# A look into Bluetooth v4.2 for Low Energy Products

**Gustavo Litovsky** - May 04, 2015

The Bluetooth v4.2 Specification was officially adopted in December of 2014 by the Bluetooth Special Interest Group (Bluetooth SIG) and it brings a host of updates to Bluetooth Low Energy (BLE) or Low Energy (LE) for short. Although no Bluetooth chipset vendor is officially supporting it yet, support will make its way into devices in the next few quarters. There are quite a few updates in the v4.2 specification, and we're going to go over them and how they can affect your product and design decisions.

**LE Data Packet Length Extension**

One of the most exciting changes in the specifications is the increase in the Packet Data Unit (PDU) size from 27 to 251 bytes. This is the amount of data sent during connection events. To support the increase requires several updates. One difference is a change in the Header of the Data PDU. This header precedes the payload sent. In the header, the packet length field increased from 5 bits to 8 bits. Below is the header for the Data Channel PDU, comparing the v4.2 and v4.1 (v4.0 as well) variants:

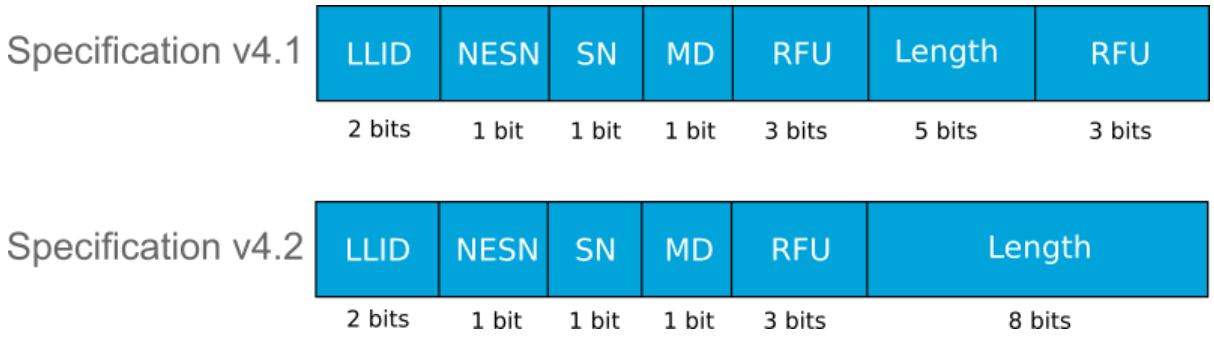



*Figure 1 - Comparison of Data PDU Header Definition*

The extra 3 bits used from the Reserved for Future Use (RFU) field enable the controller to indicate that the packets it is sending are up to 256 bytes.

Although the length field has a range of 0 to 255 bytes (for 8 bits), the MIC at the end of the packet is 4 octets (bytes) long, so that leaves us with 251 bytes which is the maximum payload size.

As part of the connection process, both devices go through a data length update procedure where the LL_LENGTH_REQ_PDU and the LL_LENGTH_RSP PUD are exchanged to negotiate the maximum size used. During this process, any data already queued uses the previous size. If a device

sends a LL_LENGTH_REQ to a device that doesn't support it, it will receive a LL_UNKNOWN_RSP PDU back. This allows backward compatibility with devices that don't support the longer length packets, such as v4.1 and v4.0 devices.

The extra packet length is extremely important in the emerging IoT applications and for many current products, as we'll see.

Take, for example, Over-The-Air (OTA) Updates, one of the most important features that products implement aside from their main functionality.

Even after a BLE product is sold, it's common to continue and update the firmware on devices with both new features and bug fixes. Due to the 27 byte limit of Bluetooth v4.0/v4.1, a full OTA download can end up taking 10 minutes in some cases. This can be very frustrating for customers who expect fast updates. Interference and connection loss may happen during this long period, so it's not uncommon to have an OTA process fail. With v4.1's byte limitation, the workarounds to this issue are expensive and complicated, so in reality only faster speeds are the solution.

With Bluetooth v4.2, you get a theoretical data rate of 800kb/s (increased from 270kbps for v4.0 & v4.1). In practice, of course, you won't get 800kb/s because of data overhead, throughput limitations in other devices, interference, etc. but you can expect firmware downloads to go much faster.

OTA isn't the only case where high data rates are used. Sensor logging applications are also becoming increasingly common, where large amounts of data are transferred. Faster data transfer reduces errors since transmissions are shorter and leave less time for other devices to interfere. It also speeds up the overall system and improves user experience due to lower latency.

Larger packets also prevent the fragmentation needed to transmit data in IPv6 data packets that would otherwise be split into 27 byte packets.

Efficiency is another advantage with large packets. When sending multiple 27 byte packets, there's significant header overhead since every packet has its own header and needs to be reassembled and processed separately.

As an example, using 27 byte packets, a 160 byte message would require 6 transmissions. In addition to the data, each transmission adds a 2 byte header, plus the optional 4 byte Message Integrity Check (MIC helps detect errors and is required in some cases when encryption is used). So, we would have sent an extra 36 bytes for a total of 196 bytes.

With the increased packet length only one header and one MIC are needed for a total length of 166 bytes, so we reduce the number of bytes sent by 15%. The radio can then stay off for 15% more of the time, reducing power consumption.

What's worse with small packets is that the extra packets don't just incur the extra time during transmission, but also waste time in starting up, dead time between transmission, processing, etc.

Less packets sent mean less power is used, which is extremely good for BLE applications. The small payload in BLE data packets is probably one of the biggest issues developers are facing, and it's good to see the Bluetooth SIG made it a priority.

**LE Secure Connections**

**LE Secure Connections**

From its inception, BLE left a lot to be desired from a security standpoint. In designing the security in LE, the designers left out some of the proven security features and the key-exchange mechanism used in Classic Bluetooth. By removing these features in the original v4.0 specification, the Bluetooth SIG simplified the LE controllers and helped lower the cost of BLE products, but it also made BLE insecure. With medical devices, locks and other security critical devices adopting BLE due to ease of use and integration, security had to improve.

To understand the problem with Bluetooth v4.0 LE security, we have to look at how Bluetooth devices ensure they are talking to each other. The process is called an association mechanism. How this process is secured also makes a big difference. You can find more information on BLE Security and the association mechanisms mentioned below on the Bluetooth SIG's website. There are a few common scenarios when you buy a new BLE device and you want to pair it to your smartphone (or some other BLE device):

1. You bought a device that has no buttons and no display, and you want to pair it to your smartphone. In this case, the device has no I/O capability so the association mechanism used is called Just Works. This mechanism assumes the number 0 in both the BLE device and smartphone. This is the least secure method because an attacker knows when it's used and knows that the fixed value is 0.
2. You bought a device that has buttons (like a keyboard) but no display and you want to pair it to a smartphone. Your smartphone shows a 6 digit number during pairing and you type it into the BLE device. This method is called Passkey Entry. It is slightly more secure than Just Works because the PIN is 6 digits.
3. You bought a device that has a display and a yes/no button and want to pair it. Only the insecure Just Works method can be used since the Numeric Comparison method is not available in Bluetooth v4.1 and prior.
4. You bought a device that has another interface, such as NFC, and your smartphone supports NFC as well. In this case, NFC can be used to perform the pairing securely using what is called Out-O--Band communications (because it doesn't use BLE at all). This is secure depending on the security of NFC.

So BLE v4.0 and v4.1 support only 3 association mechanisms, Just Works, Passkey and Out-Of-Band.

In both Just Works and Passkey, the two devices (BLE and Smartphone) have to exchange information on an insecure BLE channel (because no security has been established). This insecurity means that a passive eavesdropper (someone just sniffing BLE packets) can get all the necessary data to break the encryption. What is needed is a Key Exchange mechanism that is secure regardless. This is where the Elliptic Curve Diffie-Hellman (ECDH) key agreement protocol comes into play. ECDH is a cryptographic protocol that allows two devices that have not interacted before to securely exchange information.

Bluetooth v4.2 finally adds ECDH for the key exchange as a new security method called LE Secure Connections, so the key exchange is secure against passive eavesdroppers. This also allows for the BLE communications to be secure against MITM attacks with the right association model.

Because ECDH was not available in the initial BLE specification, many product manufacturers developed their own security on the application layer. This in turn meant that consumers depended on the security implementation of each vendor, which could be flawed. It also prevented interoperability since the Smartphone App or other BLE device needed the same proprietary security mechanism.

Standardized security means consumers can rely on it, and you can focus on developing the product, not re-inventing the wheel.

**Link Layer Privacy**

BLE packets include a source address, which means that a BLE device can be tracked as it is moving and communicating, unless it changes its address periodically. This was and continues to be a concern with Classic Bluetooth which can be tracked because a fixed static address is used. BLE added the ability to periodically change the address it uses in the packets. But, to be able to communicate with a device that's constantly changing its address means that its real address has to be resolvable.

When a device wants to remain private, it uses private addresses. In the case of Resolvable Private Addresses, where the device wants to be identified, the addresses are generated by an algorithm using the Identity Resolving Key (IRK). This key is another cryptographic key exchanged between the Master and Slave during pairing. Because the addresses are not random but depend on a key, another device that has the IRK can identify the device even though it is changing its addresses.

In Bluetooth v4.2, the address resolution has been moved from the CPU to the controller, so that the CPU doesn't need to wake up. Even better is the fact that the controller can decide to wake up the host only when a trusted device is in range. Both of these features help lower the power consumption of BLE in real-world scenarios while helping keep a user private.

**Link Layer Extended Scanner Filter Policies**

**Link Layer Extended Scanner Filter Policies**

Bluetooth Low Energy helps lower power consumption by filtering advertisements at the lowest layers. This has proven to be extremely helpful in Smartphones, where background scanning can drain the battery significantly. In previous versions of the specification, BLE could either ignore all advertising packets, or accept those in a whitelist.

The Scanner filter in v4.2 can now use the resolvable private addresses as well as part of the filtering process.

**IoT and the IPSP Profile**

All the changes in Bluetooth v4.2 make BLE lower power, and help make products better for users. But Bluetooth is gearing to position itself better on the IoT stage, so a few words on this are in order.

Around the same time it adopted the Core Specification, the Bluetooth SIG also adopted the Internet Protocol Support Profile (IPSP) which helps devices using IPv6 (the most recent version) over BLE to communicate.

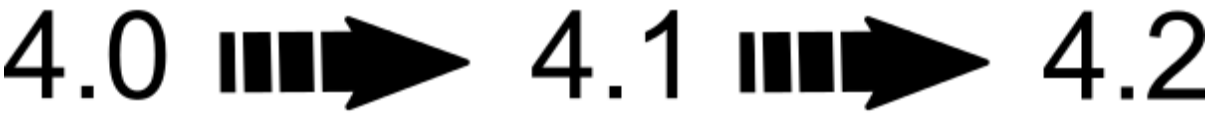
IPSP isn't part of the Core Specification, but it's probably the biggest beneficiary of the new changes, since larger data packets help transfer large UDP/TCP packets faster. IPv6 is one of the reasons for many of the changes in the specification and allows BLE devices to connect directly to the internet.

Unlike Zigbee which supports mesh networking, Bluetooth Smart (the official marketing designation for Bluetooth Low Energy), is mostly a point-to-point standard. CSR is the only vendor that provides mesh capabilities in its devices, but it has not been adopted by other vendors. The mesh capability is being worked on at the Bluetooth SIG, which is rumored to be including it in the Bluetooth v4.3 release.

Devices using the current v4.1 specification can communicate with a BLE to Internet gateway using the IPSP profile, as Nordic Semiconductor recently demonstrated . But it will require Bluetooth v4.2 with its larger packets to really make it viable from an energy and speed standpoint.

Once both IPv6 support and mesh capabilities are rolled into BLE (mesh is currently being developed by the SIG Mesh Workgroup), Zigbee will likely find itself with significant competition as the brand recognition and sheer amount of critical mass gained by Bluetooth will help it pull past Zigbee. Some consumer home routers include radio chipsets that may support BLE out of the box with just a firmware change, which makes BLE solutions less expensive and simpler to use. Consumers may thus avoid buying a separate gateway.

**Making the Leap to v4.2**




Four months after the adoption of the new specification, there still aren't many devices qualified for v4.2, though the Bluetooth SIG shows a few vendors such as MediaTek, Broadcom, MindTree and CSR with qualified controllers or components. Many of the changes to the specifications require hardware changes, so it may not be until late 2015 or early 2016 before v4.2 devices show up.

Using new hardware and software brings risk. It takes time for most chipset vendors to provide mature silicon and software and hammer out any bugs. Whether you should go ahead as soon as

devices appear depends on a few things, including your risk tolerance and willingness to take the time to work with the vendor to investigate issues.

1. If you transfer a lot of data or perform frequent OTA updates, then v4.2 will help you do it faster. This can have a big impact on your users. For applications that log information it's almost a must from a time and energy consumption perspective.
2. If you need security and haven't implemented your own application layer key-exchange mechanism, then the new security features will help you avoid the time spent doing so.

Choosing the right chipset and getting the operation right is still critical.

The new specification also has a few other aspects you should consider:

- Testing equipment needs to be updated to support the new tests needed for v4.2 qualification

- Your product will need to qualify for the updated specification, adding cost and time to market since many modules and devices are not v4.2 qualified

- One of the biggest issues will be Smartphone support for the new features, although Apple, Samsung, and other Smartphone developers have been preparing for v4.2. A new firmware update can add support for the new features, but there will still be consumers with older phones supporting only v4.1 or v4.0. This means you still have to test and support those versions until the market acceptance becomes more widespread.

- For those already in production, switching parts can be a costly thing. After all, you need to manage leftover and unused inventory. This also affects everything from customer satisfaction and customer support and issues resolution.

To really make use of the improved throughput may also force you to change your firmware to take advantage of DMAs or other quick transfer mechanisms.

Despite all this, it's evident the new v4.2 specification helps make BLE faster, lower power, and more secure. These updates will help you create new products for new applications and with better user experience, helping place Bluetooth Low Energy at the center of the IoT revolution.