature and battery state of health (SOH) sensors. The Voyager 3 and AI version sensors use ADI MEMS accelerometers (ADXL356, ADXL359) to measure vibration amplitude and frequency for industrial equipment. Increasing vibration amplitudes and frequencies are identified using FFT spectra, which can indicate faults such as motor imbalance, misalignment, and damaged bearings.

Table 3. ADI Wireless Industrial Sensor Prototypes

Parameter	Voyager 3	Next-Generation Sensor
Wireless standard	SmartMesh	BLE
Ultra low power edge AI	No	Yes
Temperature sensor	Yes	Yes
MEMS accelerometer	Yes (triaxial 1 kHz)	Yes (triaxial 8 kHz)
Battery SOH monitoring	Yes	Yes

Figure 2 provides an overview of a typical operation for Voyager 3 and the AI enabled vibration sensors. Like many industrial sensors, the duty cycle is 1%; most of the time the sensor is in a low power mode. The sensor wakes up periodically for bulk data gathering (or in a high vibration amplitude shock event) or to send the user a status update. The user is typically notified with a flag to state that the monitored machine is in good health, and the user is given the opportunity to gather more data.

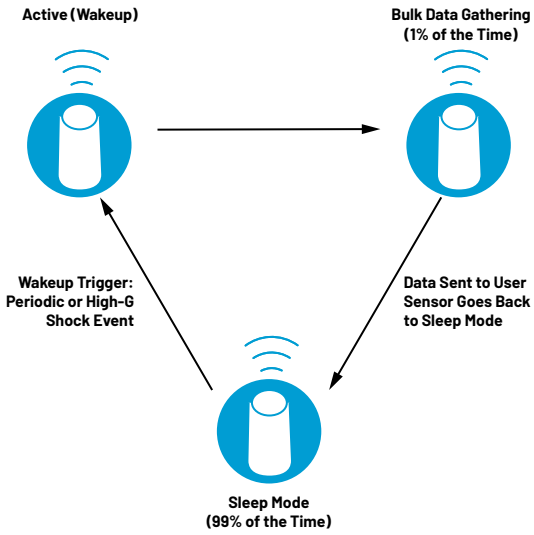

Figure 2. An industrial wireless sensor typical operation.

Security

SmartMesh IP networks have several layers of security, which can be categorized as confidentiality, integrity, and authenticity. A summary of SmartMesh security is provided in Figure 3. Confidentiality is achieved with AES-128-bit encryption end to end, even if there are multiple mesh nodes in the network. Data transmitted is protected by message authentication codes (message integrity check, or MIC) to ensure that it has not been tampered with. This protects against man in the middle (MITM) attacks, as shown in Figure 3. Multiple device authentication levels are possible, which prevents unauthorized sensors from being added to the system.

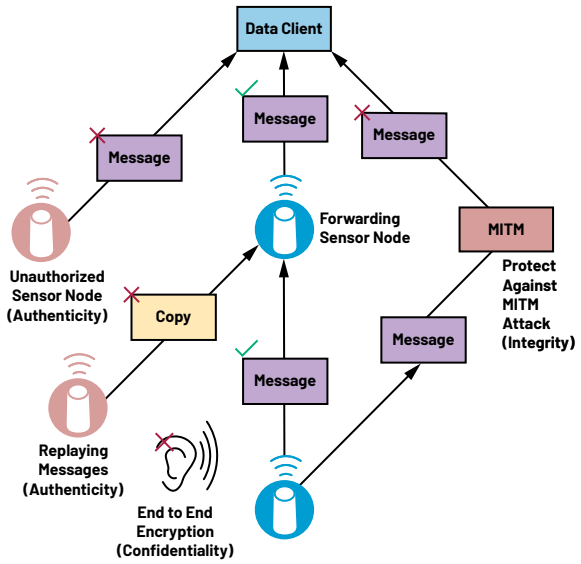

Figure 3. Security implementation for BLE and SmartMesh networks.

Devices operating with versions 4.0 and 4.1 of the BLE standard are security vulnerable, however, versions 4.2 and above include enhanced security (as described in Figure 3). ADI's MAX32666 is compliant to the BLE standard 5.0. This version introduces the P-256 Elliptic Curve Diffie-Hellman key exchange for pairing. In this protocol, the public keys of the two devices are used to establish a shared secret between the two devices, called the long-term key (LTK). This shared secret is used for authentication and generation of keys to encrypt all communication, protecting against MITM attacks.

Low Power Consumption

The sensors described in Table 3 operate on a 1% duty cycle, with Voyager 3 maximum payload of 90 bytes, and the AI version maximum payload of 510 bytes. Figure 4 (adapted from Shahzad and Oelmann[3]) shows that for 500 bytes to 1000 bytes, BLE consumes less energy compared to Zigbee and Wi-Fi. BLE is thus a good match for the AI enabled use case. SmartMesh provides ultra low power consumption, especially for payloads of 90 bytes or less (as used in the Voyager 3 sensor). The SmartMesh energy consumption is estimated using the SmartMesh Power and Performance Estimator tool available on the website. The SmartMesh power estimator tool accuracy has been experimentally verified 87% to 99% accurate depending on whether a sensor is a routing or leaf node.

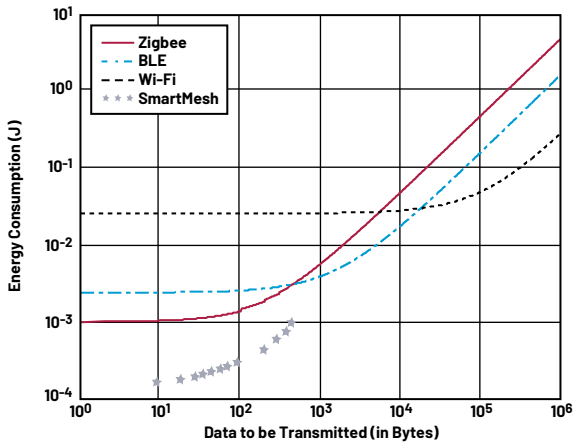

Figure 4. Data transmitted (radio transceiver PHY) and energy consumption (adapted from Shahzad and Oelmann).[3]

In addition to radio transmit power consumption, one must consider the total system power budget and total cost of ownership. As described in Table 2, BLE and Zigbee both operate using a single gateway. However, both also require line power for routing nodes. This increases the power budget and total cost of system ownership. In contrast, SmartMesh routing nodes only require on average 50 µA of current, and an entire network can operate using a single gateway. SmartMesh is clearly a more energy efficient implementation.

Reliability and Robustness

As mentioned previously, SmartMesh uses TSCH, which has the following characteristics:

- All nodes in a network are synchronized.
- Communication is orchestrated by a communication schedule.
- Time synchronization results in low power.
- Channel hopping results in high reliability.
- The scheduled nature of communication brings a high level of determinism.

The synchronization accuracy is less than 15 µs across the entire network. This extremely high level of synchronization results in extremely low power. On average 50 µA current draw, and 1.4 µA greater than 99% of the time.

Table 4 provides some key application challenges and how SmartMesh and BLE mesh meet these challenges.

Table 4. Key Challenges for Wireless Networks in Industrial Application and BLE/SmartMesh Performance

Challenge	Problem	SmartMesh	Bluetooth Mesh
Robust communications in densely formatted networks	Nodes interfere with each other, slowing down network	Efficient channel allocation eliminates collisions	Relies on collisions that slow down network
Long battery life when sensors mounted in shielded locations	Requires power efficient edge node connections to meet battery lifetime specs	Battery-powered routing nodes establish close range connection to edge nodes	Line-powered routing nodes establish close range connections to edge nodes
Reliable connections in dynamic industrial environments	Movement of equipment or opening/ closing of doors cause multipath reflections	Employs channel hopping to avoid reception nulls	Employs channel hopping to avoid reception nulls
Reliable communications in congested radio bands	Interferers restrict data traffic bandwidth on the network	Channel hopping to avoid interferers and efficient bandwidth allocation maintains traffic	Designed for small networks and suffers from network flooding

SmartMesh performs better for dense networks with large numbers of nodes. Both BLE and SmartMesh perform well in dynamic industrial environments.

The reliability of SmartMesh was tested in ADI's wafer fab facility.[5] This is a harsh RF environment, with dense metal and concrete. Thirty-two wireless sensor nodes were distributed in a mesh network, with four hops between the furthest sensor node to the gateway. Four data packets were sent every 30 seconds from each sensor node. Over a time period of 83 days 26,137,382 packets were sent from the sensors, with 26,137,381 packets received, resulting in 99.999996% reliability.

Artificial Intelligence at the Edge

The next-generation wireless sensor includes the MAX78000 microcontroller with AI hardware accelerator. This AI hardware accelerator minimizes data movement and leverages parallelism for optimal energy use and throughput.

Wireless industrial sensors currently available on the market typically operate on very low duty cycles. The user sets the sensor sleep duration, after which the sensor wakes up and measures temperature and vibration, and then sends the data over the radio back to the user's data aggregator. Commercially available sensors typically quote a 5-year battery life, based on one data capture every 24 hours, or one data capture every 4 hours. The next-generation sensor will operate in a similar fashion but take advantage of Edge AI anomaly detection to limit the use of the radio. When the sensor wakes up and measures data, the data is only sent back to the user if a vibration anomaly is detected. In this way the battery life can be increased by at least 20%.

For AI model training the sensor collects healthy data for the machine, which is then sent over the air to the user for AI model development. Using the MAX78000 tools the AI model is synthesized into C code, and then sent back to the wireless sensor and placed in memory. When the code is deployed the wireless sensor wakes up at predefined intervals, or in a high-g shock event. Data is gathered and an FFT is generated. From the FFT, the MAX78000 makes an inference based on this data. If no anomaly is detected the sensor goes back to sleep. If an anomaly is detected the user is notified. The user can then request FFT or raw time domain data for the measured anomaly, which can be used for fault classification.

Conclusion

This article provides an overview of wireless standards and assesses the suitability of BLE, SmartMesh (6LoWPAN over IEEE 802.15.4e), and Thread/Zigbee (IEEE 802.15.4) for use in industrial harsh RF environments. SmartMesh has superior reliability and low power operation compared to BLE and Thread/Zigbee. BLE can operate more reliably and at lower power compared to Zigbee and Thread for networks requiring 500 bytes to 1000 bytes of data transmission. Microcontrollers with embedded AI hardware accelerators provide a path to better decision-making and longer battery life for wireless sensor nodes.

References

[1] "Predictive Maintenance in Motor Driven Systems – 2020." Interact Analysis Market Study, April 2020.

[2] Kris Pister and Jonathan Simon. "Secure Wireless Sensor Networks Against Attacks." Electronic Design, April 2014.

[3] Khurram Shahzad and Bengt Oelmann. "A Comparative Study of In-sensor Processing vs. Raw Data Transmission Using ZigBee, BLE and Wi-Fi for Data Intensive Monitoring Applications." 11th International Symposium on Wireless Communications Systems (ISWCS), August 2014.

[4] Thomas Watteyne, Joy Weiss, Lance Doherty, and Jonathan Simon. "Industrial IEEE802.15.4e Networks: Performance and Trade-offs." 2015 IEEE International Conference on Communications (ICC), June 2015.

[5] Ross Yu. "Verifying SmartMesh IP >99.999% Data Reliability for Industrial Internet of Things Applications." Analog Devices, Inc. January 2016.

About the Author

Richard Anslow is a senior manager working in the field of software systems design engineering within the Industrial Automation Business Unit at Analog Devices. His areas of expertise are condition-based monitoring, motor control, and industrial communication design. He received his B.Eng. and M.Eng. degrees from the University of Limerick, Limerick, Ireland. Recently, he completed a postgraduate program in AI and ML with Purdue University.