Laird™
CONNECTIVITY

Bluetooth Deployment in Hospital Settings

Introduction

There is no argument that the global rise of wireless connectivity continues to increase and at a rapid pace. The majority of the world population is now connected to the internet. Business Insider (BI) Intelligence estimated years ago that by 2020, 24 *billion* devices would be connected to the IoT or Internet of Things. As connectivity increases, so does our reliance on it which reinforces its use in a wide range of environments and situations.

Hospitals and other healthcare settings are not immune to this trend. Between the sky-rocketing use of personal monitoring devices and the fact that actual medical equipment is increasingly going wireless, healthcare in general has become far more mobile than ever before. With this mobility comes ever increasing pressure for consistent and reliable wireless connectivity to effectively manage and support patient care.

Even more critical than consistency and reliability is the need for secure wireless connectivity. According to a 2022 IBM Security study, healthcare data breaches cost the industry, on average, $10.1 million per incident, up 41.6% from 2020. If compromised, healthcare facilities can face not just legal expense, but costs related to patient notifications, breach detection, and the cost of responding to and fixing the breach. Adding to these financial expenses, they can also suffer the expense of downtime while the problem is repaired, damage to their reputation, and the loss of patient trust.

There are currently three primary wireless connectivity methods that are used for IoT within hospital settings – Wi-Fi, Bluetooth, and (increasingly) ultra-wideband or UWB – a short-range, very high frequency wireless technology). With the rapid pace of innovation and the increasing growth of IoT, healthcare providers experience more and more pressure to adopt these wireless technologies (individually or as part of a multi-technology network) for both improved patient care and a reduction in cost (a priority of both for-profit and non-profit organizations alike). Added to this pressure are the challenges (and headaches) that accompany the proper deployment of an effective wireless network.

There are currently three primary wireless connectivity methods that are used for IoT within hospital settings – Wi-Fi, Bluetooth, and (increasingly) ultra-wideband or UWB – a short-range, very high frequency wireless technology).

Bluetooth is an innovative way to improve patient care, make healthcare operations more efficient (and quicker with the aid of AI processing the generated data), decrease clinical errors, and reduce the overall costs. This white paper describes several Bluetooth technologies that enable its reliability and efficiency in hospital settings.

This white paper focuses on Bluetooth technology. The reason for this focus is to counter the fact that, traditionally, healthcare organizations have typically avoided relying on Bluetooth due to concerns about performance and security. Adding Bluetooth devices to hospital settings was simply adding yet one more RF technology in an already-congested wireless space. But, because the security aspect of Bluetooth is greatly improved and newer technologies counter the RF interference often caused by wireless overcrowding, Bluetooth is becoming a much more trustworthy connectivity solution even in hospitals and other healthcare facilities.

And this is good news! Bluetooth technology brings with it a variety of benefits to these environments:

- It's widely used, especially with its integration with smart phones, tablets, and personal monitoring devices;
- It's a low power technology which, with the addition of Bluetooth Low Energy, significantly extends battery life;
- It's a relatively low-cost solution for wireless connectivity;
- With newer technologies, it operates or cooperates well in noisy or crowded RF environments;
- New Bluetooth 5.2 features like LE Coded and 2M PHY yield higher throughput and longer range;
- With greater adoption in medical devices, Bluetooth LE is becoming common in healthcare environments, such as in surgical sensors, patient monitor peripherals. and asset/patient tracking Additionally, healthcare can extend to the patients' home, such as in as fitness trackers, blood pressure and glucose monitoring sensors. This decreases the length of hospital stays, increasing the comfort level of patients, and greatly reducing costs for both the hospitals and the patients.

In other words, Bluetooth is an innovative way to improve patient care, make healthcare operations more efficient (and quicker with the aid of AI processing the generated data), decrease clinical errors, *and* reduce the overall costs.

This white paper describes several Bluetooth technologies that enable its reliability and efficiency in hospital settings. We also provide a brief overview of Bluetooth security and its impact on reliability in hospital settings as well as counter the myth that Bluetooth and Wi-Fi cannot coexist in a medical environment.

Hospital Settings And Its Effect On Connectivity

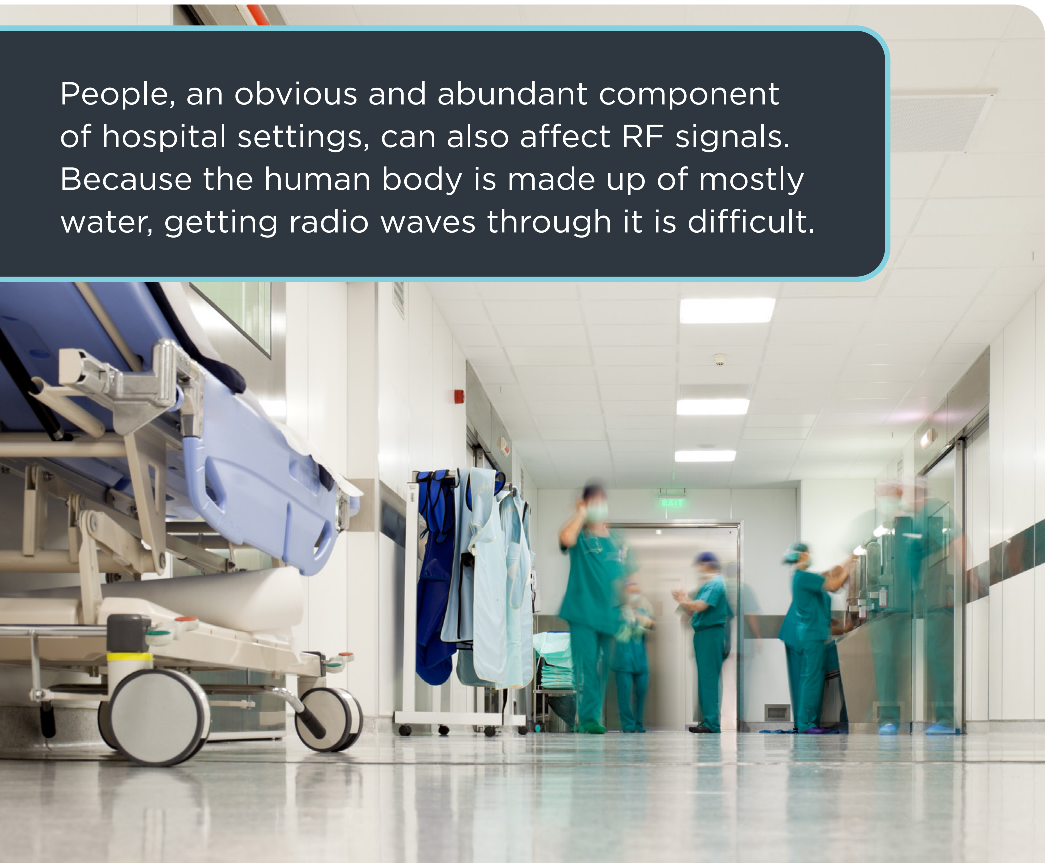
Hospital settings are both hectic and fast-paced. Yet, in the midst of this seemingly chaotic environment, hospitals provide critical, life-saving services on a daily basis to hundreds of thousands of patients. The evolution of connectivity technologies greatly enhances a hospital's ability to successfully deliver these vital services but the fact remains... there are a multitude of RF obstacles inherent to a hospital or other medical setting. The following are just a few of these obstacles.

Challenging Physical Environment

The challenging physical environment of hospital settings is brutal when it comes to the wireless connectivity that is required for RF technologies. Fundamentally, hospitals are made up of walls, electronic equipment, and a lot of people. Each of these components are obstacles to efficient and reliable wireless communication.

- Walls are often made of extremely dense materials such as concrete which can block radio-frequency signals
- The issue with general hospital equipment is three-fold:
  - It's often metallic, which can disrupt or block radio signals
  - It's often mobile, continuously and unpredictably moving throughout the hospital facility
  - The hospital environment itself is very vast, creating a challenge in terms of wireless coverage across the facility
- Hospital personnel often report that the use of industrial 900 MHz microwave ovens (often in use in hospital cafeterias and breakrooms) cause interference with their electronic hospital equipment.
- People, an obvious and abundant component of hospital settings, can also affect RF signals. Because the human body is made up of mostly water, getting radio waves through it is difficult. With so much inherent water, human body can both reflect and absorb RF energy which means that, the busier the hospital, the more likely the disruption of radio signals due to the vast number of patients, patients' families, and hospital personnel. This is especially applicable to the 2.4 GHz band.

> People, an obvious and abundant component of hospital settings, can also affect RF signals. Because the human body is made up of mostly water, getting radio waves through it is difficult.



Unpredictable Capacity

Hospitals generally operate all the time... 24/7. Sometimes these hospitals are busy and hectic while at other times they experience lulls in the chaos. The fact that they operate around the clock makes it difficult to predict capacity and plan for wireless connectivity needs. When the hospital faces an influx of patients, this means not only an increased use of wireless medical devices used to treat the patients, but a significant increase of associated non-medical devices as well. The patients and their accompanying family members or friends bring their own devices and their own bandwidth usage – streaming videos, movies, music as well as the plethora of other internet outlets (can anyone truly survive and thrive without constant connection to the internet?).

With the ever-growing reliance on wireless communication and the sheer number of wireless devices, it's important that hospitals can handle the varying bandwidth needs without sacrificing critical connectivity.

Unique Sites or Situations

Although hospitals in general serve a common purpose, there is no one-size-fits-all connectivity solution for healthcare facilities. Each situation or site is unique and requires a custom solution. Understanding the physicality of the site as well as predicted network needs.

Understanding Bluetooth Technologies

As we've already stated, Bluetooth technology brings with it many advantages to hospitals and other healthcare environments. By understanding various Bluetooth capabilities and how they work can enhance its use in medical facilities. This section delves into coexistence issues that may arise with the use of Bluetooth (and ways to mitigate them) as well as Bluetooth mesh technology which can greatly boost its connectivity performance.

Coexistence Between Bluetooth and Wi-Fi Technologies

Although the risk of interference is present, Bluetooth and Wi-Fi connectivity solutions can be deployed and successfully coexist in a single hospital environment. To better mitigate potential RF clashes between these two technologies, let's take a look at what types of interference could occur in a healthcare environment. The better we understand what causes what types of interference, the better able we are to reduce or avoid it altogether.

Within a hospital setting, there is a wide variety of both medical and non-medical equipment that can create RF interference. For example, there are likely different devices within the hospital that use Wi-Fi, Bluetooth, Zigbee, LTE, or ANT technologies, all of which operate in the 2.4 GHz band. This fact alone presents RF challenges when they are collocated and operate simultaneously. Add to this all of the personal devices being used by patients, patients' family and friends, as well as hospital personnel – streaming services, voice and video chats, general internet use – and you're likely dealing with some RF chaos.

While Bluetooth and Wi-Fi often use the same frequency band, they are practically non-competing technologies. Each has its own specific applications and, oftentimes, these applications even require that both technologies co-exist in the same network and sometimes even in the same system. If this coexistence isn't handled effectively, performance of both can be greatly affected. To ensure that Bluetooth and Wi-Fi technologies are not hindered by one another's presence, engineers must not overlook coexistence or collocation when designing RF systems that include both Bluetooth and Wi-Fi

> While Bluetooth and Wi-Fi often use the same frequency band, they are practically non-competing technologies. Each has its own specific applications and, oftentimes, these applications even require that both technologies co-exist in the same network and sometimes even in the same system.

Bluetooth Low Energy

Bluetooth Low Energy, also referred to as Bluetooth LE, is a low power yet extremely robust technology that is intended for situations where battery life is more important than high data rates. It's similar to Classic Bluetooth in the fact that both operate in the 2.4 GHz frequency band and are part of the Bluetooth Core Specification. But they operate in very different ways.

The most significant difference between the two and the reason why Bluetooth LE is an excellent connectivity solution for hospital settings is the fact that Bluetooth LE uses far less power than Classic Bluetooth. Bluetooth LE is ideal for applications that intermittently send small amounts of data – applications we see, for example, in a wide variety of medical devices such as blood glucose monitors and pumps, pulse oximeters, asthma inhalers, fitness trackers, blood pressure monitors, and more.

For reliable operation in the crowded 2.4 GHz frequency band, Bluetooth LE utilizes frequency-hopping spread spectrum methods that involve what's called a channel map update procedure. This procedure can be utilized with both non-adaptive channel blocking and Adaptive Frequency Hopping (AFH). We'll dive into both of these methods later in this paper. But first, we'll look at other spread spectrum technologies used by Wi-Fi and Classic Bluetooth.

Spread Spectrum

Both Wi-Fi and Bluetooth are based on spread spectrum signal structuring where, to put it simply, a narrow band signal is spread over a wider frequency band. In other words, with this radio transmission technique, a narrowband signal such as a stream of zeros and ones is expanded (or spread across a given portion of the radio frequency spectrum) to result in a broader or wideband signal.

Spread spectrum signaling was originally developed for military applications and offers two main benefits. First, a wideband signal is far less susceptible to intentional blocking (jamming) and unintentional blocking (noise or interference) than a narrowband signal. Second, a wideband signal sometimes can be perceived as a part of the noise floor (static interference) and thereby remain undetected.

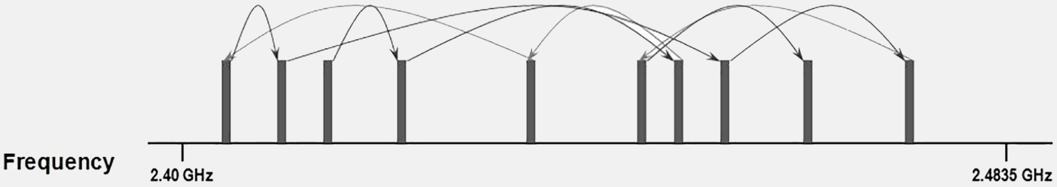


Figure 1: With Frequency Hopping Spread Spectrum, the signal is transmitted on different frequencies at intervals to spread the signal across a relatively wide operating band

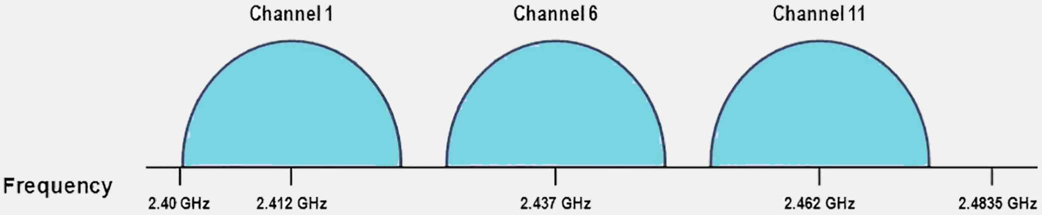


Figure 2: With Direct Sequence Spread Spectrum, the signal is transmitted on a continual basis across a range of frequencies referred to as a channel

The two most popular spread spectrum signal structuring techniques are Frequency Hopping Spread Spectrum (FHSS) and Direct Sequence Spread Spectrum (DSSS). Bluetooth uses FHSS whereas Wi-Fi uses DSSS. Given that both technologies operate in the same frequency band, this use of differing techniques is the heart of potential Wi-Fi/Bluetooth coexistence issues. FHSS devices and DSSS devices perceive each other as noise—Wi-Fi and Bluetooth are mutual interferers.

FHSS vs DSSS

FHSS spreads a narrowband signal by “hopping” across channels at set intervals in the 2.4 GHz frequency band. The transmitter and the receiver adhere to a common hopping pattern or sequence of channels during a given session so that the receiver is able to anticipate the frequency of the next transmission. Because of this, Bluetooth makes full use of the 2.4 GHz band.

DSSS starts with the same sort of narrowband signal as does FHSS but spreads that signal across a spectrum in a very different way. With DSSS, the narrowband signal is divided and then combined with a sequence called a chipping code. The chipping code spreads multiple copies of the original signal across a wider portion of the operating band to form a channel. Wi-Fi’s 2.4 GHz band overlaps with the Bluetooth range, and the Wi-Fi channels are 22 MHz wide. Because the 2.4 GHz band is 83 MHz wide, three non-overlapping Wi-Fi channels are available in Wi-Fi’s 2.4 GHz band. Upon receiving a wideband signal, the receiving station decodes the original narrowband signal by using the same chipping code as the transmitting station.

Channel Map Update

As you know, Bluetooth operates on the unlicensed 2.4 GHz ISM frequency band. Although the 5 GHz frequency band has absorbed some of the RF congestion, Bluetooth coexists on this 2.4 GHz band with Wi-Fi, ZigBee, and other commercial applications. It is important that Bluetooth devices can mitigate the interference and communicate effectively on this crowded frequency band.

The channel map update procedure (which was originally part of the Bluetooth 4.0 specification) allows peer devices to determine (or agree on) which channels are best to use – which ones are not hindered by interference. With this information, the master device can then initiate an update to the channel map, disabling any channel that is experiencing a level of interference that adversely affects communication performance. This update is driven solely on the master side.

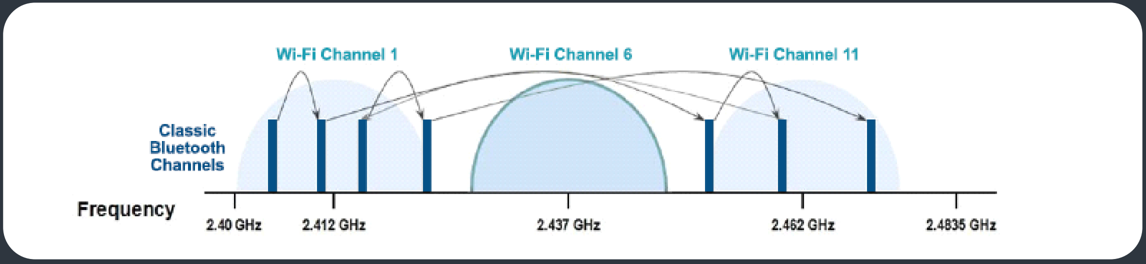
There are multiple ways that Bluetooth technology companies can implement channel map updates. At the most basic, ‘no frills’ level, channel map updates simply involve any of the associated Bluetooth devices detecting a channel with high interference and ‘suggesting’ that it not be used. The master device then disables this ‘bad’ channel and it remains disabled for the remainder of the current connection. If the interference dissipates, the channel still remains disabled until the devices are disconnected and a new connection is made.

There are two general methods to improve upon this most basic version of channel map updates. In some cases, Bluetooth technology companies develop and initiate their own (often proprietary) algorithm to manage this process. With an effective algorithm in place, the current Bluetooth connection can be monitored for interference across the channels. Periodic updates can then be made (whether to disable a 'bad' channel or re-enable a 'good' channel) based on channel performance and RSSI.

Other Bluetooth manufacturers use Adaptive Frequency Hopping (AFH) to tackle the issue of channel map updates. AFH means different things to different people, but in Bluetooth it involves scanning for busy channels and, when found, altering the channel map to avoid them. The key difference is that, with AFH, it is a dynamic process – the communication devices constantly monitor and can continuously change the channel map to mitigate the interference. Bad channels are excluded only until they are no longer congested. In addition, AFH involves the ability for the selected channel to frequently change to allow the transmission of data over a wider collection of channels to avoid interference and perform better in busy radio environments. Bluetooth Low Energy allows use of a channel map to mark bad channels, under control of the application

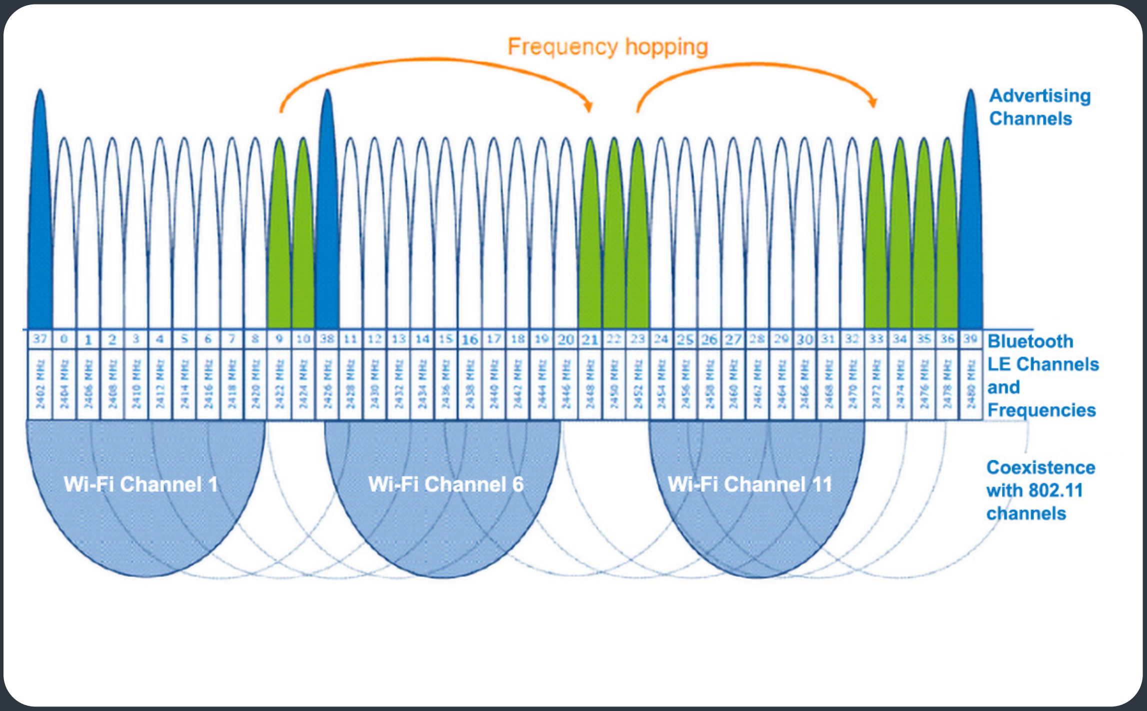
So, to summarize… channel map updating technologies universally monitor channel health to determine whether or not effective and reliable Bluetooth communication can occur. In addition, for all methods, the master device can disable any channel deemed 'bad' to ensure it's not used. The difference in specific technologies, to put it very basically, is how often this monitoring (and response to monitoring) occurs. Non-adaptive channel blocking might be implemented by keeping channels disabled until a new connection is made, or by periodically making updates to the channel map during the current connection. Adaptive Frequency Hopping, on the other hand, continuously monitors and dynamically adjusts selected channels accordingly. The selected channel can change (hop) frequently which allows Bluetooth communication over a wider group of channels.

Adaptive Frequency Hopping functions a bit differently between Classic Bluetooth and Bluetooth LE…



Classic Bluetooth: Radios scan on 79 individual one-Mhz wide operating channels.

Hopping occurs at a fixed rate: Every 1.25 msec



Bluetooth LE radios scan on 40 channels that are two megahertz wide with more tolerant modulation to get better penetration.

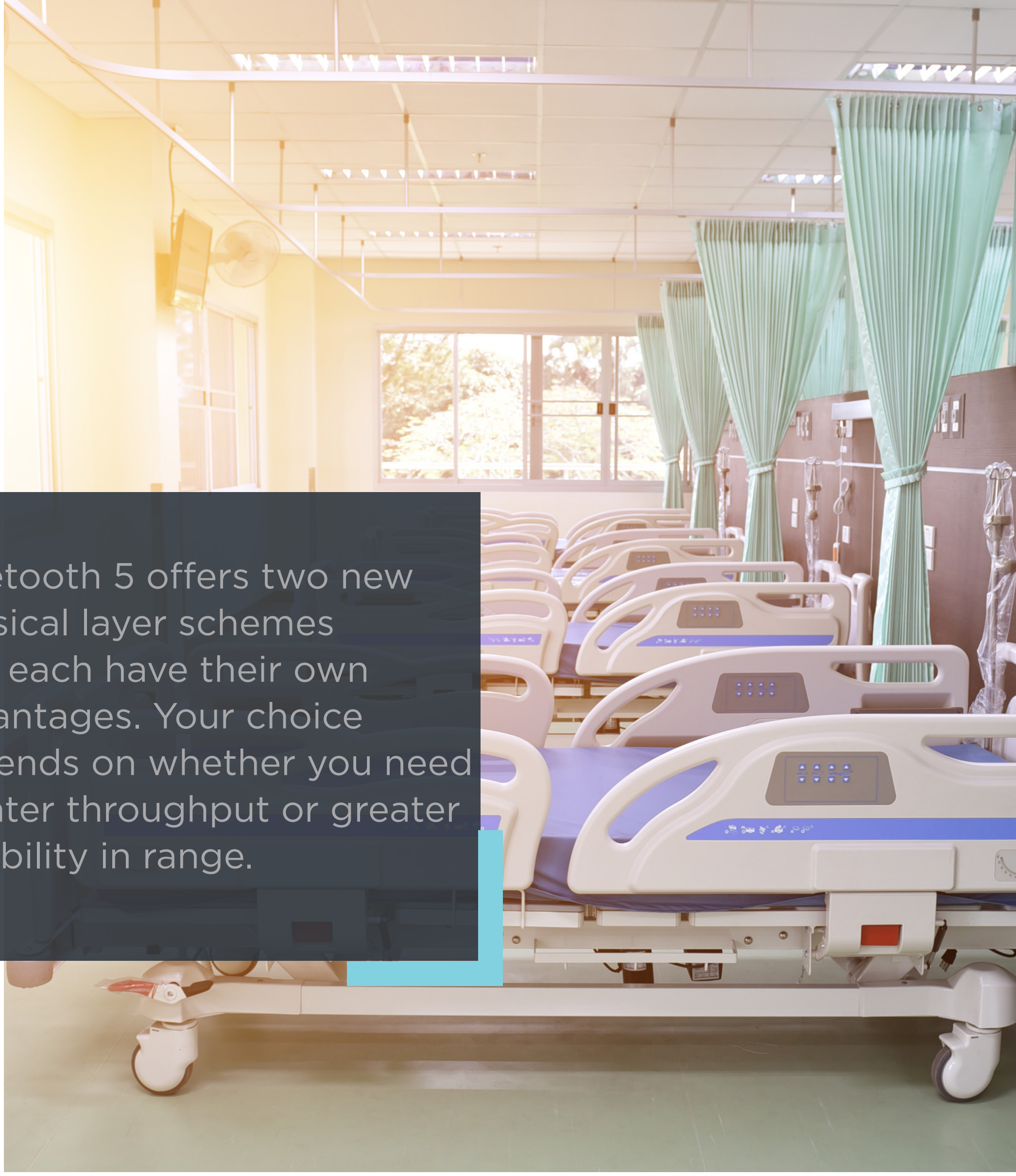
Hopping ranges from 7.5 msec to ~4 seconds (negotiated at the time of connection and can be renegotiated during the connection).

Throughput and Range Tradeoffs in Bluetooth LE

To adjust to difficult environments where Bluetooth connectivity might be challenged, Bluetooth 5 offers two new physical layer schemes that each have their own advantages. Your choice depends on whether you need greater throughput or greater reliability in range.

Better Range with LE Coded PHY

Bluetooth 5 has an excellent feature for expanding the range of wireless devices, called LE Long Range/ Coded PHY, which provides increased range not by increasing the output power but by using bit expansion using Forward Error Correction (FEC) coding. It sends each bit in the data packet as coded 2- or 8-bits in order to give more devices at farther distances the opportunity to successfully receive transmissions.



> Bluetooth 5 offers two new physical layer schemes that each have their own advantages. Your choice depends on whether you need greater throughput or greater reliability in range.

Initially, it may not seem plausible that simple expansion can truly improve the range of listening devices that can successfully receive transmissions – especially since range issues have traditionally been solved by pushing more power into antennas. But there's a simple analogy that illustrates it in everyday terms: if there is a large room of people at various distances from you, only the closest people will be able to closely follow a story you are telling at a normal speaking voice. Let's say everyone within eight feet of you. To help more people follow along, you could yell your story (i.e. increase power to the antenna to amplify output), or you could continue speaking at a normal volume but repeat each word two or eight times. Each person in the room would simply need to hear one of those repetitions to follow your story, which gives the people in the back of the room a far better chance to understand what you're saying.

Repetition is remarkably effective at increasing range without the need to "yell across the room," and testing by the Laird Connectivity team and other organizations show that LE Long Range/Coded PHY can successfully increase range up to 4 times while also improving sensitivity of receiving devices by 4 or 12 dB.

Higher Throughput with LE 2M PHY

Prior to Bluetooth 5, BLE operated on 1 Mbps modulation only. Bluetooth 5 adds support for an 2 Mbps PHY, known as LE 2M PHY. It allows data to be transmitted at the higher two Mbps symbol rate, which achieves around 1.5x the final throughput of the original 1 Mbps modulation.

Both 2M PLY and LE Coded PHY achieve their results without an increase in power, and both have their advantages and disadvantages. In general, if higher throughput isn't a requirement for your application, LE Coded PHY provides an obvious advantage. Connectivity in medical applications is critical, and LE Coded PHY provides a reliability boost, especially considering the densely populated environment of a hospital.

Ultimately it's about choice and flexibility, and your application and environment can make the decision about which modulation scheme is right for your devices.

Bluetooth Security

Earlier Bluetooth devices were shunned in healthcare due to the importance of secure patient and medical data. Early pairing implmentetaions by OEMs tended to have simple 4 digit preset passcodes (0000, 1234) for user simplicity, which were therefore fundamentally easy to guess.But as Bluetooth security has been enhanced using asymmetric cryptography, major security concerns have been addressed (especially beginning with BT 4.2) and adoptions of Bluetooth in medical have increased.

Bluetooth 2.1 and Simple Secure Pairing introduced new 6 digit random passcodes with confirmmation. During pairing with SSP, security features (such as I/O capabilities and requirements for MITM attack protection) were exchanged via the pairing request and pairing response packets. For example, if one device had a display and the other had a keyboard input, the first device can show a 6 digit random key and the second device can confirm it, ensuring they are each paired to the correct device.

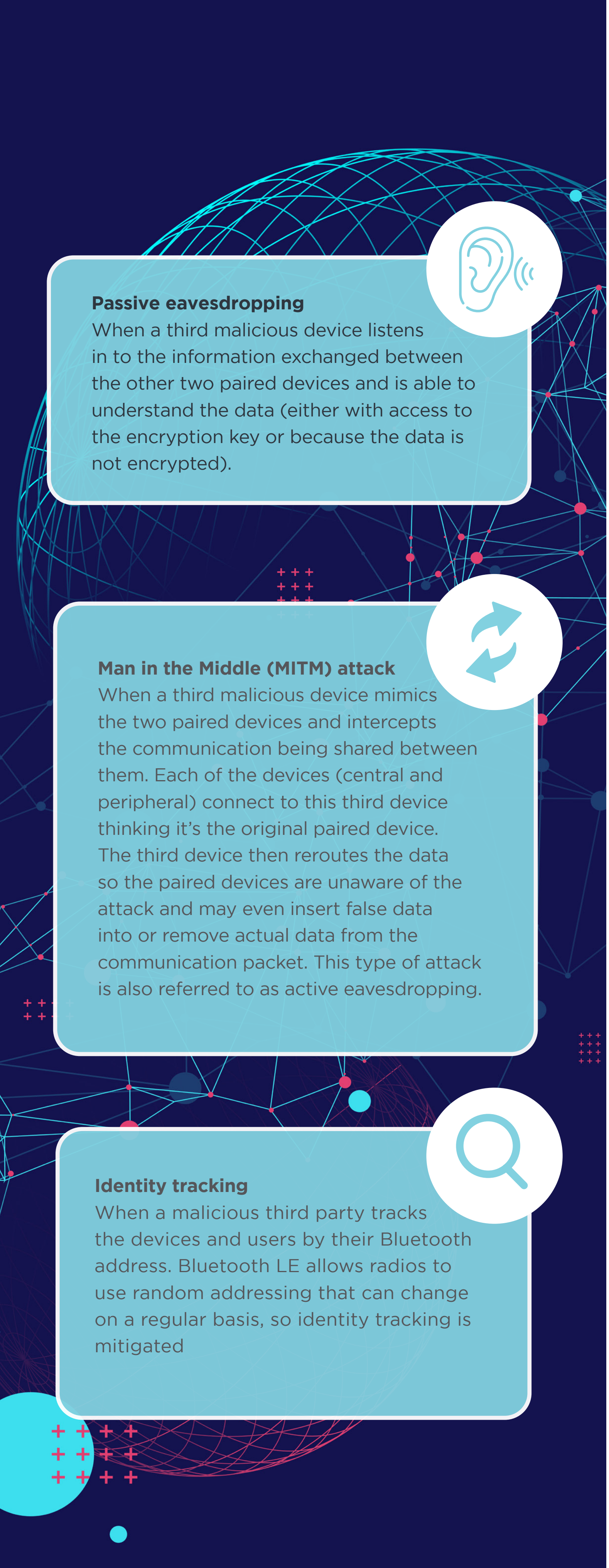
Pairing modes prior to Bluetooth 4.2 are now known as legacy pairing. Since Bluetooth 4.2, pairing now involves LE Secure Connections based on Eliptic Curve Diffie-Hellman cryptography. By incorporating ECDH into Simple Secure Pairing, Bluetooth now uses private and public key pairs that are extraordinarily difficult to break.

Once paired, Bluetooth LE modules within devices are extremely secure. The most vulnerable time for attacks is during the pairing process itself. These include Man in the Middle (MITM) attacks (or active eavesdropping), and identity tracking. (See *Figure A*) Once paired, the encryption information is stored, and these two devices no longer need to pair to connect. They are bonded, and no longer require sharing vulnerable secrets openly to reconnect.

Some of the other enhancements since Bluetooth 4.2 include: connection orientated isochronous communication and mode 3 security for LE audio; enhanced attribute protocol to require encrypted connection to transmit data; configurable minimum key size to ensure connections have a baseline level of security; 2M PHY for faster and easier OTA updates. Bluetooth continues to innovate in this area to meet requirements for existing and emerging use cases.

For a deep look at security features in Bluetooth LE and some comprehensive design recommendations, we recommend reading the Bluetooth SIG's Bluetooth LE Security Study Guide, and in particular the recommendations it makes to developers in chapter 2.

Pairing is a three-step process for both LE Legacy Pairing and LE Secure Connections. Phases one and three are identical for both but the second phase is where the main differences lay. The following defines each of these phases and explains how they are different.



Passive eavesdropping
When a third malicious device listens in to the information exchanged between the other two paired devices and is able to understand the data (either with access to the encryption key or because the data is not encrypted).

Man in the Middle (MITM) attack
When a third malicious device mimics the two paired devices and intercepts the communication being shared between them. Each of the devices (central and peripheral) connect to this third device thinking it's the original paired device. The third device then reroutes the data so the paired devices are unaware of the attack and may even insert false data into or remove actual data from the communication packet. This type of attack is also referred to as active eavesdropping.

Identity tracking
When a malicious third party tracks the devices and users by their Bluetooth address. Bluetooth LE allows radios to use random addressing that can change on a regular basis, so identity tracking is mitigated

Figure A

	LE Legacy Pairing (Bluetooth 4.0 and 4.1 devices)	LE Secure Connections (Bluetooth 4.2 and later devices)
Phase 1	**Pairing Feature Exchange** The two Bluetooth devices exchange the following information: • I/O capabilities • Authentication requirements • Maximum link key size • Bonding requirements	
Phase 2	**Key Generation Method Selection** **Short Term Key (STK) generation** The two devices exchange a TK in order to generate the STK using one of the following pairing models: • Just Works • Passkey • Out-of-Band (OOB)	**Long Term Key (LTK) generation** The two devices generate an LTK to encrypt the connection using one of the following pairing models: • Just Works • Passkey • Out-of-Band (OOB) • Numeric Comparison
Phase 3	Transport Specific Key exchange (optional)	

Note LE Secure Connections uses a FIPS-compliant algorithm called Elliptic Curve Diffie Hellman (ECDH) public key cryptography. This method provides enhanced security against threats such as passive eavesdropping and MITM attacks because no information is transmitted over an unencrypted link that can be used to establish or spoof the encryption keys.

The following are detailed descriptions of the pairing methods mentioned in the previous table:

Just Works

In this model, the six-digit TK is set to all zeros. This method is common especially for devices with no display (such as a speaker or headphones). Because the TK is set to 0, it's fairly easy for an attacker to eavesdrop on the connection. Also, this method provides no MITM protection because it offers no way to verify the devices involved in the connection.

Passkey

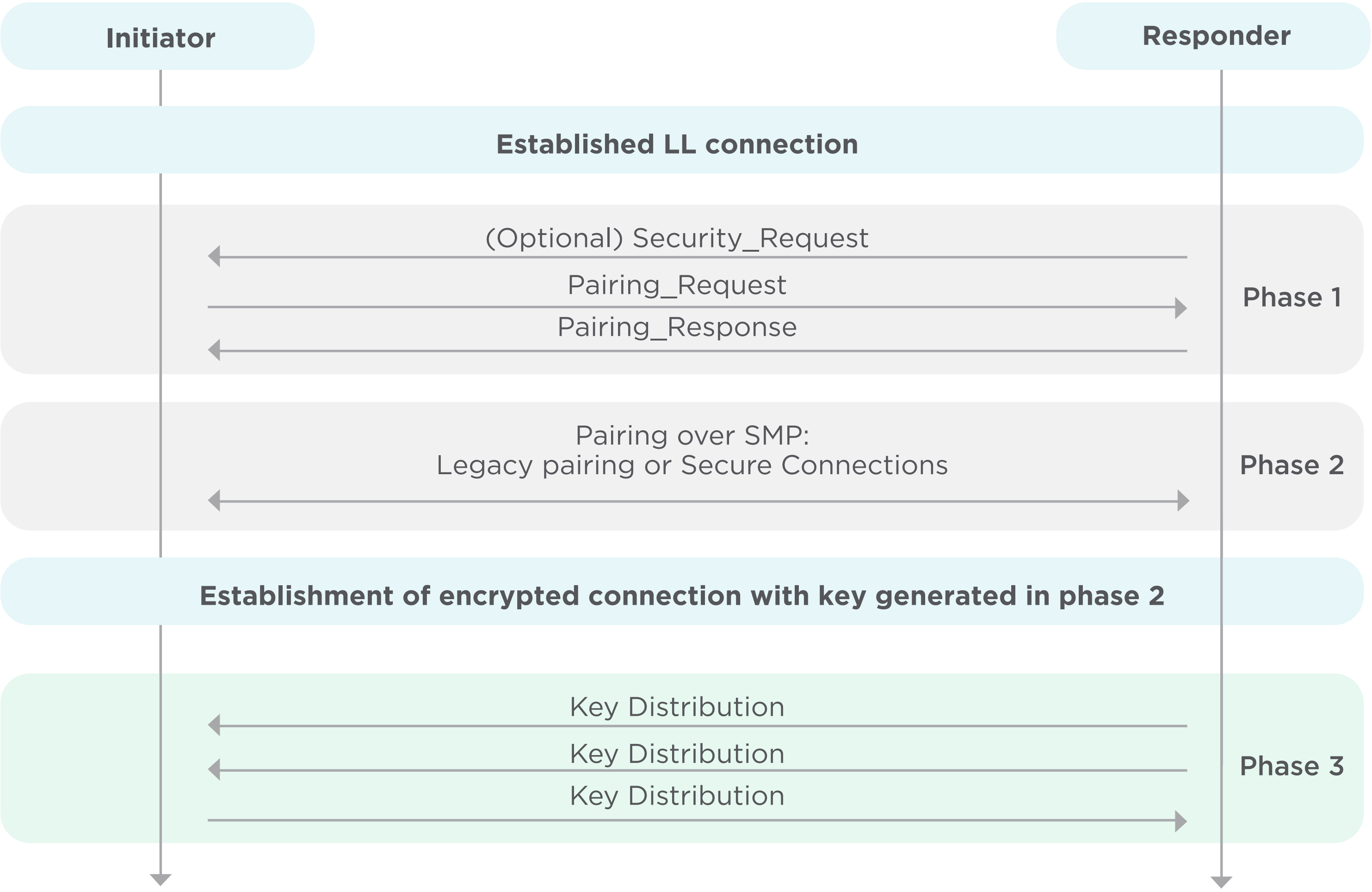
With this method, the user passes the TK between the devices as a six-digit number. This can be done in a variety of ways. For example, one of the devices may generate a random six-digit number that is then displayed on an LCD for the user to manually enter into the other device (Bluetooth pairing in automobiles, for example). Unless an attacker is listening during this pairing process, this method is relatively secure from passive eavesdropping. It is also considered secure from most MITM attacks as long as the attacker cannot acquire the passkey in another way (other than the Bluetooth LE connection).

OOB

With Out of Band pairing, a different wireless technology (such as NFC) is used to exchange the TK. One significant benefit of this type of exchange is the fact that a very large TK (up to 128 bits) can be used. With the larger TK, security is enhanced. The Bluetooth LE connection is protected from MITM attacks and passive eavesdropping as long as the OOB channel is also protected from these two attacks. Of these three legacy pairing methods (Just Works, Passkey, and OOB), OOB is the most secure.

Numeric Comparison

This method functions identical to Just Works except that it adds an extra step at the end. After the initial confirmation, both devices then independently generate and display a final six-digit number. The user must then manually confirm that both values match before the connection is approved. This extra step is what protects this method from MITM attacks.


Initiator
Responder
Established LL connection
(Optional) Security_Request
Pairing_Request
Pairing_Response
Phase 1
Pairing over SMP:
Legacy pairing or Secure Connections
Phase 2
Establishment of encrypted connection with key generated in phase 2
Key Distribution
Key Distribution
Key Distribution
Phase 3

Because of its advanced protection against threats such as passive eavesdropping, MITM (active eavesdropping), and identity tracking, the advanced LE Secure Connections (LESC) and LE Privacy v1.2 offered with Bluetooth 4.2 (and later) devices provide the enhanced security required for critical environments such as hospitals and other healthcare facilities.

Note: For more information on this pairing process, refer to the **Bluetooth SIG website** for a series of pairing 'tutorials': https://www.bluetooth.com/blog/bluetooth-pairing-part-1-pairing-feature-exchange/

Conclusion: Ready for Prime Time

Hospitals are full of people, equipment, obstacles. People spend a lot of time in hospitals with their cell phones, video games, and other potential sources of RF interference.

Hospitals and other healthcare facilities are critical environments where reliable and secure wireless connectivity is vital. Because these environments are already flooded with wireless signals and early Bluetooth pairing could be easily cracked, it was easy to say no to Bluetooth. It seemed counter-productive to add another RF technology to an already-congested 2.4 GHz frequency band and risk experiencing interference and disruption of wireless communication. Maintaining consistent and reliable connections between RF devices was far too critical in a healthcare setting to take the risk.

But, as Bluetooth technology has evolved to be more secure, more and more applications that leverage this technology have come into play, even in medical spaces. Personal monitoring devices such as fitness trackers and glucose monitors leverage Bluetooth and because of the increasing use of these devices, critical care environments have recognized the usefulness of this technology. In addition to these monitoring devices, it's also being effectively used as a wire replacement in hospital operating rooms and other medical locations where a high number of devices are in use. Simply put, with its low-power consumption ability, its prolific global use, and its scalability, Bluetooth is a great add-on to wireless infrastructures that support critical healthcare settings.

Laird Connectivity's Bluetooth Modules:

Implementing a Bluetooth solution for your product has never been this easy. Our Bluetooth module portfolio is designed to provide robust performance, easy global certification and simple implementation to accelerate your entire new product development cycle. We are the ideal Bluetooth/Bluetooth Low Energy (BLE) partner to help you simplify your next Bluetooth design. For more than 15 years, we have developed and produced Bluetooth modules, products and associated development kits.

Our portfolio spans the full Bluetooth connectivity range from the latest Bluetooth LE 5.4 modules to Classic Bluetooth BR / EDR. They support some of the latest software features such as Bluetooth LE audio — all available in software stack onboard or host-based modules.

For more information, visit lairdconnect.com/bluetooth

About Laird Connectivity:

Laird Connectivity simplifies wireless connectivity with market-leading RF modules, system-on-modules, internal antennas, IoT devices, and custom wireless solutions. Our products are trusted by companies around the world for their wireless performance and reliability. With best-in-class support and comprehensive product development services, we reduce your risk and improve your time-to-market. When you need unmatched wireless performance to connect your applications with security and confidence, Laird Connectivity Delivers – No Matter What.

Learn more at lairdconnect.com

Laird™
CONNECTIVITY