Bluetooth® Core 5.0 Feature Enhancements

Bluetooth® Core Specification v5.0 (Bluetooth® Core 5.0) includes several primary updates. This document summarises and explains each change.

Author: Martin Woolley

Version: 1.1.1

Revision Date: 13 January 2025

Bluetooth®

Revision History

Version	Date	Author	Changes
1.0.0	26 October 2017	Martin Woolley	Initial Version
1.1.0	9 September 2021	Martin Woolley	Format Updated
1.1.1	13 January 2025	Avi Negrin	Language Changes

Table of Contents

Table of Contents

At a Glance

LE 2M

The bottom layer of the Bluetooth® Low Energy (LE) stack is called the Physical Layer. Particular configurations of the physical layer are often referred to as a *PHY*. Bluetooth® Core Specification v5.0 (Bluetooth® Core 5.0) adds a new way in which the physical layer may be used with a PHY called *LE 2M*.

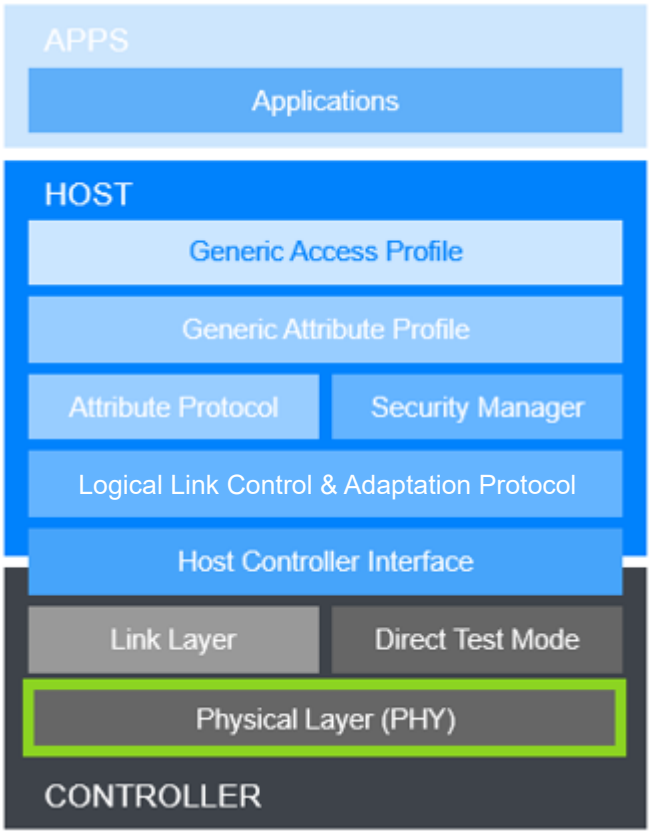

Figure 1 - The Bluetooth® LE stack

The LE 2M uses a symbol rate of 2 mega-symbols per second which given that Bluetooth technology uses a binary modulation scheme is equivalent to 2 megabits per second at the physical layer. LE 2M makes higher application data rates possible.

LE Coded

A further PHY, designed to support longer range communication has been defined in Bluetooth® Core 5.0. It is called the *LE Coded PHY* and uses a technique called *Forward Error Correction (FEC)* to enable longer range communication without any need to increase transmission power.

Extended Advertising

Bluetooth LE can perform connectionless communication using a procedure called *advertising*. *Legacy advertising* uses three channels from the 2.4 GHz radio band, specifically channels 37, 38 and 39. Bluetooth® Core 5.0 introduces *Extended Advertising* which uses all 40 Bluetooth LE channels, providing better spectral efficiency, scalability and reduced vulnerability to reliability issues which can be caused by packet collisions in busy radio environments.

Extended Advertising allows more data to be transmitted in a single packet and even larger application layer payloads to be fragmented and then transmitted in a series of *chained* packets. It also supports a new concept called Periodic Advertising which involves advertising packet transmission taking place at precisely timed intervals and provides a mechanism for observer devices to discover the advertising device's periodic advertising schedule and to then synchronize their scanning with it.

Finally, Extended Advertising allows multiple advertising configurations to be active at the same time through a capability known as *advertising sets*.

Slot Availability Mask

The Mobile Wireless Standard (MWS) radio bands used by 4G LTE in smartphones can interfere with Bluetooth radio communication when the two systems are collocated in the same device. A new Bluetooth BR/EDR feature called the Slot Availability Mask (SAM) helps mitigate this issue by allowing the time slots used by the two radios to be coordinated.

Improved Frequency Hopping

Bluetooth LE uses *adaptive frequency hopping* to spread communication across channels in the 2.4Ghz band. A new channel selection algorithm improves the way in which channels are selected and produces a greater degree of randomness and substantially more potential channel sequences. This improves both spectral efficiency and reliability in busy environments.

1. The LE 2M and LE Coded PHYs

1.1 Background

In a Bluetooth® LE stack, the lowest layer is called the physical layer. It is responsible for the representation of digital bits in analogue radio signals. A bit, when encoded in a radio signal is called a *symbol*. The physical layer encodes bits as symbols when transmitting data and decodes symbols to produce bits when receiving.

The basis for encoding digital information within a radio signal is called a *modulation scheme*. Bluetooth LE uses a modulation scheme called *Gaussian frequency shift keying* which in simple terms involves shifting a central carrier signal up by a small frequency deviation to represent a digital value of one or down by the same frequency deviation value to represent a digital zero. The frequency shifted signal is then transmitted for a certain period of time and this constitutes a single transmitted symbol. The number of symbols that can be transmitted per second is called the *symbol rate* and this is a property of the PHY.

All implementations of Bluetooth LE must include a PHY called LE 1M which operates at a symbol rate of 1 mega-symbol per second. At the application layer, a data rate of up to approximately 800 kilobits per second is possible when using LE 1M depending on other parameters and packet scheduling details established by the implementation.

1.2 About the LE 2M

Bluetooth® Core 5.0 introduced a new PHY called LE 2M.

1.2.1 Capabilities and Benefits

The LE 2M PHY operates at a symbol rate of 2 mega-symbols per second. This is double the symbol rate of the mandatory LE 1M PHY. The same data, transmitted in the same number of packets and using the LE 2M PHY rather than the LE 1M PHY will use half the radio airtime since the same number of symbols will be transmitted but at twice the rate. This represents a significant benefit in improved spectral efficiency.

At the application layer, a data rate of up to approximately 1.4 megabits per second is possible[1] when using LE 2M depending on other parameters and packet scheduling details established by the implementation.

1.2.2 Example Use Cases

Many use cases involving Bluetooth LE tend to involve small amounts of data, perhaps transmitted only occasionally. But there are use cases gaining prominence which demand a low-power wireless communications technology which supports higher data rates.

1 sources: Novel Bits and Nordic Semiconductor

Firmware upgrades are an important practice which as well as delivering new functionality, will often deliver bug fixes and security improvements which help keep users, businesses, and industrial systems safe and secure. Being able to initiate and complete a firmware upgrade over the air quickly helps with the task of keeping device firmware up to date. Consumers in particular are likely to be reluctant to apply firmware updates if their experience is that they take an excessive amount of time to complete. User experience and human behaviour are as much a consideration in security as are the technical aspects.

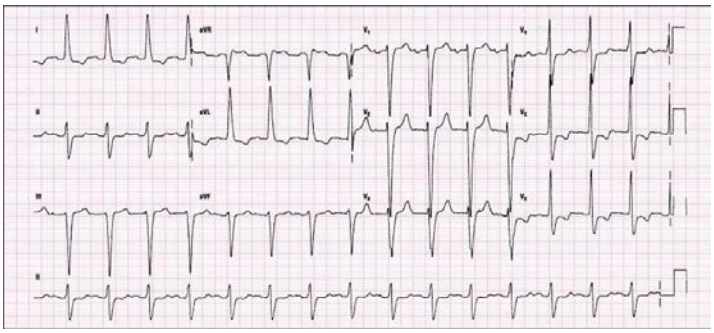

Figure 2 - We're collecting more data from sensors

Sports and fitness devices are getting increasingly sophisticated and now often measure multiple dimensions of the human body more frequently and with greater accuracy. A similar trend is taking place with some medical devices. The ECG has evolved from a device which had one lead to the 12 lead ECG of today. Such changes bring with them a substantial increase in the amount of data being collected.

There has also been a rise in devices that act as buffered sensors, especially in fields like Lifestyle Analysis where the user will wear a sensor, often for several days, before transferring all the accrued data to another device such as a smartphone or computer.

Quantity of data is not the only driver behind the introduction of LE 2M. Transmitting a given amount of data using a reduced amount of airtime also provides better spectral efficiency and requires less energy[2].

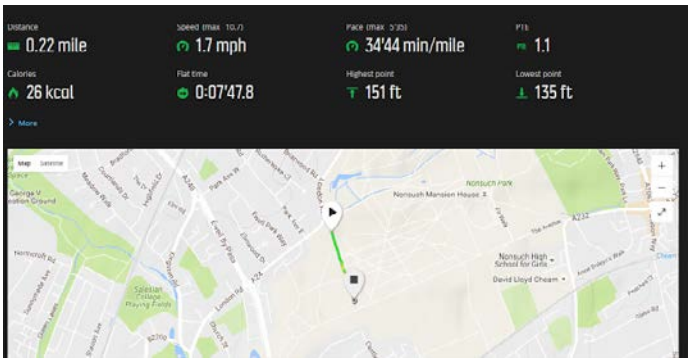

Figure 3 - Informal testing of Bluetooth® range using LE 1M PHY: 0.22 miles = 354 metres

1.3 About the LE Coded

The original LE 1M PHY has a much longer range than is popularly believed to be the case. Informal testing by the author, using a standard smartphone, a Bluetooth LE microcontroller unit (MCU) and the LE 1M PHY demonstrated the successful receipt of Bluetooth notifications by the smartphone at a distance of over 350 meters from the MCU in an environment which was sub-optimal with respect to radio communication, containing numerous people and trees. And there are commercial Bluetooth

2 See https://docs.silabs.com/bluetooth/2.13/general/system-and-performanceoptimizing-current-consumption-in-bluetooth-low-energy-devices

modules on the market whose data sheets state that a range of 500 meters is possible.

Given the fact that the LE 1M PHY has a remarkably healthy range for a low-power wireless communications technology, why increase it still further? There are many use cases where greater range can be advantageous. The smart home sector is one example and it, to a degree, led to the effort to introduce the long range LE Coded PHY.

1.3.1 Capabilities and Benefits

LE Coded allows range to be approximately quadrupled compared to LE 1M and this has been accomplished without increasing the transmission power required.

1.3.2 Understanding Range

To understand how range has been so dramatically increased without a need for a corresponding increase in transmission power requires the question of what we mean by range in wireless communications systems to be considered.

Bluetooth is a radio technology and radio is a form of electromagnetic radiation. In the context of telecommunications, the question of maximum range is better expressed as *what is the maximum range at which data can be correctly extracted from the received signal*, rather than *how far can this electromagnetic energy travel and still be detected*.

The distinction relates to how we use radio to encode and transmit data and how background noise can impact the decoding of that data by a radio receiver. Symbols created by modulating a carrier signal to represent binary zeroes or ones get transmitted. The receiver must receive the signal, turn it back into the same symbols and the same binary values higher up the stack. A transmitted zero, decoded by the receiver as a one or vice versa, represents an error.

The receiver has its work complicated by the fact that there is background radiation known as *noise* in the environment. The closer the level of the background noise to that of the received signal, the harder it becomes to decode the received signal and at some point, errors in the decoding process start to occur. Formally, we term the ratio of our transmitted signal power to that of the background noise the Signal-to-Noise Ratio (SNR). The strength of the received signal diminishes as the receiver moves further away from the transmitter and consequently with a more or less constant background noise level, the SNR reduces and with it, the probability of decoding errors increases.

We can quantify the level of errors experienced and we call this the Bit Error Rate (BER). BER is the probability that a transmitted bit will be incorrectly decoded by the receiver. We can then state the limit to the BER which we will tolerate at a given receiver input level. The Bluetooth® Core Specification defines a BER of 0.1% as the limit which is permitted.

So, increasing the range of Bluetooth technology without increasing the transmitter power was really a problem concerned with achieving the same maximum permitted BER at a greater distance from the transmitter and hence, at a lower SNR.

1.3.3 Dealing with Errors

In communications systems, errors are dealt with using either or both of two main strategies. The first is *error detection* and the second is *error correction*.

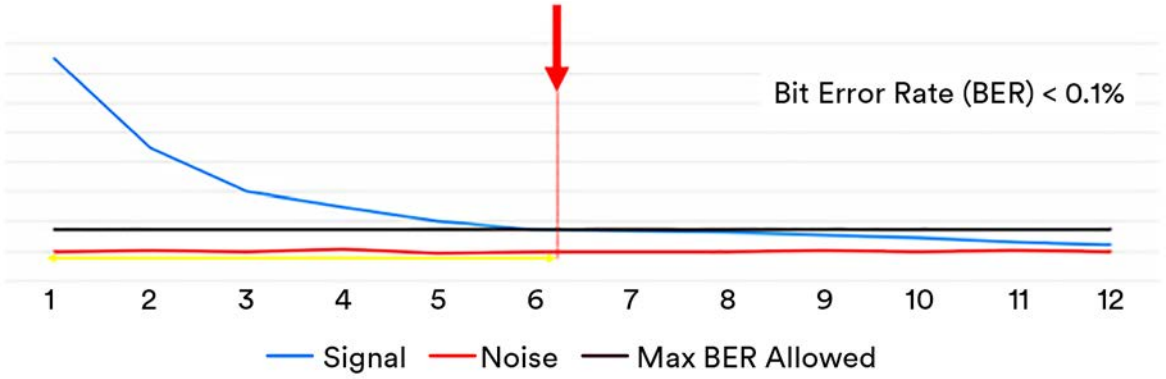

Figure 4 - Relationship between SNR and BER - not to scale

1.3.3.1. Error Detection

There are various schemes which allow a receiver to detect errors. Parity bits were first used many decades ago in both paper and magnetic tape systems. Wired, serial communications systems still rely on parity bits to allow the receiver to detect that one or more bits have been incorrectly decoded.

There are also several types of checksum which can be used. Bluetooth LE uses a type of checksum known as a Cyclic Redundancy Check (CRC). All packets have a 24-bit CRC value calculated for them by the transmitter and appended to the packet. The receiver recalculates the CRC and compares the calculated value with the value appended to the packet. If they are not the same, an error has occurred.

In the event that errors are detected, systems may respond in one or two ways. They could regard the error as fatal and abandon the communication, or they could request or hint that the transmitter should send the data again in the hope that a subsequent attempt will be successful. Bluetooth LE does not acknowledge packets when the CRC check has failed. Failure to receive an acknowledgment may cause the transmitter to send the data again.

1.3.3.2 Error Correction

It is possible to not only detect errors at the receiver but also up to certain limits to correct them so that the receiver does not need to have the data retransmitted.

The LE 1M and LE 2M PHYs do not perform error correction, only error detection.

Correcting errors using advanced error-correction techniques has the major advantage that data can be correctly decoded at a lower SNR and hence at a greater distance from the transmitter. This is the basis upon which the increased range which is possible using the LE Coded PHY has been achieved.

The LE Coded PHY uses Forward Error Correction (FEC) to correct errors. This works by adding redundant bits to transmitted packets, whose sole purpose is to support the application of the FEC algorithm and to allow the determination of the correct value that erroneous bits should have.

The process adds two stages to the bit stream process in Bluetooth LE. This is depicted below.

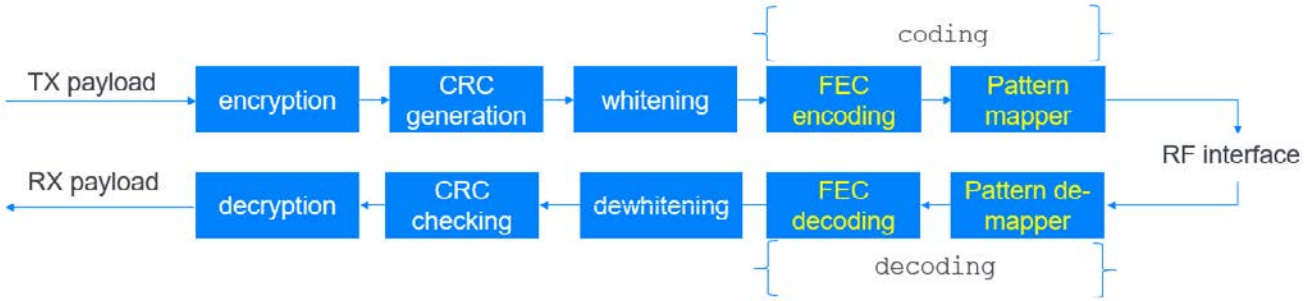

Figure 5 - FEC bit stream processing introduced in Bluetooth® Core 5.0

FEC encoding uses a convolutional encoder which generates 2 bits for every input bit using the following generator polynomials:

$$G_0(x) = 1 + x + x^2 + x^3$$

$$G_1(x) = 1 + x^2 + x^3$$

Figure 6 - FEC generator polynomials

The LE Coded PHY may be used with a choice of 2 different coding schemes, termed *S=2* and *S=8*. The *pattern mapper* process converts each bit from the convolutional FEC encoder into P symbols, where the value of P depends on the coding scheme in use. If S=2 then there is no change (i.e. P=1), but if S=8 then each bit from the FEC encoder produces 4 output bits (i.e. P=4) from the pattern mapper. Specifics are as shown below.

Input (from FEC Encoder)	Output with S=2	Output with S=8
0	0	0011
1	1	1100

Figure 7 - Pattern Mapper

The choice of coding scheme S=2 or S=8 with the LE Coded PHY has two consequences. With S=2, range will be approximately doubled whilst with S=8 it will be approximately quadrupled. But as can be seen, due to the requirement for redundant data to support the FEC algorithm at the receiver, it also impacts the number of symbols which must be transmitted. This reduces the overall data rate at the application layer.

1.4 Host Controller Interface (HCI)

The Host Controller Interface (HCI) has several commands relating to PHY use which may be invoked by the host. The *HCI_LE_Set_Default_PHY* command allows the host to indicate which PHY or PHYs it prefers to use for either transmission (TX), reception (RX) or both and for these preferences to be used as the default.

The host may also dynamically change the current PHY preferences for a specific connection using the *HCI_LE_Set_PHY* command. It is envisaged that applications may wish to switch into *high speed mode* for those use cases where the highest data rates are required or switch to *long range mode* when longer range is required and this will be achieved using an API which exploits the new HCI command.

The host may also determine the PHY being used by the controller for a particular connection for both TX and RX using the HCI_LE_Read_PHY command.

1.5 Comparing the Three LE PHYs

The following table presents key metrics relating to the three LE PHYs.

	LE 1M	**LE Coded S=2**	**LE Coded S=8**	**LE 2M**
Symbol Rate	1 Ms/s	1 Ms/s	1 Ms/s	2 Ms/s
Protocol Data Rate	1 Mbit/s	500 Kbit/s	125 Kbit/s	2 Mbit/s
Approximate Max. Application Data Rate	800 kbps	400 kbps	100 kbps	1400 kbps
Error Detection	CRC	CRC	CRC	CRC
Error Correction	NONE	FEC	FEC	NONE
Range Multiplier (approx.)	1	2	4	0.8
Requirement	Mandatory	Optional	Optional	Optional

Definitions

Term	Definition
Symbol Rate	The rate at which analog symbols are transmitted at the physical layer.
Protocol Data Rate	The transmission rate of bits relating to Bluetooth protocol data units (PDUs) including their application data payload but excluding FEC data which is included in packets when LE Coded is in use.
Approximate Max. Application Data Rate	An approximate maximum rate at which application data can be communicated between applications on connected devices. Application data is transported in the payload part of various PDUs with the remainder of the protocol data rate being consumed by Bluetooth protocol data.

2. Extended Advertising

2.1 Background

Legacy advertising packets are 37 octets long with a 6 octet header and a payload of at most 31 octets. Advertising packets are transmitted on up to three dedicated channels numbered 37, 38 and 39 out of a total of 40 Bluetooth® LE radio channels, each of which are 2MHz wide. The full set of channels are numbered from 0 to 39.

2.2 About Extended Advertising

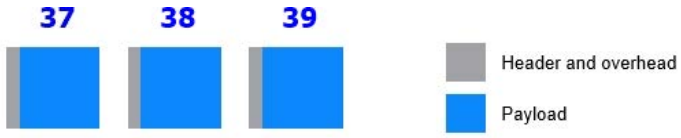

Figure 8 - Legacy advertising and channel use

Bluetooth® Core 5.0 introduced some major changes to how advertising may be performed. Eight new PDUs relating to advertising, scanning, and connecting have been added and new procedures defined. Collectively this new set of advertising capabilities are known as Extended Advertising.

Extended Advertising allows much larger amounts of data to be broadcast, advertising to be performed to a deterministic schedule and multiple distinct sets of advertising data governed by different configurations to be transmitted. There are significant improvements regarding contention and duty cycle too.

One of the many interesting things about Extended Advertising is the way in which radio channels are now used, with primary advertising channels 37, 38 and 39 carrying less data and general-purpose channels 0 - 36 doing most of the heavy lifting. With advertising data using all available channels, and only small headers using the primary channels, there will be less contention on those channels.

Furthermore, legacy advertising transmits the same payload up to three times on three different channels. Extended Advertising transmits payload data once only, with small headers referencing it from the primary channels. The total amount of data transmitted is thus less and so duty cycle has been reduced

The next sections explore each aspect of the Extended Advertising feature in turn.

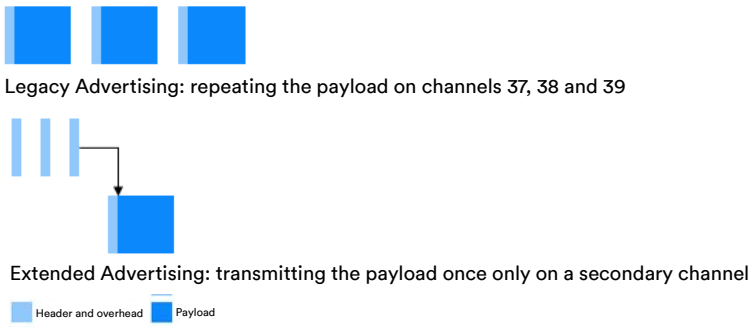

Figure 9 - Reduced contention and duty cycle

2.2.1 Capabilities and Benefits

2.2.1.1 Larger Packets and Advertising Channel Offload

Extended Advertising allows packets to be up to 255 octets long. This is accomplished in part through offloading the payload to one of the other channels in the 0-36 channel number range, previously only used for connection events (a connection event is a time slot during which data may be transmitted over a connection). In addition to allowing larger packets in connectionless communication, this has other benefits which we'll come to.

Figure 10 - Extended Advertising supports larger advertising packets and channel offload

When performing Extended Advertising only header data is transmitted on the *primary channels* numbered 37, 38 and 39. This includes a field called AuxPtr.

The AuxPtr field references an associated *auxiliary packet* containing the payload which will be transmitted on a *general-purpose* channel from the set of channels numbered 0 - 36. AuxPtr includes the general-purpose channel number that the auxiliary packet will be transmitted on so that receivers know where to find it.

2.2.1.2 Advertising Packet Chaining

For those use cases where an application would like to broadcast even more data (up to 1,650 bytes), it is now possible for the controller to fragment data and chain packets together with each packet containing a subset of that data.

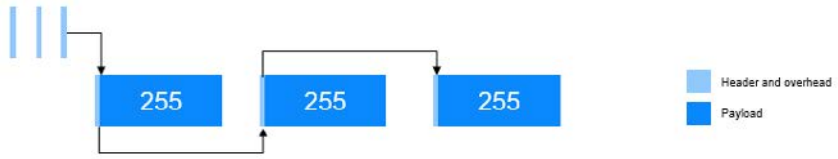

Figure 11 - Extended Advertising packet chaining

Each chained packet can be transmitted on a different channel, with the AuxPtr header field referencing the next in the chain.

2.2.1.3 Advertising Sets

Legacy advertising does not make formal provision for advertising payload and parameters to vary. Extended Advertising includes a standard mechanism for having multiple, distinct sets of advertising data.

Advertising sets have an ID which is used to indicate which set a given packet belongs to and each set has its own advertising parameters, such as its advertising interval and the PDU type to be used.

The task of scheduling and transmitting the different sets falls to the Link Layer in the Controller rather than it having to be driven by the Host, which would be far

less power efficient. The Host needs only to inform the Controller of the advertising sets and their respective parameters initially, after which the Link Layer takes over.

2.2.1.4. Periodic Advertising

Advertising usually includes a degree of randomness in the timing of advertising packet transmission. Random delays of between 0 and 10ms are deliberately inserted in the scheduling of advertising events to help avoid persistent packet collisions. Using legacy advertising this is the only way in which advertising can work.

Bluetooth® Core 5.0 introduces the ability to perform advertising to a deterministic schedule and provides a mechanism which allows observer devices to synchronize their scanning for packets with the schedule of the advertising device. This new advertising capability is called Periodic Advertising, it is part of the overall Extended Advertising feature, and it uses the general-purpose channels.

Periodic Advertising can benefit observer devices by offering a more power-efficient way to perform scanning and is also likely to pave the way for new uses of Bluetooth LE in connectionless scenarios, such as broadcast audio applications.

The Generic Access Profile (GAP) now defines a *synchronizable mode* and a *non-synchronizable mode*. When operating in synchronizable mode, a Periodic Advertising Synchronization Establishment procedure is defined.

Periodic Advertising performed in synchronizable mode, leverages a new header field called SyncInfo, which contains timing and timing offset information. Periodic advertisements use a new PDU type called AUX_SYNC_IND.

2.3 Additional Changes to Bluetooth LE Advertising

In addition to the introduction of the new Extended Advertising feature, Bluetooth® Core 5.0 reduced the minimum allowed *Advertising Interval* from 100ms to 20ms for non-connectable advertising. This enables *high duty cycle non-connectable advertising* and will be of benefit in allowing a rapid recognition of and response to advertising packets from devices like beacons.

2.4 Comparing Legacy Advertising and Extended Advertising

	Legacy Advertising	Extended Advertising	
Max. host advertising data size	31 bytes	1,650 bytes	Extended Advertising supports fragmentation which enables a 50x larger maximum host advertising data size to be supported.
Max. host advertising data per packet	31 bytes	254 bytes	Extended Advertising PDUs use the Common Extended Advertising Payload Format which supports an 8x larger advertising data field.
TX channels	37,38,39	0-39	Extended Advertising uses the 37 general-purpose channels as secondary advertising channels. The ADV_EXT_IND PDU type may only be transmitted on the primary advertising channels (37, 38, 39) however.

	Legacy Advertising	Extended Advertising	
PHY support	LE 1M	LE 1M LE 2M (excluding ADV_EXT_IND PDUs)	All Extended Advertising PDUs except for ADV_EXT_IND may be transmitted using any of the three LE PHYs except for the ADV_EXT_IND PDU which may be transmitted using LE 1M or LE Coded.
Max. active advertising configurations	1	16	Extended Advertising includes Advertising Sets which enable advertising devices to support up to 16 different advertising configurations at a time and to interleave advertising for each advertising set according to time intervals defined in the sets.
Communication types	Asynchronous	Asynchronous Synchronous	Extended Advertising includes Periodic Advertising, enabling time-synchronized communication of advertising data between transmitters and receivers.

3. Slot Availability Mask

3.1 Background

Bluetooth® technology uses the 2.4 GHz ISM band and this is immediately adjacent to the Mobile Wireless Standard (MWS) bands which are used by Long Term Evolution (LTE) radios. When a device includes both Bluetooth technology and an LTE radio as is commonly the case with smartphones, there is potential for interference, with transmissions from one radio desensitizing the receiver on the other. The set of issues relating to the inclusion of multiple radios in the same device is known as *collocation*.

3.2 About Slot Availability Mask

3.2.1 Capabilities and Benefits

Bluetooth® Core 5.0 defines the Slot Availability Mask (SAM) feature which allows devices to take into account the transmit/receive schedule of MWS radios in their scheduling of Bluetooth BR/EDR transmission and reception. By sharing time slot data, devices can coordinate the two radios and avoid interference that might otherwise occur.

3.2.2 Technical Highlights

The basic assumption behind SAM is that Bluetooth transmissions should not take place during an MWS time slot used for MWS downlink operations and Bluetooth reception should not occur during a time slot used for MWS uplink operation.

The SAM feature defines procedures and PDUs which allow two Bluetooth BR/EDR devices to share data which indicates which time slots are available for transmission or reception or neither. This data takes the form of a map called the *SAM slot map.* An example of a SAM slot map, reproduced from the Bluetooth® Core Specification appears in Figure 12.

Bluetooth Slot	C	P	C	P	C	P	C		C	P	C	P
Can Transmit	✗	✗	✓	✓	✓	✗	✗		✓	✓	✓	✗
Can Receive	✓	✗	✗	✗	✗	✓	✓		✓	✓	✓	✓
Type Code	2	0	1	1	1	2	2		3	3	3	2

Figure 12 - Example slot availability map

Type codes in Figure 12 are defined as:

Slot Type Code	Meaning
0	This slot is not available for either transmission or reception
1	This slot is available for transmission but not reception
2	This slot is available for reception but not transmission
3	This slot is available for both transmission and reception

The Link Manager Protocol (LMP) defines PDUs that support communication of SAM data between devices.

4. Improved Frequency Hopping

4.1 Background

Bluetooth® LE uses Adaptive Frequency Hopping (AFH) when in a connection. This involves using an algorithm to determine the radio channel to transmit and receive on. The selected channel is changed frequently such that data is transmitted over a wide selection of channels. This helps make Bluetooth communication work well in busy radio environments.

The original selection algorithm used in frequency hopping produced only 12 distinct sequences of channels and all packets in a given connection event would use the same channel, which is not optimal for some applications, such as audio. This algorithm is now known as Channel Selection Algorithm #1.

4.2 About Improved Frequency Hopping

4.2.1 Capabilities and Benefits

A new channel selection algorithm called Channel Selection Algorithm #2 (CSA 2) has been defined in Bluetooth® Core 5.0. Hopping sequences are now pseudo-random and the number of distinct sequences which can be generated is very large.

Channel Selection Algorithm #2 can be used for channel selection in both connection-oriented communication and in Periodic Advertising (see section 2.2.14). The diverse, randomly selected channel sequences which it generates improve communication reliability through reducing the probability of packet collisions.

4.2.2 Technical Highlights

Devices can indicate whether or not they support Channel Selection Algorithm #2 by setting the *ChSel* field in the header of certain advertising PDU types to 1 or by setting ChSel to 1 in CONNECT_IND PDUs when requesting a connection. When requesting a connection, if both the advertising Peripheral device and the connection-initiating Central device have indicated that they support Channel Selection Algorithm #2 then this algorithm will be used. If either or both devices do not support the newer algorithm, then Channel Selection Algorithm #1 is used instead.

Channel Selection Algorithm #2 makes use of a shared event counter which enables all devices involved in the communication to determine the index of the next channel in the pseudo-random sequence.

References

Item	Location
Bluetooth® Core Specification v5.3	https://www.bluetooth.com/specifications/specs/