A LOOK AT BLUETOOTH TECHNOLOGIES AND WHY THEY MATTER FOR YOUR MEDICAL DEVICE – PART 2: Security, restrictions and use applications

We are seeing a revolution in wireless biomedical device technologies and by far, the most popular that use WiFi and cellular applications are Bluetooth Classic and Bluetooth Low Energy (BLE).

Significance of Connectivity Choices

In Part 1, we defined general use cases for Bluetooth Classic and BLE. For continuous connectivity, Bluetooth Classic may be the best choice, and when a system calls for intermittent, as-needed use, BLE may be the wiser choice. By and large, each device's design is individual: it carries its own specific use profile and careful examination is suggested so that suboptimal choices are avoided.

We have found that the tendency exists for device manufacturers to commit their design to a specific operating system and connectivity protocol without considering how this might limit their device's system or type of functionality. The earlier that these factors and their options can be brought out, discussed and more carefully examined in the development cycle of a product, the fewer cost overruns and delays will be experienced.

Use of BLE in Android and iOS

One difference to consider is that BLE allows for about twice as much throughput in Android as it does in iOS. (Throughput is defined as the rate of successful data delivery over a communication channel.)

The caveat here is that speed is a negotiated parameter and different operating systems will negotiate them differently. It has been our observation that Android will typically negotiate a higher throughput speed than iOS will. That does not mean that throughputs are always higher on Android, however. Because of packet loss and re-transmission the effective throughput rate may be less. Other factors affecting throughput rate are the processing power of the device to which the radio is attached, the number of processes the device is running, the number of data streams that the chip is handling, etc.

Unlike operations using Bluetooth Classic or BLE with Android, iOS restricts the ability for a connected device to "wake up" or verify an application on the iOS device. Despite attempts to get the application to periodically verify, iOS application management forces a 10-second hard shutdown for that type of activity. For many types of use case, such as continuous monitoring of ECG or other waveform data, that's simply not enough time.

Therefore, certain applications can be said to be suboptimal when using BLE in an iOS environment, such as passive activities and continuous monitoring.

BLE requires a user in order to maintain a connection and transmit data. Incidentally, this means that the application/system must give the user a reason to connect periodically.

Security Considerations

In a word, security is an important consideration when selecting a connection protocol for your medical device because of cyber threats. All medical devices carry an element of security risk,

and threats such as device tracking, eavesdropping and man-In-the-middle (MITM) attacks are increasing significantly. Additionally, many integrated systems are connected to central processing units which often utilize commercially-available software and off-the-shelf hardware. As such, these systems may be at increased risk of cyber threat, especially with increased use.

Computer viruses and gaining access through wireless connections can endanger high concentrations of medical device systems in the healthcare environment unless hospitals and other facilities take appropriate risk mitigation measures.

Security measures found in Bluetooth Classic and BLE, as well as in software and firmware updates within the specific medical device networks, can decrease vulnerabilities.

Bluetooth Classic security: As stated in our Part 1 article, pairing is mandatory in Bluetooth Classic, providing a level of security since only those trusted devices will communicate. This is accomplished via Secure Simple Pairing (SSP).

BLE security: BLE provides two options. One, pairing is not required and data is advertised publicly. Two, secured pairing can be enabled on a BLE device to ensure that only authorized devices are connected.

It is never recommended that medical device networks bypass pairing. Since the majority of data packets sent via BLE contain the source addresses of the medical devices, third-party devices are able to associate the addresses to a particular user identity and track them.

BLE supports a Privacy Feature that reduces the ability to track a device over a period of time by changing the Bluetooth device address on a frequent basis. This frequently-changing address is called the private address and the trusted (paired) devices can resolve it.

The following are provided by the Bluetooth Special Interest Group and cover the subjects of Privacy and Security with regard to the Bluetooth Classic and BLE technologies

Bluetooth Core Specification

BLE Security:

Examples of Use

Following are examples of two successful Bluetooth-based systems. Each example illustrates a continuous remote monitoring system. The main differences are in the protocols used.

Medical device startup Nanowear designed a system to monitor chronically ill patients that incorporates iOS and Bluetooth Classic with embedded nanosensors in undergarments that monitor heart rate, respiratory data and ECG. Their system caters to the long-term needs of patients who need to be monitored remotely.

Another startup, PhysIQ developed a system that employs use of Android and BLE for remote monitoring of ECG and other vital signs, then sends out alerts from wearable biosensors based on differentials to baseline patterns in their patients.

Why is this important?
Although other connective technologies exist, new devices employing Bluetooth Classic and BLE connectivity continue to emerge in the marketplace. Understanding their attributes as well as the existent security issues, limitations with iOS and Android as well as how they may affect device functionality, can encourage discussions that lead to well-thought-out solutions. They should also aid in the successful development of new device technologies.

Whether you need a continuous or periodic connection between your device and smartphone; large or small package transmission size; support for multiple platforms or just one—all are considerations in your protocol selection.

Lessons Learned/Key Takeaways

- Think about what kinds of uses your connected medical device and companion software system will be put to
- BLE on iOS will severely restrict what types of systems you can build.

Related Posts

- Testing for mobile and connected care
- Parallel Hardware and Software Development
- Requirements and Validation before you start building
- Designing hardware with a consideration to its companion software
- Pitfalls of Bluetooth for medical devices
- Pros and Cons of different types of connectivity for medical devices
- Leveraging pre-built chipsets/assemblages and how to evaluate them