

Understanding Bluetooth

Cole Overstreet

Radford University

Radford, VA

Roverstreet1@radford.edu

Table of Contents

I. Introduction	1
II. A Brief History	1
A. History of the name “Bluetooth”	1
B. A Brief History of the Creation of Bluetooth.....	1
III. Background Information.....	2
A. Bluetooth Classic	2
B. Bluetooth Low Energy (BLE)	2
IV. How Bluetooth Works.....	2
A. Bluetooth Packets.....	3
B. Bluetooth Connection Sequence	3
V. Final Thoughts.....	4
VI. References.....	4

Abstract—Bluetooth is all around us in everyday life but where did Bluetooth come from and how does it work? The Bluetooth technology has been developed for many years, starting with being developed as a technology used for headsets for voice calls and not being able to handle music playback. This has since changed, and Bluetooth is used for Bluetooth headphones with the specific purpose of delivering high quality audio to the wearer. Bluetooth is used for much more than just music in today’s world. Bluetooth can be found in anything from headsets for phone calls (like its original purpose) to Internet of things (IoT) devices with Bluetooth Low Energy (BLE).

Keywords—*Bluetooth, Bluetooth Low Energy, Internet of Things*

I. INTRODUCTION

Bluetooth is a commonly used form of communication between computers and other network

enabled devices. Bluetooth technology has been around for many years but how does it actually work? The technology can be found in everything from smart phones, computers, all the way to coffee makers [1].

II. A BRIEF HISTORY

A. History of the name “Bluetooth”

The creator of Bluetooth, “originally called their technology 'Bluetooth' after Harald Bluetooth, who was king of Denmark between 940 and 981” [2]. It was during his ruling that Denmark and Norway were Christianized and united. The creator, “used the analogy that he “allowed greater communication between people” when naming their wireless communication protocol” [2].

B. A Brief History of the Creation of Bluetooth

“The Bluetooth standard was originally conceived by Dr. Jaap Haartsen at Ericsson back in 1994” [3]. Bluetooth is a personal area network (PAN) protocol for short-range and low-power data transmission.

Bluetooth was originally developed to replace the RS-232 cable, a serial cable used for data transmission. The group known as IEEE (Institute of Electrical and Electronics Engineers) first standardized the Bluetooth protocol as IEEE 802.15.1. Since then “the Bluetooth SIG (Special Interest Group) oversees development of the specification, manages the qualification program, and protects the trademarks” [4]. The Bluetooth SIG was formed in 1998 [4]. Bluetooth has been around since development was initiated in 1989 by Nils Rydbeck at Ericsson Mobile in Lund, Sweden. The original goal was to develop wireless headsets for communication [5]. Bluetooth has had five major revisions with some revisions having sub revisions later on in their respected lifetime. The major revisions are numbered one through five, five being the most current major revision and one being the original. That being said the most current version of Bluetooth as of now is Bluetooth 5.1. This version was revealed to the world on January 21 2019 [6].

III. BACKGROUND INFORMATION

There are what is known as Bluetooth classic, Bluetooth HS (high speed), and the newer Bluetooth Low Power. Each of these are used for different things. Bluetooth 3.0 introduced Bluetooth HS (high speed) and this was for high speed data transfer using Wi-Fi. Bluetooth HS, “provides theoretical data transfer speeds of up to 24 Mbit/s, though not over the Bluetooth link itself. Instead, the Bluetooth link is used for negotiation and establishment, and the high data rate traffic is carried over a collocated 802.11 link” [7]. Bluetooth 4.0 introduced Bluetooth Low Energy (BLE) also known as Bluetooth Smart. Bluetooth 4.0 includes Bluetooth Classic, HS, and BLE. It is important to note that HS is a part of classic. Bluetooth Low Energy (BLE) is used frequently for IoT (Internet of things) devices because of the long battery life. Since Bluetooth Low Energy (BLE) is not compatible with classic some, “chip designs allow for two types of implementation, dual-mode, single-mode and enhanced past versions” [8]. The frequencies that Bluetooth classic and Low Energy both use are 2.4000GHz to 2.4835GHz. There is a 2MHz guard band at the bottom end of the allocated spectrum and a 3.5MHz guard band at the top end of the allocated spectrum. Bluetooth uses 79 channels including both guard bands that were mentioned earlier. These channels are spaced 1MHz apart [9]. See figure 1 for example of different protocols operating in the 2.4000GHz to 2.4835GHz spectrum.

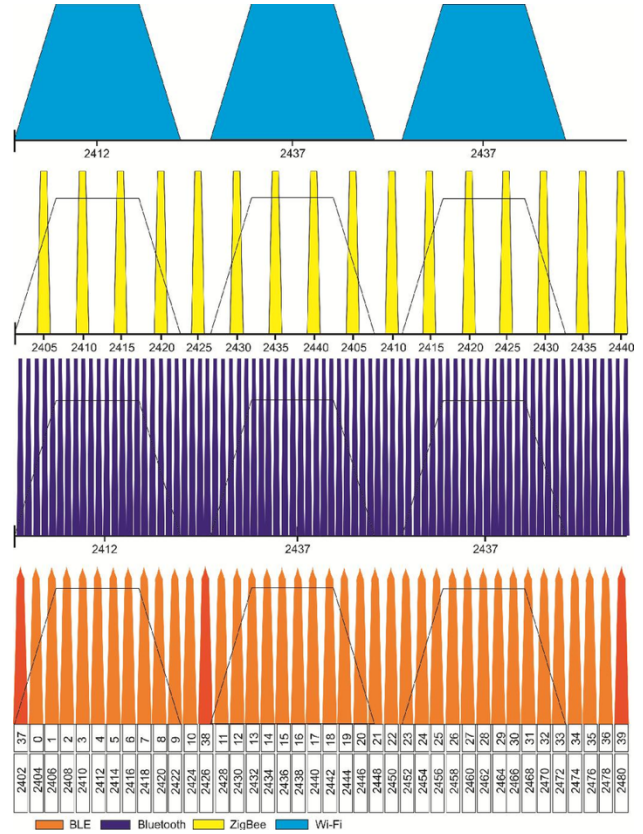


Figure 1: 2.405GHz to 2.440 example

Source: Adapted from [12]

A. Bluetooth Classic

Bluetooth Classic offers higher data rates and longer range at the cost of higher power. An example of what this is typically used for is audio streaming for wireless headphones. Bluetooth classic is also broken down to four power level classes, class 4 that uses 0.5mW, class 3 that uses 1mW, class 2 that uses 2.5mW, and class 1 that uses 100mW. Bluetooth Classic has data transfer speeds of up to 3Mb/s [9].

B. Bluetooth Low Energy (BLE)

Bluetooth Low Energy (BLE) uses lower data rates and lower range to allow it to also run at lower power. Bluetooth Low Energy (BLE) is used in a lot of Internet of Things (IoT) devices. Bluetooth Low Energy (BLE) has a maximum power level of 10mW. Bluetooth Low Energy (BLE) has data transfer speeds up to 2Mb/s [9].

IV. HOW BLUETOOTH WORKS

Bluetooth networks, also called piconets, use a master/slave model to control when and where devices can send data. For every master device there can be seven slave devices. See figure 2.

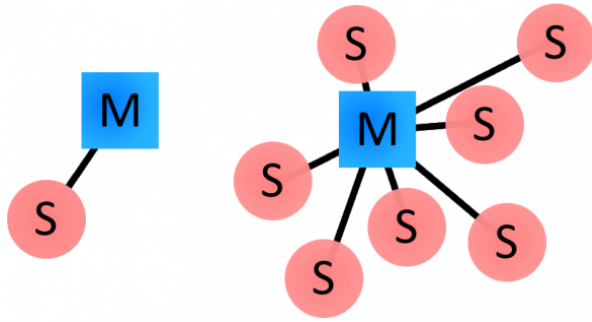


Figure 2: Examples of Bluetooth master/slave piconet topologies.
Source: Adapted from [9]

“The master coordinates communication throughout the piconet. It can send data to any of its slaves and request data from them as well. Slaves are only allowed to transmit to and receive from their master. They can’t talk to other slaves in the piconet” [9]. All Bluetooth devices have a 48-bit address, this is normally abbreviated BD_ADDR and is typically shown in the form of a 12-digit hexadecimal value. The BD_ADDR “contains two parts: company ID which is unique across the world, and device ID which is unique within the products of the company” [11]. To create a Bluetooth connection it takes a multistep process that uses three states, Inquiry, Paging or Connecting, and Connection. Inquiry is defined as, “If two Bluetooth devices know absolutely nothing about each other, one must run an inquiry to try to discover the other. One device sends out the inquiry request, and any device listening for such a request will respond with its address, and possibly its name and other information” [9].

Paging or Connecting is defined as, “the process of forming a connection between two Bluetooth devices. Before this connection can be initiated, each device needs to know the address of the other (found in the inquiry process)” [9]. Connection is defined as, “after a device has completed the paging process, it enters the connection state. While connected, a device can either be actively participating or it can be put into a low power sleep mode” [9]. After a master and slave are paired there are different modes, Active mode is the regular connected mode. This is where the device is transmitting or receiving data. Sniff mode is a power-saving mode. It will sleep and only listen for transmissions at a set interval. Hold mode is a temporary, power-saving mode where a device sleeps for a set period of time then goes back to active mode. The master can tell a slave to hold and for how long. Park mode is the deepest sleep mode. A master can tell a slave to “park” and after that the slave will become inactive till the master wakes the slave back up [9]. Bonding is when the devices pair automatically after they are set up, examples of this are smart watches. Pairing is when you must confirm the connecting of the two devices, examples of this are when the user is asked to match a PIN code.

Bluetooth uses Frequency-hopping spread spectrum (FHSS) to lower the interference between other devices in the area. Bluetooth will make 1600 hops per second in a pseudorandom order determined by the masters MAC address (BD_ADDR). Timing is

also determined by the master’s clock. Adaptive frequency-hopping spread spectrum (AFH) is used in Bluetooth to avoid crowded frequencies when it is hopping [10]. This means that a Bluetooth device will try to avoid frequencies with in the allocated 2.4000GHz to 2.4835GHz because that more than likely already has a lot of use and could cause interference.

A. Bluetooth Packets

If there is already a Bluetooth connection the packets that the devices will use to talk to each other will be made up as follows: 72 bits for the access code, 54 bits for the header and any amount from 0 – 2745 bits for the payload. See figure 3.



Figure 3: Bluetooth General Packet

Source: Adapted from [11]

This general packet must be broken down further to understand what is going on. The access code is made up of 4 bits of pre-amble, 64 bits of synchronization, and 4 bits of a trailer. The synchronization bits are derived from the masters BD_ADDR that was mentioned earlier in the paper [11]. See figure 4.

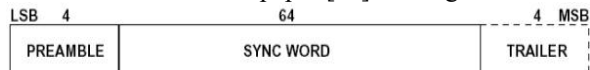


Figure 4: Access Code Bits Broken Down

Source: Adapted from [11]

The next section in the general packet to break down in the header that is 54 bits. This part of the packet starts with the active member address or “AM_ADDR” and this is 3 bits because you can only have 7 slaves. This is used to keep track of what goes to what slave. When 7 is converted to binary it equals 111 which takes up 3 bits. Next is the type of packet that is being sent and this takes up 4 bits. It is also worth noting that there are 12 different types of data types and 4 control types. Then there is the flow bit, the ARQN bit, the SEQN bit for ordering the packets, and lastly 8 bits for the HEC or header error check [11]. See figure 5.

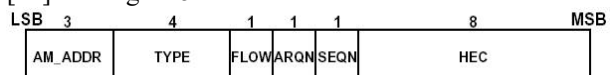


Figure 5: Header Broken Down

Source: Adapted from [11]

The last section of the general packet is the data bits and this can be 0 to 2745 bits long. This is where the data that you want to send over Bluetooth is stored.

B. Bluetooth Connection Sequence

If the two Bluetooth devices have never been talking before you must make the slave discoverable. This could be pushing a button on the actual device or in the settings on a smart phone, computer, or similar device. After the slave device is in this mode if it gets an inquiry from a master it will answer. When in discoverable mode the device is listening in on 32 channels that are spaced 1 MHz apart. These 32 of the 79 mentioned earlier in the paper are channels that have

been marked as inquiry channels. When the master gets an inquiry back from the slave it will cycle through the 32 inquiry channels and send out ID packets. The ID packets include the general inquiry access code. When the slave you were trying to pair to a master gets this response it will stop what it is doing and then send an inquiry response that has its FHS (frequency hopping sequence). The FHS includes the slaves ID and clock. If the master picks this up it will enter page mode and the slave will go into page scan mode. The master pages the slave and if the slave answers with a device access code then the master responds with its FHS that contains and uses the master ID and master clock. After this the slave replies with its local device access code and switches to the master channel. After this the devices are connected. Now this is where the master can tell the slave what mode to be in [9]. These modes are the modes that were referenced earlier in the paper.

V. FINAL THOUGHTS

Bluetooth has been around for many years and will be here for many years to come. Bluetooth is all around us and is used in almost all modern smartphones and computers. With the emergence of Bluetooth Low Energy (BLE) it now powers many Internet of Things (IoT) devices. With how versatile and adaptable Bluetooth is, whether it be Bluetooth Classic or Bluetooth Low Energy (BLE) one thing is for sure it is here to stay and will only grow in importance to modern day life.

VI. REFERENCES

- [1] [1] W. Greenwald, "The Best Smart Coffee Makers," PCMag, 22-Jun-2018. [Online]. Available: <https://www.pcmag.com/article/361898/the-best-smart-coffee-makers>. [Accessed: 06-Dec-2019].
- [2] "Where does the computer term 'Bluetooth' come from? Did they name the system after the Viking kings?," The Guardian. [Online]. Available: <https://www.theguardian.com/notesandqueries/query/0,5753,-18959,00.html>. [Accessed: 06-Dec-2019].
- [3] R. Triggs, "A quick history of Bluetooth," Android Authority, 23-Mar-2018. [Online]. Available: <https://www.androidauthority.com/history-bluetooth-explained-846345/>. [Accessed: 06-Dec-2019].
- [4] Bluetooth SIG, "About Us," Bluetooth Technology Website. [Online]. Available: <https://www.bluetooth.com/about-us/>. [Accessed: 06-Dec-2019].
- [5] Information Age, "Information Age," The bluetooth blues | Information Age, 24-May-2001. [Online]. Available: https://web.archive.org/web/20071222231740/http://www.information-age.com/article/2001/may/the_bluetooth_blues. [Accessed: 06-Dec-2019].
- [6] M. Woolley, "Bluetooth Core Specification v5.1 Feature Overview," Bluetooth Technology Website, 27-Sep-2019. [Online]. Available: <https://www.bluetooth.com/bluetooth-resources/bluetooth-core-specification-v5-1-feature-overview/>. [Accessed: 06-Dec-2019].
- [7] Bluetooth SIG, "Specification Documents" Bluetooth SIG. [Online]. Available: http://www.bluetooth.org/docman/handlers/DownloadDoc.ashx?doc_id=40560&ei=25GiT8L3CuTa0QGnmqDVDA&usg=AFQjCNGXY5pm4Tkju1KGs4dYRJLtd03FEg. [Accessed: 06-Dec-2019].
- [8] Bluetooth SIG, "SIG Press Releases," Bluetooth.com | SIG INTRODUCES BLUETOOTH LOW ENERGY WIRELESS TECHNOLOGY, THE NEXT GENERATION OF BLUETOOTH WIRELESS TECHNOLOGY, 17-Dec-2009. [Online]. Available: https://web.archive.org/web/20091221175650/http://www.bluetooth.com/Bluetooth/Press/SIG/SIG_INTRODUCES_BLUETOOTH_LOW_ENERGY_WIRELESS_TECHNOLOGY_THE_NEXT_GENERATION_OF_BLUETOOTH_WIRELESS_TECHNOLOGY. [Accessed: 06-Dec-2019].
- [9] SparkFun, "Bluetooth Basics," Bluetooth Basics, 17-Sep-2017. [Online]. Available: <https://learn.sparkfun.com/tutorials/bluetooth-basics/>. [Accessed: 06-Dec-2019].
- [10] Electronics Notes, "Bluetooth radio interface, modulation, & channels," Electronics Notes. [Online]. Available: <https://www.electronics-notes.com/articles/connectivity/bluetooth/radio-interface-modulation-channels.php>. [Accessed: 06-Dec-2019].
- [11] S. Liu, "1. Bluetooth Overview," Bluetooth Technology. [Online]. Available: http://progtutorials.tripod.com/Bluetooth_Technology.htm. [Accessed: 06-Dec-2019].
- [12] "Find and share research," ResearchGate. [Online]. Available: https://www.researchgate.net/figure/Wi-Fi-ZigBee-Bluetooth-abd-BLE-spectrum_fig1_265602069. [Accessed: 06-Dec-2019].