NORDIC SEMICONDUCTOR

AVNET
Reach Further™

Bluetooth technology is the smart choice for industrial IoT (IIoT)

Table of contents

INTRODUCTION

Most people use at least one form of Bluetooth daily without giving it much thought. Bluetooth enables us to stay connected to a seemingly countless number of devices including cellphones, headphones, smart speakers and automobiles. While the application and adoption of Bluetooth has been driven by the consumer market, there are many more practical applications of Bluetooth technology.

A few of the other markets that have seen broad adoption of Bluetooth technology:

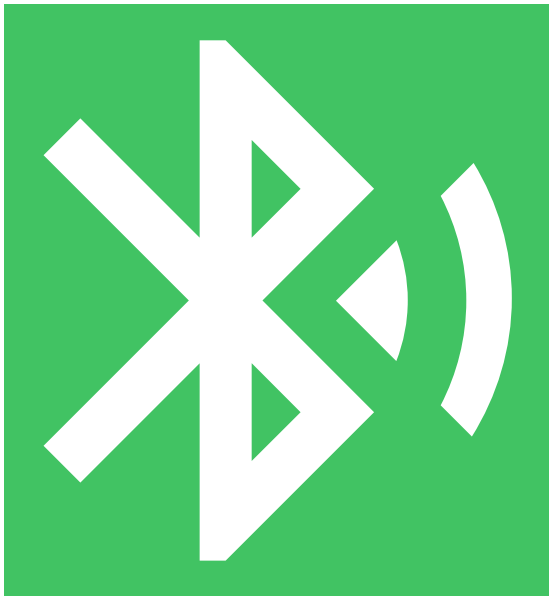
- Internet of Things (IoT)
  - Smart home sensors, devices and controllers
  - Industrial IoT sensors, devices and controllers
  - Edge and Artificial Intelligence (AI) applications
- Advanced computer peripherals like mice, keyboards, multi-touch trackpads
- Interactive entertainment devices like remote controls, gaming controllers, headsets, game consoles
- Advanced wearables
  - Health/fitness sensors and monitoring devices
  - Wireless payment-enabled devices

The possibilities for the application Bluetooth technology appear endless. But where did it all start? We'll review the beginnings of Bluetooth technology, its progression and current capabilities with a focus on IoT in industrial applications and security options for connected devices.

BLUETOOTH 1998 – 2020

Since the standard's introduction in 1998, Bluetooth adoption and device production has grown dramatically every year. An estimated 4.4 billion Bluetooth devices are slated to ship in 2020 alone. Nearly 20 billion were shipped over the last five years. To put this into perspective, the global population of the Earth is nearly 7.5 billion people. The number of Bluetooth devices produced in the last five years is nearly enough for every human in the world to own three.

While the format is more than 20 years old and is backwardly compatible, the Bluetooth of today differs greatly from earlier versions.



A FEW BLUETOOTH MILESTONES:

Bluetooth Classic Pre-Low Energy (LE) period:

- 1998: Bluetooth v1.0 is introduced as a replacement for physical cables.
- 2004: Bluetooth v2.0 is introduced with Enhanced Data Rate (EDR).
- 2009: Bluetooth v3.0 is introduced with high speed over Wi-Fi.

Low Energy (now referred to as Bluetooth LE) period:

- 2010: Bluetooth v4.0 is introduced featuring Bluetooth Low Energy (Bluetooth LE).
- 2014: Bluetooth v4.2 is introduced, addressing major security concerns for connected devices.
- 2016: Bluetooth v5.0 is introduced with new Bluetooth LE features including long-range mode with a new Physical Layer (PHY), a high-speed mode with a new Physical Layer (2M PHY) and extended advertisements.

- 2017: Bluetooth Mesh is released as a separate specification and standard based on Bluetooth LE version 4.x allowing Bluetooth 4.x devices to support Bluetooth Mesh.
- 2019: Bluetooth v5.1 is introduced with new direction-finding/location features for Bluetooth LE.
- 2020: Bluetooth v5.2 is introduced with new features including LE power control, enhanced attribute protocol and LE Audio, the next generation of Bluetooth audio.

BLUETOOTH 5.0 – 5.2: WHAT CAN IT DO?

BLUETOOTH 5.0 UPDATES

Bluetooth 5.0 delivered three main advancements over previous generations when introduced in 2016:

- Twice the speed
- Four times the range
- Eight times the advertising capacity

Twice the speed

The on-air data rate for previous versions of Bluetooth (4.2 and earlier) was fixed at 1 Mpbs. Bluetooth 5.0 introduced a new mode with an on-air data rate transfer of 2 Mbps. The increase delivered important benefits. Among them was lower power consumption as the same amount of data could be transmitted in half the time. Another improvement was wireless coexistence with other wireless technologies that operate in the 2.4 GHz range.

Compared to other low power wireless protocols that include ZigBee, Z-Wave and Thread, Bluetooth LE offers the highest data rate, even at the original 1 Mbps data transfer rate. The addition of the 2 Mbps high-speed mode has made IoT applications more feasible. Examples include video streaming, audio streaming and short bursts of large data transfers such as images.

Four times the range

Bluetooth 5.0 also introduced a long-range mode that employs error correction called Forward Error Correction (FEC). FEC enables the receiver to recover data from errors that occur due to interference and noise. Instead of requiring data to be retransmitted when an error occurs, the receiver can recover the original data transmission through data redundancy.

This long-range mode is referred to as the Coded PHY mode. PHY stands for physical layer radio and refers to the radio interface layer in network architecture. While PHY mode increases range, the trade-off is an increase in power consumption and reduced speed to 125 Kbps or 500 Kbps, depending on the coding level used.

Operating in Bluetooth long-range mode, achievable line-of-sight data transmission ranges from 1 mile (1,600 meters) with the Nordic nRF52840_DK (125kbps/8dBm) to 2,600 feet (800 meters) with the Nordic nRF52-DK (1Mbps/4dBm). This makes Bluetooth LE a good choice for applications that require communication with a device at a great distance or elevation. Examples include long-distance remote-control devices, home automation and industrial applications.

Eight times the advertising capacity

In Bluetooth LE, there are three main operating states for Bluetooth devices. They are advertising, scanning or connected. To get Bluetooth LE devices to connect, one device needs to advertise and the other must scan for it, then initiate the connection. Advertising involves broadcasting data packets which allow another scanning device to discover them. The scanning device then decides to initiate a pairing connection if the advertisement device allows it.

Previous versions of Bluetooth capped the advertising data payload at 31 bytes. Bluetooth 5.0 introduced extended advertising mode. Extended advertising allows up to 255 bytes of payload data per packet and is used in all Bluetooth LE devices. The addition of increased advertising capacity allows for broadcasting audio to an unlimited number of recipients, something not supported with Bluetooth Classic Audio. Another capability that utilizes the extending advertising function are beacons. Beacon devices stay in the advertising state and broadcast data that other devices read. Through the increased advertising and data transmission capacity in Bluetooth 5.0, beacons can support new applications and use cases for IoT.

BLUETOOTH 5.1 UPDATES

Bluetooth 5.1 was released in the first quarter of 2019. It contained a number of improvements including advertising and caching enhancements, better state management and, most importantly, direction finding.

Direction finding

The revolutionary direction-finding feature that was introduced in Bluetooth 5.1 combines proximity and positioning data to identify approximate physical location down to a centimeter (.39 inches).

This feature utilizes two different methods for determining the angle that a Bluetooth signal is being transmitted from with a high degree of accuracy. The two methods are called Angle of Arrival (AoA) and Angle of Departure (AoD).

Each technique requires one of the two communicating devices to have an array of multiple antennae, with the antenna array included in the receiving device when the AoA method is used and in the transmitting device when using AoD. Direction finding offers numerous benefits including indoor asset tracking, wayfinding, employee monitoring, security and proximity-based applications like lighting and building control.

BLUETOOTH 5.2 UPDATES

Bluetooth 5.2 was released in 2020. It contains several updates including Bluetooth LE Audio that enhances performance of Bluetooth audio, adds support for hearing aids and introduces the sharing of multi-channel audio streaming. Other key Bluetooth 5.2 updates:

- LE power control (LEPC)
- Enhanced attribute protocol (EATT)

LE power control (LEPC)

In wireless communication, the Received Signal Strength Indicator (RSSI) can be used to estimate the distance of the receiver from a transmitter if the original transmission strength is known to the receiver.

A key benefit from LEPC is the conservation of output power used to maintain active connections. The foundation for this feature is created by setting output power to the lowest value where a stable link can be maintained within a given margin. This allows for minimum power consumption on both receiver and transmitting ends. The benefits are interference reduction and the ability to have more units in the same area. Cellphone service providers have applied this technology in their networks for many years.

With the new LEPC feature, a receiving device monitoring the level of the signal (the RSSI) from a connected device may request a change in the transmission power level used by its peer in either direction. A transmitter may also change the transmission power voluntarily and relay that information to the receiver.

Utilizing LEPC and keeping the RSSI within the optimal range of the receiver provides the following benefits:

- Better quality control of the signal
- Reduced data transmission errors at the receiving end
- Improved coexistence with other non-Bluetooth signals like Wi-Fi

Enhanced attribute protocol (EATT)

The original unenhanced attribute protocol used in previous versions of Bluetooth operates in a sequential manner. The new EATT provides the capability to perform parallel transactions between a Bluetooth LE client and a server. A benefit of this is the ability of the EATT protocol to help reduce the operational latency in applications. Instead of single transaction from an application being executed at one time, multiple transactions are now possible simultaneously.

The benefits of this are immense in industrial IoT, AI and Edge computing applications where sensor data is continuously being received, processed and often quickly acted upon with little human oversight.

BLUETOOTH IN INDUSTRIAL IOT (IIOT)

Bluetooth has received a lot of attention in consumer applications, but it's also incredibly well-suited for AI, Edge computing and smart industrial applications. Bluetooth is helping drive Industrial Internet of Things (IIoT) systems, which are shaping smart factories and the growth of Industry 4.0.

Connected Bluetooth devices and sensors at a single smart factory can gather up to 1.44 billion data points per day, even from legacy equipment. This raw data is extremely valuable in making business decisions once it is collected, secured and analyzed. One such benefit of this collected data is the reduction of equipment failure and downtime. Research by Deloitte has shown that poor maintenance can reduce a plant's productivity by 5 to 20 percent and cost manufacturers worldwide an estimated $50 billion annually.

5 WAYS BLUETOOTH IS WELL-SUITED FOR IIOT

1. Bluetooth is highly resistant to interference.

Adaptive frequency hopping helps ensure data successfully makes its way through the noise clutter. Individual messages are broken into small data packets, which are sent securely over different channels in a predefined sequence, known only to the transmitting and receiving devices. As many as 1,600 channel-switches can take place every second.

2. Bluetooth can operate many wireless devices in the same space.

Bluetooth allows for the operation of large numbers of devices in close proximity, perfect for the smart factory environment. Short data packages, which are ideal for industrial measurement and control applications, only need to be briefly transmitted over the air. Bluetooth's automatic power control features ensure that data is broadcast at only the required strength, saving on power and reducing noise. These factors help free up airwaves for other devices to share.

3. Bluetooth can correct errors.

When data is transmitted over long distances, in noisy environments or areas with physical interference the chance of errors entering the data stream increases. Bluetooth can automatically correct these by switching data channels or through Forward Error Correction (FEC) once data arrives at the receiver.

4. Bluetooth can be integrated with existing industrial systems.

Many industrial devices still rely on serial ports, but these devices can still be adapted to Bluetooth through a Universally Unique Identifier (UUID). Bluetooth LE provides for a separate UUID that identifies each device. The UUID is also used by the Bluetooth application to help process data. The code running on the connected Bluetooth devices can all be the same, the only difference would be the UUID.

5. Bluetooth has built-in security.

In addition to secure programming and secure provisioning, three other security features make Bluetooth a great platform for sharing data wirelessly. The first is adaptive frequency hopping that transmits data on a random sequence of channels. The second is the LE Secure Connections feature in Bluetooth 4.2 and newer that prevents data from being intercepted in man-in-the-middle cyberattacks. The third is that Bluetooth devices can be made invisible, meaning hackers can't discover them. Device connections are only permitted between devices that have been previously paired. Regardless of the path chosen for security, redundancy is strongly recommended.

BUILDING THE RIGHT SECURITY FOUNDATION FOR CONNECTED DEVICES

Connectivity is vital for most modern devices. It's no longer just for computers, smartphones or tablets. Televisions, baby monitors, thermostats, medical devices, automobiles and even aircraft are all connected today.

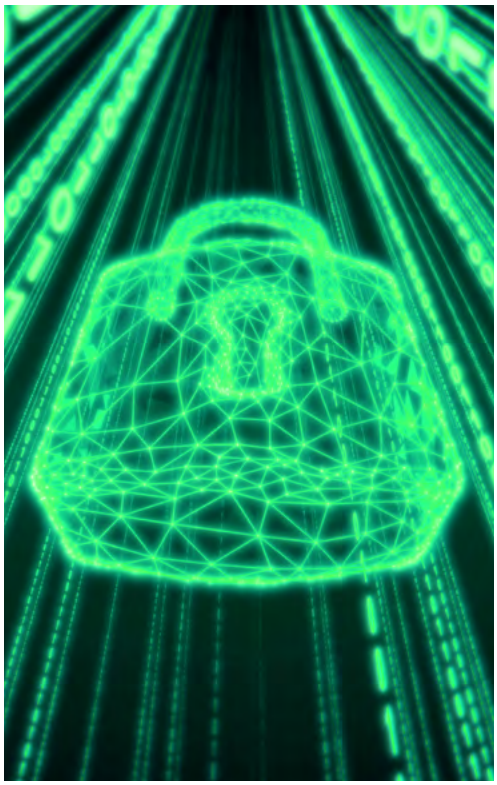
With growing connectivity comes increased security concerns. Connected devices need to establish proof of identity and origin in order to reliably determine appropriate data sharing and control with other devices and service providers. This process is defined as authentication.

Authentication is a key aspect of security that ensures robust access to trusted agents and easy identification of suspicious activity. With product-level authentication, clones and suspicious agents aren't validated so network and device access are denied. This is especially critical in applications for automotive, industrial, medical and aviation where human and environmental safety is paramount.

With any connected device, serious security planning must be factored into the early stages of the design process. Waiting until the end of the design process risks project schedule delays, drives up costs and creates unforeseen vulnerabilities in device security. Well-planned security delivers strong value by helping the device function properly from the start, avoid potentially expensive litigation and the detrimental effects to a company's brand image caused by hacking.

SECURE PROGRAMMING VS. SECURE PROVISIONING: THE RIGHT SOLUTION

What are the best ways to protect devices and software from intellectual property (IP) theft, cloning and malicious system hacking? Two primary solutions are associated with device security: secure programming and secure provisioning. Which option is best for your application? While both solutions provide security solutions, there are key differences.



SECURE PROGRAMMING

First, secure programming requires all data be generated/obtained outside the device itself, increasing the opportunity for that data to be compromised. Except for certain field programmable gate arrays (FPGAs) and multiprocessor system on a chip (MPSoCs), secure programming provides security through software that resides on the device. This can protect firmware on the device but does not provide adequate protection from some cyberattacks like counterfeiting and overbuilding.

Software defects and bugs in programming are vulnerabilities continuously exploited by hackers. Once software-based security is compromised, system recovery becomes nearly impossible. Secure programming is suitable for low-level applications that don't require advanced security, or in cases where a malfunction won't cause injury or harm to a person or property. It's also suitable for devices specifically designed to provide security without requiring bidirectional communication with the programming system. Secure programming doesn't rely on additional hardware, which delivers some cost savings at the expense of more robust security.

SECURE PROVISIONING

Secure provisioning employs added hardware in providing the best security protection for the complete lifecycle of the device. While the additional hardware will come at a financial cost, the prices are often very reasonable and can save a company expensive litigation and brand damage resulting from hacking. Secure provisioning also delivers firmware protection and prevents overbuilding, counterfeiting and protects against software programming vulnerabilities. By having the root of trust anchored to hardware, device software and operations are protected. Hardware-based security also protects against unauthorized code reading and is more resilient to physical attacks. Secure provisioning provides critical protection in devices that, if compromised, could cause harm to a person, property damage, loss of sensitive data or intellectual property.

TAKEAWAYS

By partnering with a trusted global technology partner, valuable resources can be better focused on intellectual property innovation and other areas that deliver a strong competitive edge. This partnership can improve business outcomes and customer journeys by providing the safe and reliable operation of Bluetooth devices.

Avnet and Nordic Semiconductor have partnered to deliver progressive solutions in Bluetooth technology that provide best-in-class performance of system on chip (SoC) devices that support Bluetooth 5/Bluetooth mesh/Thread/802.15.4/ANT/2.4GHz protocols.

NORDIC NRF52840

The Nordic nRF52840 is an advanced, highly flexible SoC solution for today's increasingly demanding Ultra-Low Power (ULP) wireless applications with complete multi-protocol support for Zigbee, Thread, Bluetooth LE and Bluetooth mesh networks. This powerful SoC fully supports Bluetooth 5+ by providing performance capabilities which include long range and high throughput modes. The nRF52840 delivers best-in-class security for CortexTM-M Series devices with an on-chip ARM® CryptoCell cryptographic accelerator operating independently of the CPU that supports secure provisioning with other connected devices. The **nRF52840 data sheet** provides more detail.

MARKET SOLUTIONS

Industrial automation / Industrial applications + IoT

- Handheld equipment interface / display solutions to manage device on cellphone vs. natively on device
- Sensors & remote controls

Learn more

Connected health

- Bluetooth LE connectivity / Cortex-M4 processing / Small scale design with USB for data/charging/ firmware upgrades
- Activity tracker, blood glucose and blood pressure measurement / Clinical health

Learn more

Connected home (Smart home)

- Smart locks, connected appliances, home kits (iOS app integration)

Learn more

About Avnet

With a century of success at our foundation, Avnet can guide you through our global technology ecosystem at any — or every — phase of your journey. Our experts support your innovation, turn your challenges into opportunities and build the right solutions for your success. Make your vision a reality and reach further with Avnet as your single trusted partner.

About Nordic Semiconductor

Nordic Semiconductor is a global technology provider that plays a key role in the realization of the wireless future. Nordic remains passionately committed to ultra-low power wireless technology done right.