What's New in Bluetooth v4.2

Application Note *v1.0*

Introduction

With the introduction of Laird's BL652 Bluetooth Smart + NFC modules, Laird introduces Bluetooth v4.2 to its portfolio of Bluetooth modules. Laird modules provide the best that the Bluetooth ecosystem has to offer, and the introduction of the BL652 brings the latest Bluetooth standard into our list of offerings.

Bluetooth v4.2 introduces a wide variety of new capabilities and features into the Bluetooth Smart ecosystem and pushes Bluetooth technology further into the forefront as a stable, secure, and flexible IoT technology. The advances of Bluetooth v4.2 empower heightened security, IPv6 addressing, even finer power optimization, and much much more.

New Features

The BL652 operates exclusively as a Bluetooth Smart, low energy device, often referred to simply as BLE. Whereas classic Bluetooth is designed for high-bandwidth data and audio applications, Bluetooth Smart is specifically meant for low-bandwidth applications where sensor data is intermittently relayed to a collection device. Bluetooth v4.2 introduces new features as well as significant improvements to existing features of Bluetooth Smart.

Enhanced Security

LE SECURE CONNECTIONS

ENHANCED PRIVACY

MAN IN THE MIDDLE PROTECTION

NFC-ENABLED PAIRING

LE Secure Connections

Major improvements have been introduced in Bluetooth v4.2 for increasing the security of Bluetooth Smart device connections. Low Energy connections no longer need to exchange the AES encryption keys over the connection and are FIPS capable, meaning Bluetooth Smart is fully compliant in applications with highly sensitive and confidential data. This is particularly relevant to the Medical market, especially in hospital applications, where medical OEMs can now utilize Bluetooth Smart modules that support v4.2 with full compliance to Federal Requirements.

Americas: +1-800-492-2320
Europe: +44-1628-858-940
Hong Kong: +852 2923 0610

With Bluetooth v4.2, the pairing process for BLE devices can now be secured using the **Elliptic Curve Diffie-Hellman (EDHC) algorithm** (if both ends are capable). This method uses a unique and robust scheme of private and public keys to mask the identities of both devices, making it extremely difficult to monitor the pairing process. This results in the same AES key being algorithmically generated at both ends without it actually being conveyed on the connection. Therefore, a listener cannot overhear the key, contrary to Bluetooth versions prior to v4.2.

What is FIPS?

The Federal Information Processing Standards (FIPS) are a series of regulatory guidelines for the processing and encryption of sensitive information. It is required in several industries, such as medical, in which a patient's sensitive information is handled and transmitted via electronic systems.

LE Privacy to Protect Your Device's Identity

In Bluetooth v4.2, maintaining device anonymity to scanning devices has been directly addressed through the **Privacy and Identity Tracking** mechanisms. Since Bluetooth v4.0, a mechanism has been implemented that allows the peripheral-mode device to use a randomly generated MAC address in packets that can be changed periodically (as frequently as every second). Bluetooth v4.0 and later devices utilize **Identity Resolving Keys** on both ends of the device, meaning that the randomly generated MAC no longer must be confirmed over the air but can be generated simultaneously on both ends of the connection. This makes it more difficult for a sniffer to identify which packets were sent by this device, since all the packets appear to be send from different devices. Using this process, a trusted device will always be able to determine that it is a known device from the varying MAC address.

Since Bluetooth v4.2, this random address filtering has been moved to the baseband layer, which allows this security feature to operate while utilizing even less power. This brings critical security to even more devices, meaning you don't have to compromise to achieve enterprise-grade privacy and security.

Man in the Middle Protection

Previous iterations of the Bluetooth standard have used methods to discourage Man in the Middle attacks on end devices. Bluetooth 4.2 introduces the **numeric comparison method** alongside the previously existing passkey entry and out of band pairing methods to significantly reduce the risk of active eavesdropping. During pairing, if both end devices are capable of display, they will both autonomously generate a six-digit number that is derived in part from the Diffie-Hellman algorithm. They will then both display this number, allowing the user to confirm the match. The probability of a Man in the Middle attacker generating this matching six-digit number is a mere .0001%.

NFC Pairing

In addition, Laird bolsters this security with our own contribution that vastly reduces the likelihood of interception, utilizing NFC as a pairing mechanism. In combination with LE Secure Connections, NFC-based proximity pairing addresses man-in-the-middle interceptions and ensures you always pair to the correct device securely.

Enhanced Performance

LE Data Length Extensions for Faster Communication and Higher Packet Capacity

Bluetooth Smart was designed for intermittent, small packet transmissions in sensors and other low-throughput devices. The architecture of the Bluetooth v4.0 specification is well suited to the vast majority of applications like these. However, Bluetooth v4.2 introduces the flexibility to increase the data payload of a packet from 27

Americas: +1-800-492-2320
Europe: +44-1628-858-940
Hong Kong: +852 2923 0600

octets to 251 octets. This is nearly 10 times larger and makes transmission 2.5 times faster than previously possible, giving you the flexibility to allow higher-volume packets in scenarios that require them.

CONCLUSION

Bluetooth v4.0 introduced the concept and framework for a new generation of sensor devices that opened a new class of devices into the internet of things: Bluetooth Smart. With Bluetooth v4.2, the scope and features of Bluetooth Smart have been broadened and strengthened in the critical areas of device security, data security, and data packet size. These improvements enable Bluetooth Smart devices to achieve higher volume transmissions when needed, and ensures they're compliant with the most stringent security requirements (such as FIPS) in sensitive industries like medical. Visit http://www.lairdtech.com/products/bl652-ble-module to learn more about Laird's BL652 Bluetooth v4.2 module.

REVISION HISTORY

Version	Date	Notes	Approver
1.0	20 July 2016	Initial Release	Jonathan Kaye

Americas: +1-800-492-2320
Europe: +44-1628-858-940
Hong Kong: +852 2923 0600