Expertise
and insight
for the future

Valentine Idi

Bluetooth Technology and Applications

Metropolia University of Applied Sciences

Bachelor of Engineering

Electronics Engineering

Bachelor's Thesis

27 November 2019

Author Title Number of Pages Date	Valentine Idi Bluetooth Technology and Application 37 pages 27 November 2019
Degree	Bachelor of Engineering
Degree Programme	Electronics Engineering
Professional Major	Electronics
Instructors	Janne Mäntykoski, Senior Lecturer

This thesis concerns about Bluetooth technology; the history, the name, logo and how it all started. This thesis also contains the working principle of Bluetooth and its specifications. There are also different versions of Bluetooth which will be explained in detail in chapter three of this thesis. There are different applications of Bluetooth and just like other wireless technologies, the security issues all of which will be covered in chapter four and five respectively.

The main objective of this project was to create a heart rate sensor which can be connected to a smart phone. This was carried out using nRF51 mbed, a compiler (mbed.org was used in this case), nRF connect software and a Samsung s9+ was used as the smart phone. The code to enable the heart rate sensor of the mbed and to make the mbed discoverable via Bluetooth was to be written, complied and with the drag and drop functionality of the mbed, dragged in to the mbed disc which was connected to a laptop. The nRF connect software helped to display the simulated heart rate reading.

This project will help point out the benefits of Bluetooth for educational purposes as well as personal and Business purposes

Keywords	Bluetooth, Technology, nRF51, Heart rate sensor

Contents

List of Abbreviations

AES-CMAC	Advanced encryption standard-Cipher based message authentication code
ANT	Adaptive network topology
ARM	Advanced RISC machine
CMSIS-DAP	Cortex Microcontroller software interface standard-debug access port
CTO	Chief technology officer
ECDHE	Elliptic curve Diffe-Hellman
EDR	Enhanced Data Rate
eSCO	Extended synchronous connections
Etc	etcetera
GCC	GNU compiler collection
GHz	Gigahertz
HCI	Host controller interface
HS	High speed
IAR	Ingenjörsfirman Anders Rundgren(Anders Rundgren Engineering Company)
IDE	integrated development environment
IEEE	institute of electrical and electronics engineers
I/O	input/output
Kbps	Kilobits per second
L2CAP	Logical link control and adaptation protocol
LED	Light emitting diode
Mb/s	Megabit per second
Mbit/s	Megabit per second
Ps4	Playstation 4
RF	Radio frequency
SIG	Service integration gateway

SoC	System on Chip
USB	Universal serial Bus
Tv	Television
WiFi	Wireless Fidelity

1 Introduction

Bluetooth technology is arguably one of the most popular technologies in the world. Bluetooth was discovered back in 1995 when Haartsen managed to develop the technology with his partner Sven Mattison. Bluetooth has gotten huge improvements down the years and the popular technology became even more popular and more useful. There are numerous things that can be done with this technology such as home security, transfer of information or files, communicating two devices etc.

This thesis will cover the history of Bluetooth; how the name and logo came to be and who invented the technology in the first place. Although we use Bluetooth everyday of our lives, most people do not know how it works and this thesis will cover that as well. Although the current version of Bluetooth which was released in January 2019 is version 5.0, there has been other versions of Bluetooth such as version 1.0, 1.1b, 2.0 etc and these versions had their issues which were fixed in the next version. This thesis concerns everything about the versions, the issues and how they were fixed in the next version. Along the years, a lot of people are still confused on how good or bad Bluetooth security is; if it can be accessed easily or if it has any security issues at all. There is no wireless system without any security issues and just like WiFi, infrared and other wireless systems, Bluetooth is no exception to security problems. There has been a lot of methods used such as Bluebugging, bluesnarfing etc. All these security issues will be explained in detail in chapter five of this thesis.

The purpose of this thesis was to create a heart rate sensor with an nRF51-DK mbed development kit and with the help of a smartphone and nRF connect app, get the reading from the sensor and display on the smartphone. This will be discussed in details in chapter 4 of this thesis

2 Bluetooth

2.1 History

Bluetooth is a technology that is persistent in our daily lives. It exists in wide range of our devices: in speakers, wireless headphones, our mobile phones etc. Bluetooth is one of those technologies that the world cannot do without because it is so handy and makes every connection easy and convenient. It is used in speaker connection to tv, Bluetooth wifi tethering, ps4 controllers, occasional file transfer from mobile device to laptop. Although this technology is very useful to most if not everybody, it is a surprise that most people do not know how it came about.

2.1.1 Bluetooth Technology

In 1993, Jaap Haartsen a wireless communications engineer who worked at Ericsson was given the task to develop a short-range connection for mobile phones because back then, wires/cables were hindering communication systems. [2]

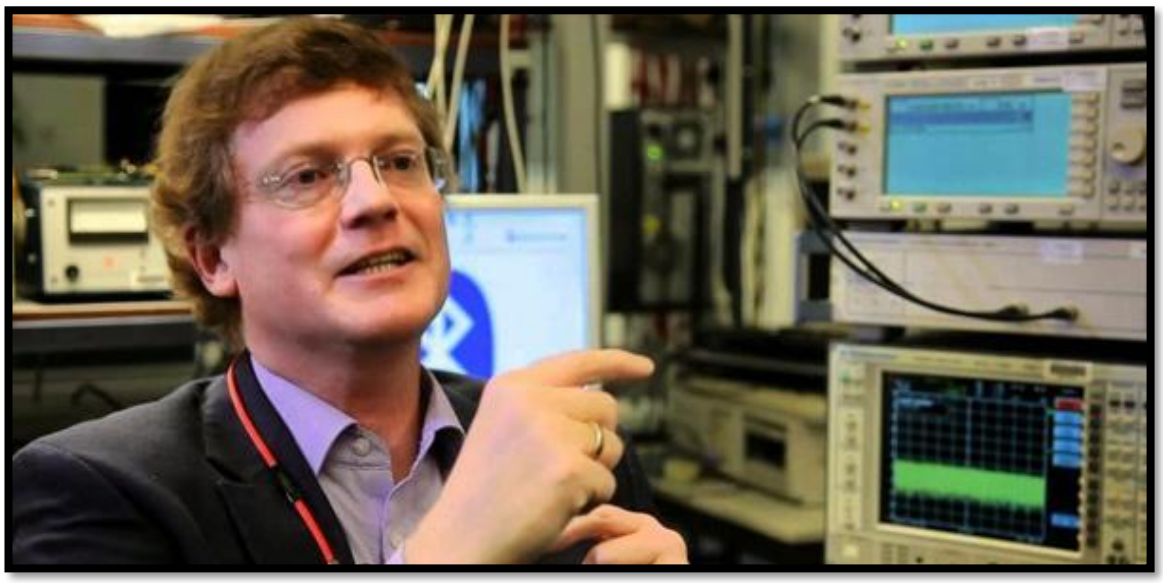

Figure 1. Jaap Haartsen [1]

In 1995 Haartsen (who can be seen in figure 1) was able to develop a technology called multi-communicator links with the help of his engineer partner, Sven Mattison. Although

it was those two that are always being credited for creating Bluetooth, it was Ericsson's CTO that came up with the idea and initiated the development four years before Haartsen was appointed for the task.[2] There were also some other people that made the creation of Bluetooth possible and each of those people contributed to the completion of the project.[2]

2.1.2 Bluetooth Name

To be a successful company, you need to have a good brand name. Just like Apple, Samsung, Nike, etc Bluetooth was a well thought brand name. Bluetooth is arguably a name that does not sound technological and that makes it unique from other brand names.

The name Bluetooth originated from the 10th century from the Danish king, Herald who can be seen from figure 2 below. It is still a debate why the king had the nickname. Some people say that he liked to eat blueberries while some others say it is because he had a 'dead/blue' tooth.

Now, the confusion is, why did a technology company decide to choose their brand name from a king who existed back in the 10th century.

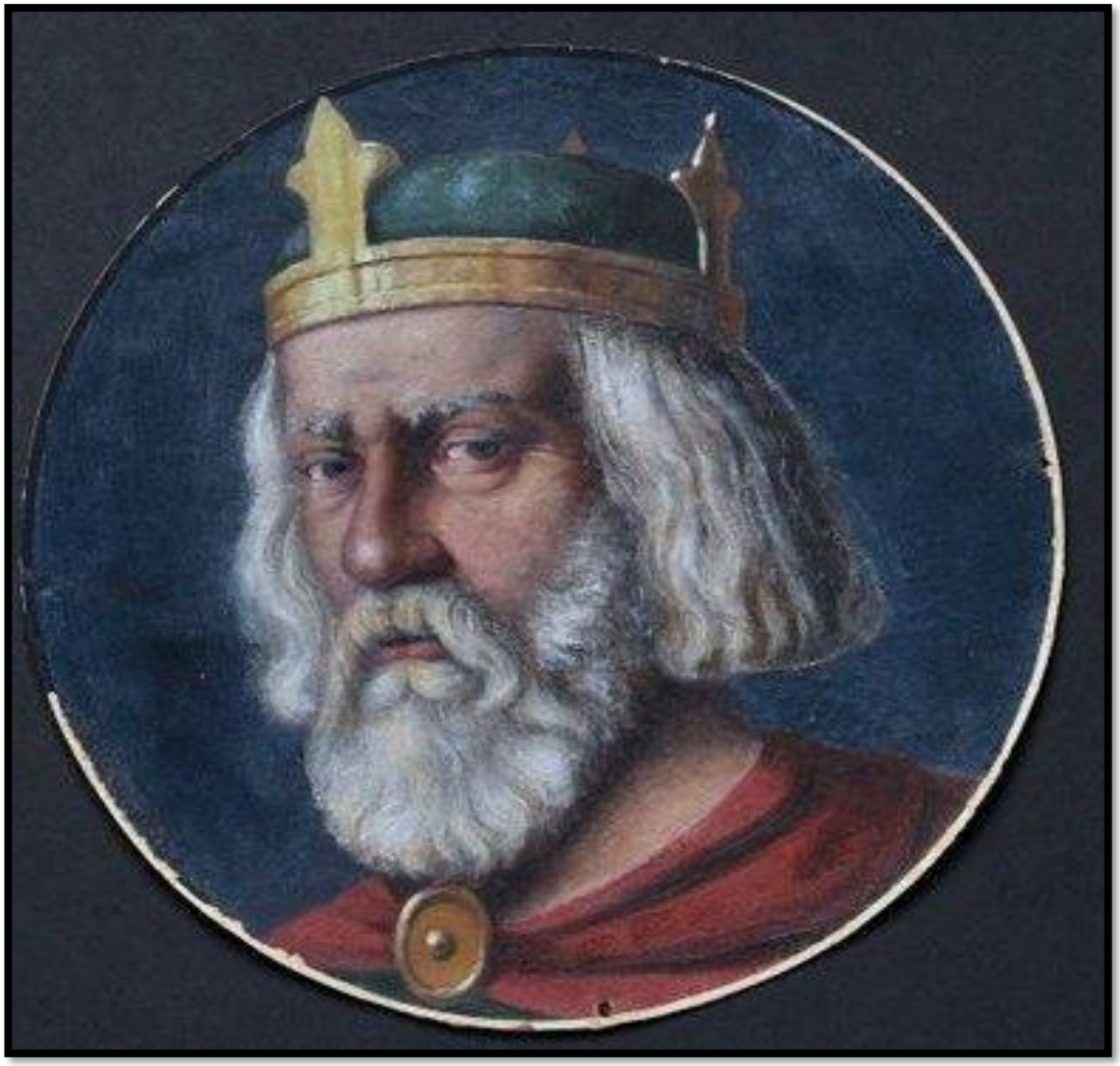

Figure 2. King Herald [3]

The brand name was given in the summer of 1997 when Sven Mattisson of Ericsson met with Jim Kardach of Intel in a local pub. They talked about history and Mattisson brought up a book called “The Longships” where he had learned about the King of Denmark, King Herald. Kardach went home after the meeting and researched more about King Herald and how he united several parts of Scandinavia together and building connections between separated groups. This makes sense as Bluetooth is all about connecting to devices.

2.1.3 Bluetooth Logo

As the name, the Bluetooth logo also came from Danish King Herald Bluetooth. The Bluetooth logo is the combination of the letter ‘H’ and the ‘B’ which are written in ancient letters that were used by the Vikings called runes. The letters can be seen in figure 3 below.

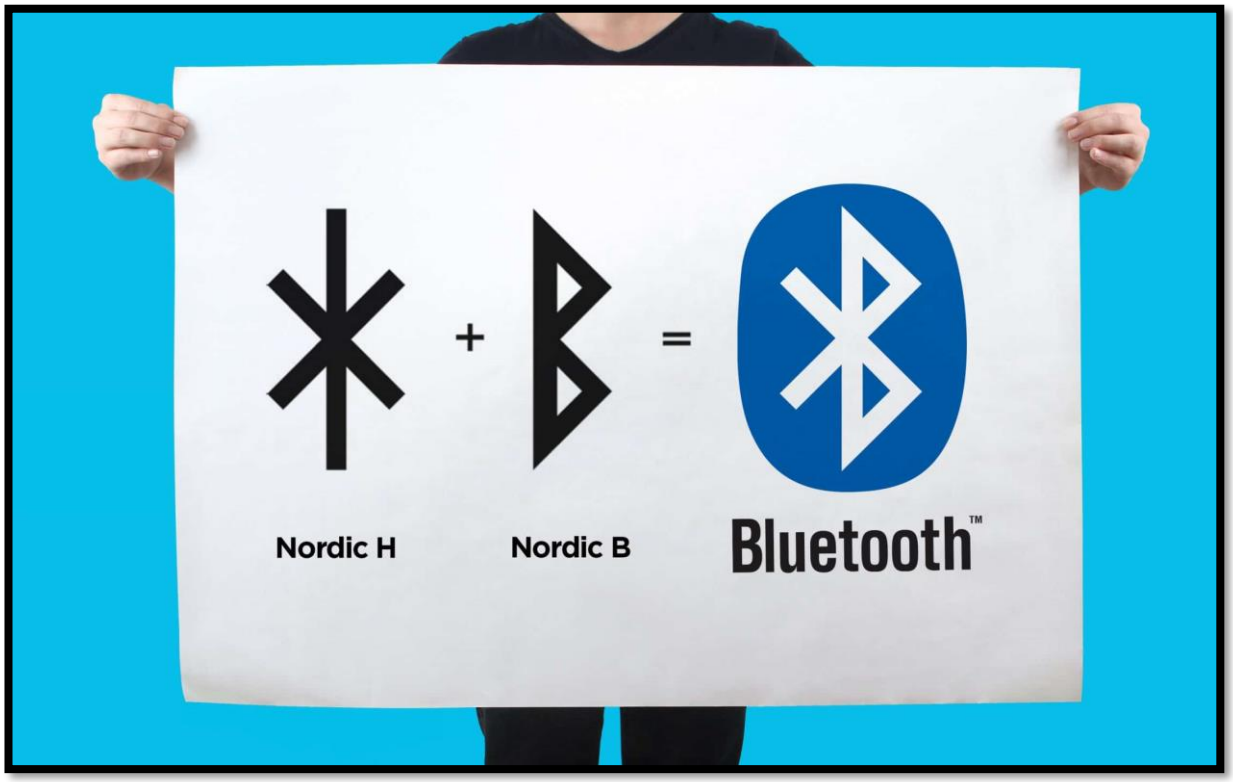

Figure 3. Bluetooth logo [4]

2.2 Working Principle

Like every other wireless communication as can be seen in figure 4 below, Bluetooth works by sending and receiving data in the form of radio waves by the help of a card-like attachment known as Bluetooth adapter in the Bluetooth enabled device. The Bluetooth adapter has the function of sending and receiving data and has a range of connection. The Bluetooth adapter is to be in range for the other adapter to communicate with it.

When they are in range, they can now communicate with each other in a process known as pairing.

Figure 4. Bluetooth adapter [5]

2.2.1 Communication Principle

As mentioned already above, Bluetooth uses radio waves to send data. When two devices are looking for each other to be paired, they are searching for a common frequency through which they can send and receive data. There are 79 frequency channels of frequency 2.4GHz in which the devices can be paired. When the common frequency is discovered, the devices are now found and can then send and receive the necessary

data. One good thing about Bluetooth connection is that the two devices connecting do not interfere other devices connecting in the same area because there are different channels (79) in which devices can communicate. Figure 5 below shows an example connection between a phone and an earphone.

Figure 5. Bluetooth pairing [6]

Another good thing about Bluetooth connection is that it is not limited to just two devices at a time meaning that multiple devices can send and receive data at same time in the same channel. When this happens, a small network is established and such micro-network formed between electronic devices is called a piconet (this can be seen in figure 6). In piconet, there must be more than two devices and not more than seven devices. Piconet uses master/slave kind of connection in which one of the devices is to be the master which creates or gives order for the connection to be created. The master devices control the communication between the other slave devices.

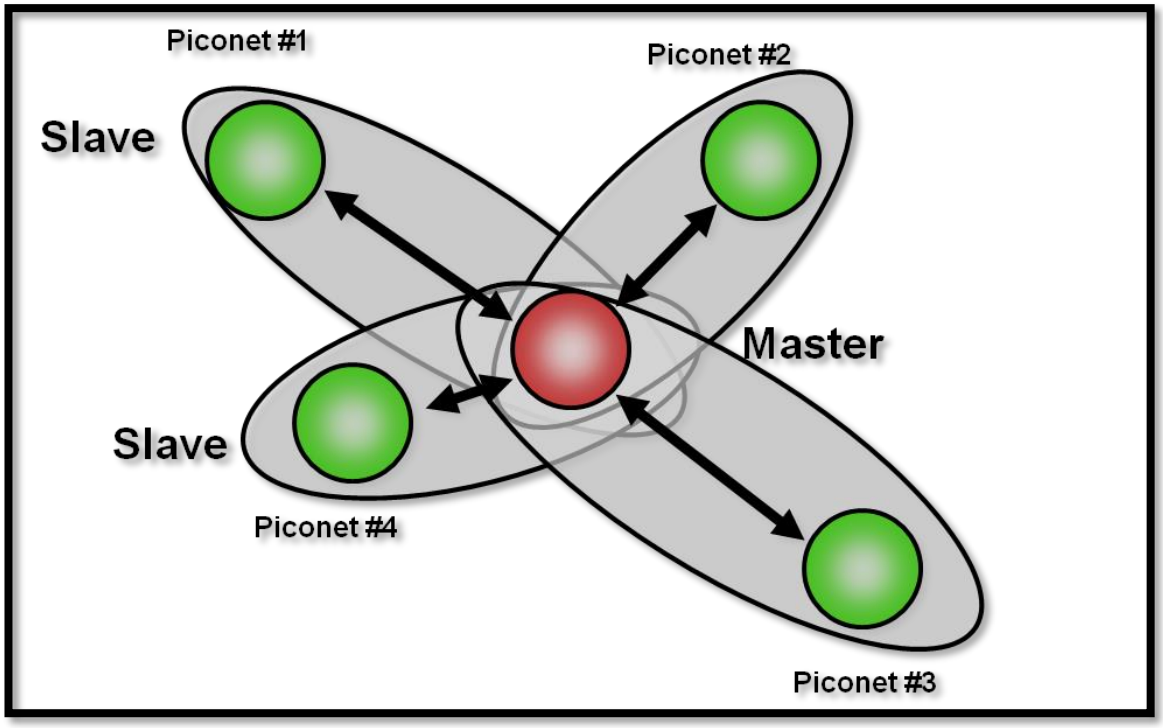

Figure 6. Piconet [7]

2.2.2 Establishing Connection

When a device is trying to establish a connection with another device, it goes through series of processes before it happens which include;

- Passive mode [8]
- Inquiry [8]
- Paging [8]
- Access point discovery [8]
- Creating channel [8]
- Pairing by pin [8]
- Using the network [8]

A device operating normally is in passive mode and during this time, it is listening to network.

When a master device (Device that sends request) is trying to establish connection with devices in its range, it sends inquiry which is called “access points” to those devices and then the devices reply with their address.

In a process known as paging, the master device then selects the address (This is usually the name of devices we see when trying to connect to another device) and then synchronizes with the access point by synchronizing the clock and frequency.

At this point, a link with the access point in now created which allows the master device to enter access point service discovery phase using a method called “service discovery method”.

At the end of this phase, the master device is now ready to establish a communication channel using protocol L2CAP

In order to restrict another device from accessing the encrypted connection, the access point sends a pairing request to the master device which asks the user to enter a pin before it proceeds to pair. This pin request does not happen in some devices.

When the two devices are paired, the master device is now able to use the established communication channel. Figure 7 below shows the pairing process between two devices (master and a slave)

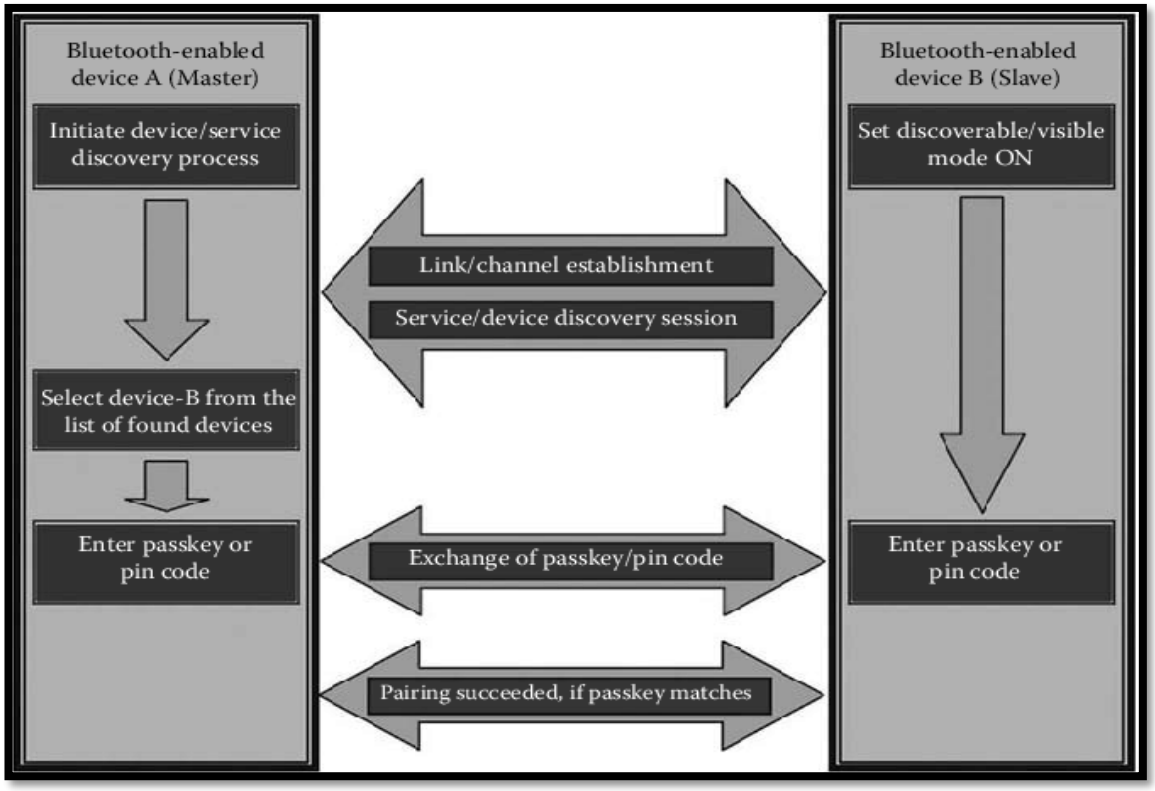

Figure 7. Bluetooth pairing process [9]

2.3 Bluetooth Specifications

2.3.1 Core Specification

This defines Bluetooth protocol stack and requirements for testing and qualification of Bluetooth-based products. This consists of five layers

- **Radio:** This specifies the requirements for radio transmission which includes frequency, modulation and power specifications for a Bluetooth receiver
- **Baseband layer:** This defines the physical and logical channels and link types
- **Link manager protocol:** This defines the process for the link setup and ongoing link management. [10]
- **L2CAP:** This is responsible for adapting upper-layer protocols to the baseband layer. [10]
- **Service discovery protocol:** This allows the querying of one device to another device for the device information, services provided and the characteristics of the services.

2.3.2 Profile Specification

This defines usage models that provide detailed information on how to use Bluetooth protocol for different types of applications

3 Bluetooth Versions

3.1 Version 1

Bluetooth version 1 contains three versions in total. Version 1.0 & 1.0b, version 1.1 and version 1.2.

Bluetooth 1.0 & 1.0b were released on July 1999 and it had many issues making it difficult for manufacturers to make their products exchange and use information between each other. These two versions also had compulsory Bluetooth hardware device address transmission in the connecting process.

On February 2001, Bluetooth 1.1 was released to fix some of the issues experienced on versions 1.0 & 1.0b. The main improvement on this version over the previous one was authentication. The process of generating the key depends on the device that is to establish the connection which is the master and how quickly the slave responds to the master's communications. If the slave can read the information faster than the master, this will cause a confusion as the slave and master will start to think that both are master. This error causes the devices to not generate matching keys causing the devices not to talk to each other since they generate different keys. Version 1.1 solved this issue by defining the steps that involves authentication more thoroughly.

Bluetooth 1.2 was released on November 2003 and this version had some improvements on the older versions and was also backward compatible with version 1.1. Some of the improvements to this version include;

- Extended Synchronous Connections (eSCO) [11]
- Host Controller Interface (HCI) support [11]
- Higher transmission speed [11]
- Adaptive frequency-hopping spread spectrum which improves resistance to radio frequency interference by avoiding the use of crowded frequencies in the hopping sequence. [11]

This version was certified as IEEE standard 801.15.1-2005

3.2 Version 2

The second version 2.0 was released on November 2004. The major difference of this to the older version was the introduction of EDR (Enhanced Data Rate). This helped in increasing transmission speed to 2.1Mbit/s, also lowered the power consumption by reducing the duty cycle.

After about three years on July 2007, version 2.1 was released and added some features which include;

- Extended inquiry response: Provides more information about devices for better filtering of devices during connection such as name of device, time for day and other necessary information.
- Sniff subrating helps in reducing the amount of power consumed by a device when in sniff low-power mode.
  This feature was created to help improve battery life for devices that are usually inactive such as keyboard, mice etc. This feature also enables devices with Bluetooth version 2.1 and above to decide how long they wait before sending keepalive message to each other. The previous implementation of keepalive

message were sent as frequently as several times per second but in Bluetooth version 2.1, devices where allowed to send these messages dynamically which can be once in 5 or 10 seconds and therefore helps in extending battery life [12]

- Cooperation with NFC: There is automatic creation of secure Bluetooth connections when two devices that has NFC enabled are in contact. This makes it so much easier and lets you skip the pairing process of only Bluetooth.
- Encryption pause resume: This enables an encrypted key to be refreshed which enables stronger encryption for connections that stay longer than 23.3 hours which is “One Bluetooth day”.

3.3 Version 3

Bluetooth 3 has only one version and that was version 3.0 which was released on April 2009.

The main feature that was added to this version was the simplification of discovery and setup of devices and making Bluetooth devices show all type of services that they provide

Bluetooth 3.0 is also known as high speed (HS) because of greatly improved speed over older versions. This allowed faster transmission rate to 20Mbits/s

Bluetooth 3.0 was adopted by SIG on August 2009

3.4 Version 4

This version contains three revisions which include version 4.0, version 4.1 and version 4.2

Version 4.0 was released on December 2009 and this improved some features such as improved connectivity and range but the most interesting improvement on this version is the introduction of Bluetooth Low energy protocol which involves putting device into sleep mode or ultra-low power idle mode when the device is not in use for a long time.

Bluetooth 4.1 was released on 4 December 2013 and it introduced updates such as;

- Better connections: This provides manufactures with more control over creating and maintaining Bluetooth connections by making the re connection time interval flexible and variable. Devices can now reconnect automatically even after going out of range and back. The user does not have to connect manually again.
- There was an improvement in data transfer by introducing a technology known as “Bluetooth smart technology” which provides bulk data transfer.

On 2nd December 2014, Bluetooth 4.2 was released. This version was mainly the improvement of speed to up to 2.6x faster than the older versions and this meant faster downloads.

3.5 Version 5

This is the latest version of Bluetooth and to date it contains two version; Version 5.0 and recently (yet to be released) 5.1.

Bluetooth 5.0 was released on December 2016 and there are few improvements over the previous version 4 which include

- Low energy for wireless headphones and other Bluetooth devices. Although this was introduced in the previous version, this feature is always being improved as power efficiency is important. Now, Bluetooth devices can hold charges for a long period of time without needing to recharge the Bluetooth device
- Dual Audio: This is a whole new feature which is only available in version 5.0. Previously, it was not possible to play audio on two connected devices at same time but now with this feature added to 5.0, it is possible
- Improved speed and range: This version also improved the speed of transmission and range in which data can be transmitted.

The latest version to date which is version 5.1 and released on January 2019. This is freshly released and so far, not much is known about it and no device supports it yet.

3.6 Summary

Table 1 below summarizes the differences in the Bluetooth versions which include EDR, HS, LS, Range, Speed and the improvements made compared to version 1.

Bluetooth Version	Basic Speed	En-hanced data speed	High speed	Low en-ergy (LS)	Speed/Data rate	Range
1	✓	×	×	×	1Mb/s	10m
2	✓	✓	×	×	3Mb/s	30m
3	✓	✓	✓	×	24Mb/s	30m
4	✓	✓	✓	✓	24Mb/s	60m
5	✓	✓	✓	✓	48Mb/s	200m

Table 1. Differences between Bluetooth versions [13]

4 Practical Work

The nRF51-DK development kit was used for this practical work. The goal was to configure the device to be able to measure heart rate and send the measurement to our device via Bluetooth. To be able to configure the heart rate sensor of the device, we will need to write a code which enables the heart rate functionality of the device. For this work, we will need:

- nRF51-DK
- Micro usb cable
- A c/c++ compiler
- A Bluetooth enabled phone (Android v4.4 or later or Iphone)

4.1 nRF51-DK

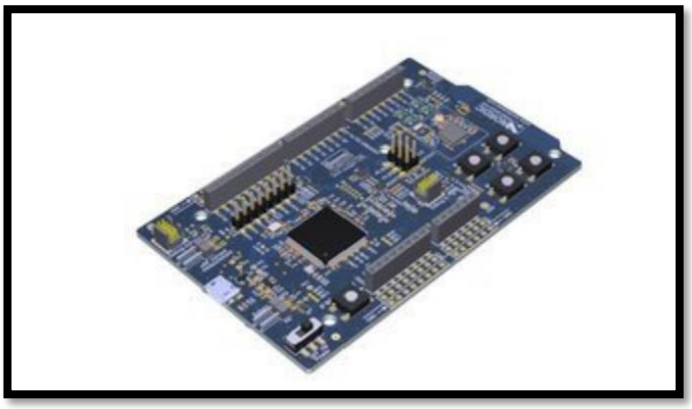

Figure 8. nRF51-DK [14]

The kit which can be seen in figure 8 is a single-board kit for Bluetooth smart, ANT and 2.4GHz applications using the nRF51 series SoC. This kit supports the following:

- nRF51822 and nRF51422 system on Chips.
- Arduino Uno 3. This makes it possible to use other shield that are compatible with this kit.
- Nordic software tools using Keil, IAR and GCC
- ARM mbed tool chain which aids in fast prototyping and development

There are different software examples which are available from the device SDK to support Bluetooth, ANT and 2.4GHz applications. [14]

Figure 9 below shows the full label of nRF51-DK

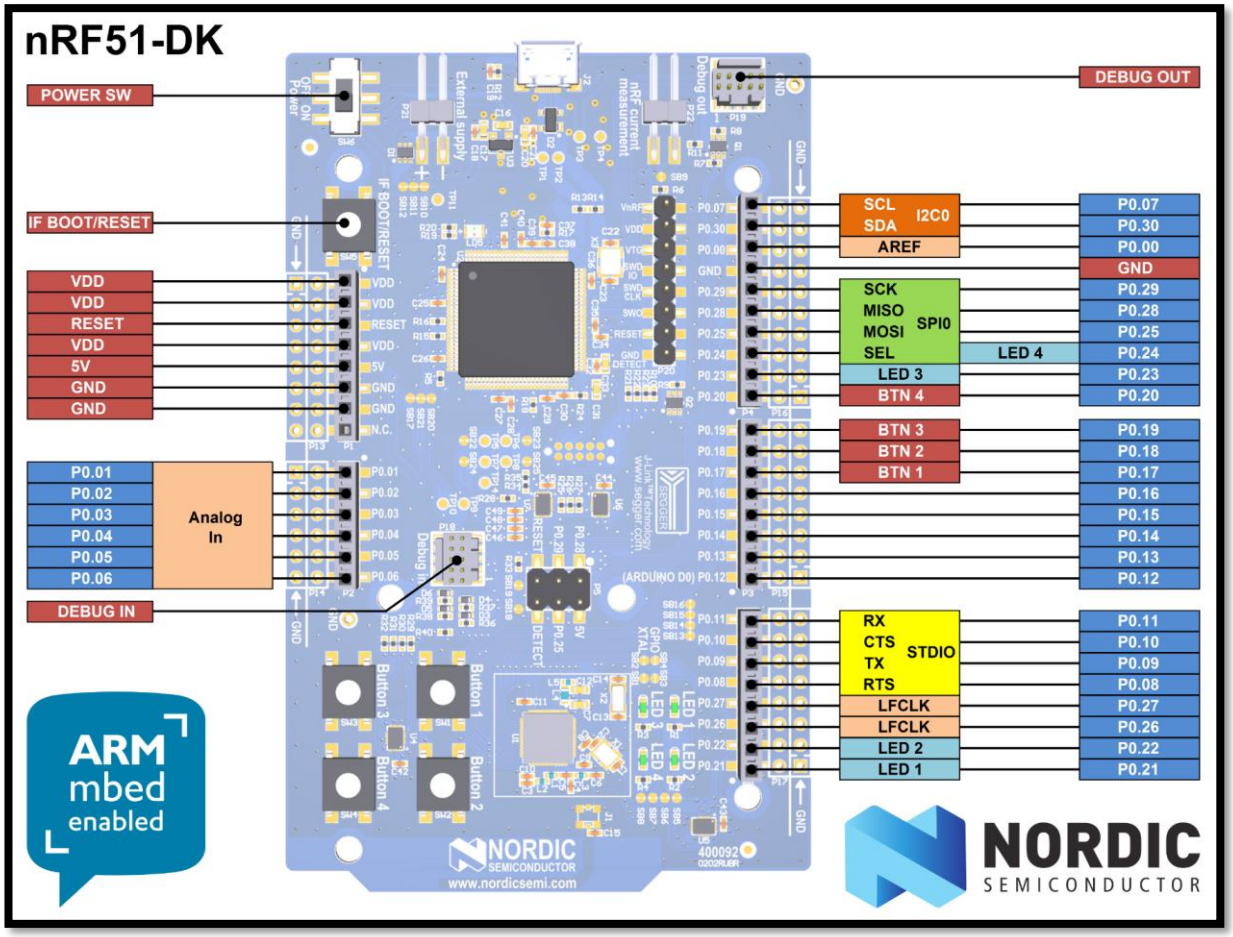

Figure 9. nRF51-DK whole body label [14]

4.2 Features

- Nordic nRF51 is optimized for ultra-low power consumption by combining Bluetooth v4.1 2.4GHz multiprotocol radio and ARM Cortex-M0 processor on a single chip.
- It has Arduino Revision 3 connector for use with 3rd party shields
- It has pins for power consumption measurements
- It accepts power through USB cable, battery and external source
- It supports drag and drop programming. This allows you to drag files into the mbed disk when connected to a computer.

- Segger J-Link Debugger with debug functionality
- Connector for RF measurements
- Buttons and LEDs for user interaction
- It is 2.4 compatible with nRF24L devices

4.3 Details

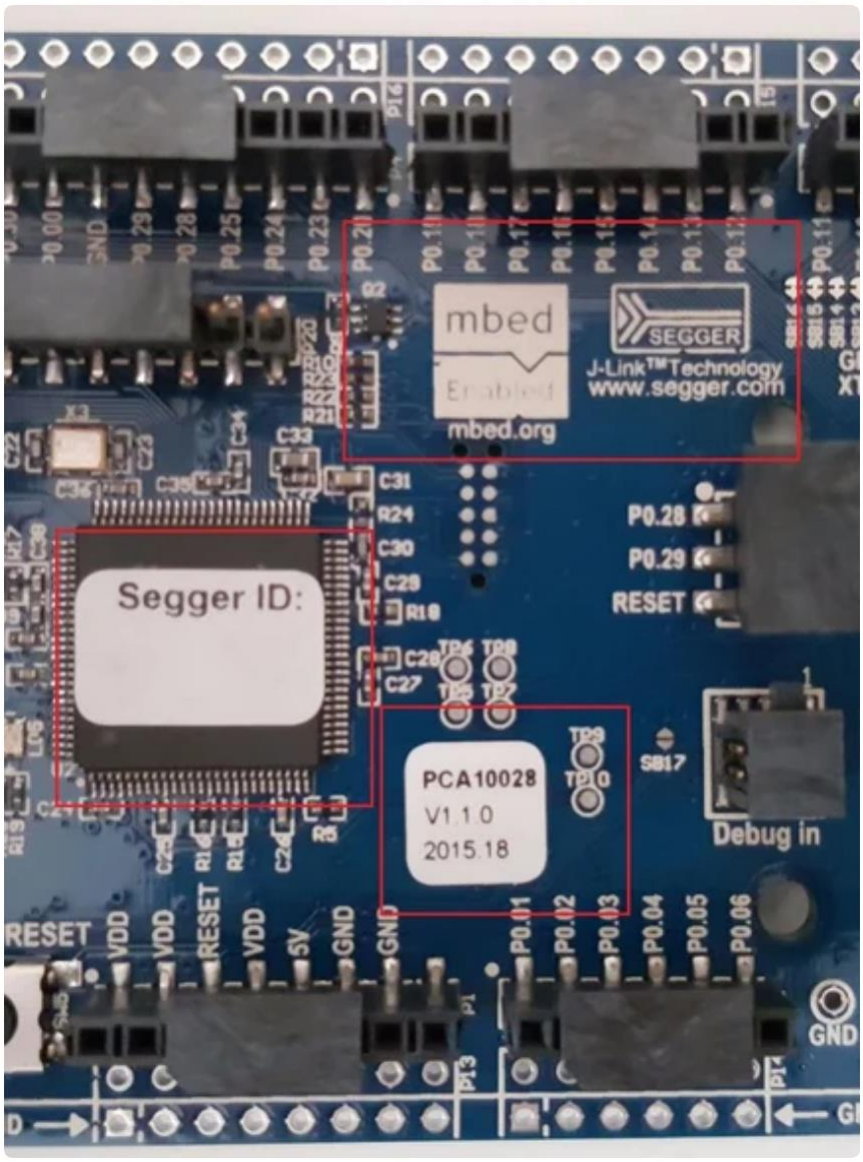

Figure 10. nRF51-DK mbed, Segger ID and version labels [15]

As seen from figure 10, the parts marked with a red square contains the mbed, segger ID and the version.

- Mbed enabled
- Segger ID sticker with PCA10028 v1.1.0 2015.11
- Segger J-Link Technology

1. Mbed enabled means you can write code online on mbed.org website

2. Segger J-Link technology allows sending of hex file to nRF51-DK board when plugged to a computer from a compiler.

4.4 Experimental Procedure

4.4.1 Getting the code ready

First, I had to get the code which will enable the Bluetooth functionality of the mbed device to connect to a Bluetooth enabled phone. I used an online compiler mbed.org which you can register for personal use free. In the online compiler, I added my device from the top right corner as seen in figure 11

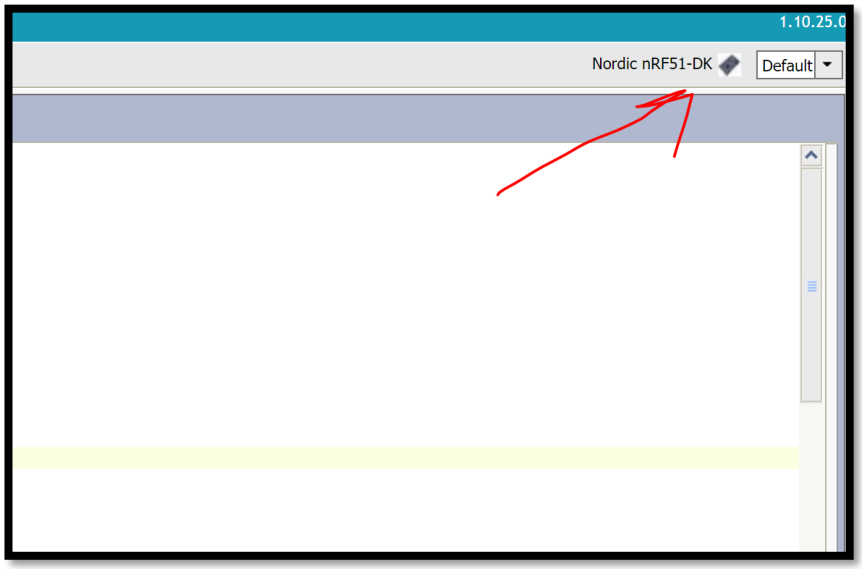

Figure 11. adding nRF51-DK to the online compiler

Figure 12 shows how I imported the code from the os.mbed.com which will enable us to connect to our device.

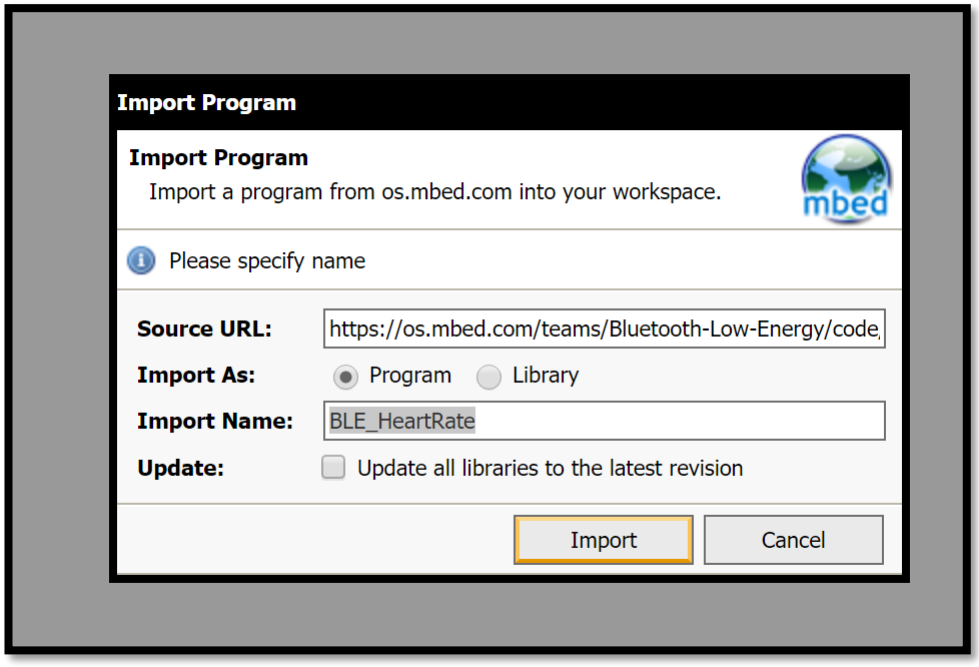

Figure 12. importing the program for enabling nRF51-DK heart rate sensor [16]

After importing the program, I compiled the code and was downloaded as a hex file.

4.4.2 Connecting nRF51-DK to our pc/laptop

To use the code, the mbed device is first connected to the computer so that the hex file can be dragged to the drive's folder. The procedure is as follows;

- Plug in micro usb cable to nRF51-DK board
- Plug in the other side of micro usb cable to your computer

When the computer has recognized the device as can be seen from figure 13, I dragged the hex file which was previously complied and downloaded to the mbed drive

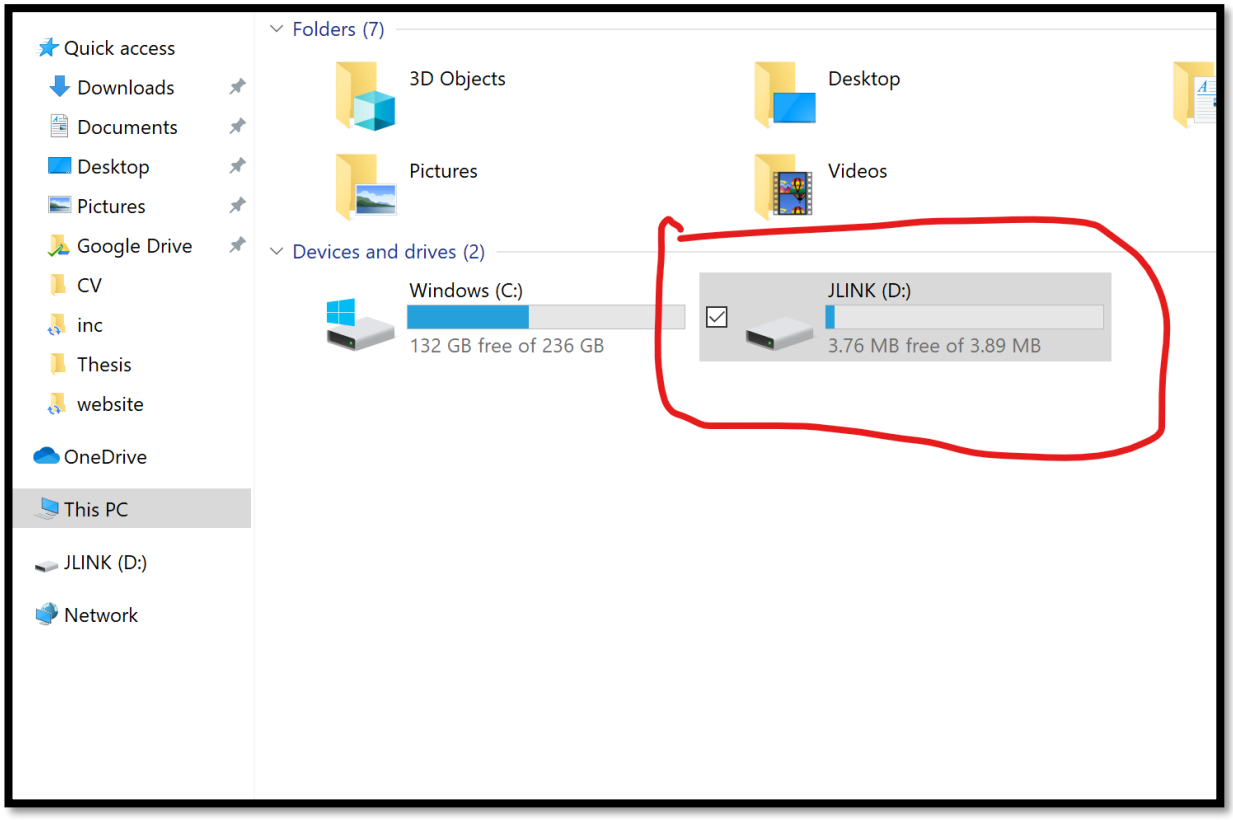

Figure 13. JLINK disk after connecting with my laptop so I can drag and drop the Hex file

When the mbed device reads the hex file, there is going to be a steady light on led 5 of the device (this can be seen from figure 14) and this means that it is ready to connect to the phone's Bluetooth.

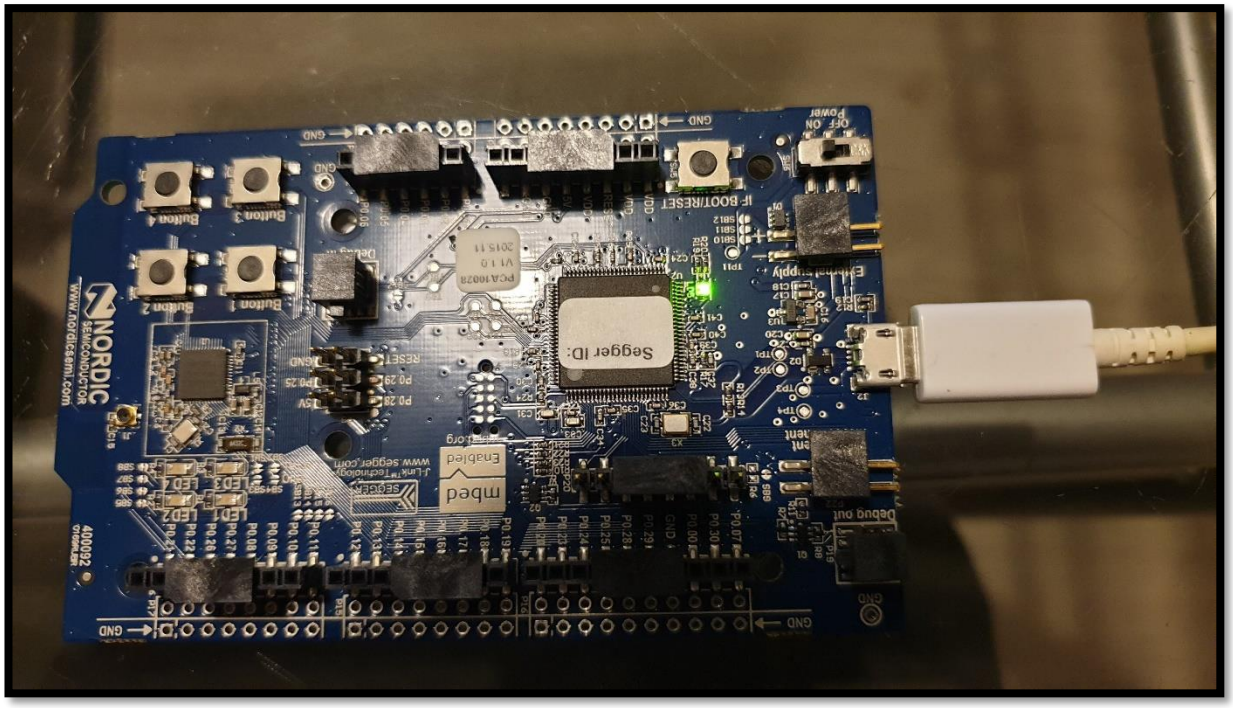

Figure 14. Steady light on Led 5 of the device confirming that it is ready for Bluetooth connection

To connect the device to my phone, I used a software “nRF connect” which can help with connecting the device, displaying the mac address of the device and displaying the reading of the heart rate.

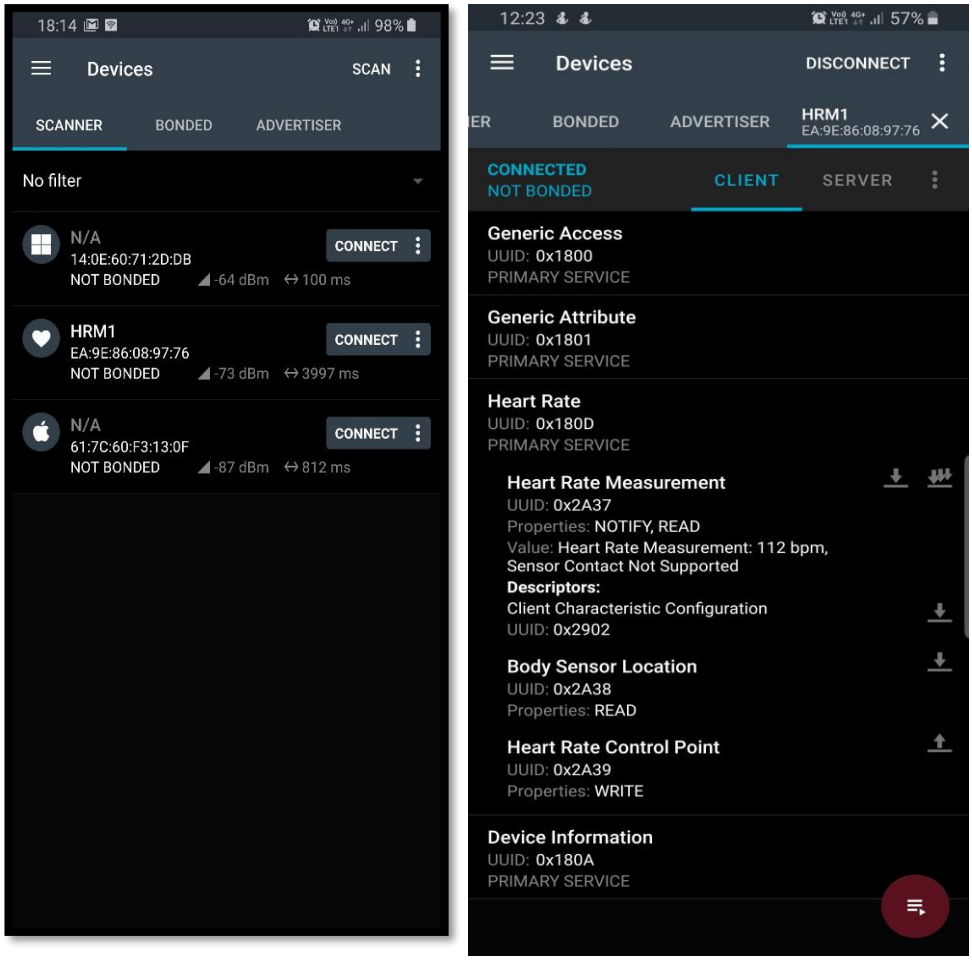

Figure 15. nRF connect reading

In Figure 15 above, the left picture shows that the device has been discovered by the nRF app and ready for connection. The picture on the right shows the MAC address of the mbed device and most importantly the heart rate showing the heart rate measurement, the descriptors, the sensor location in the body and the control point. The 112bpm reading shown above is a simulated sensor reading as there is actually no sensor connected to measure the real sensor of the body.

4.5 Analysis

In this section the code which helps to enable the Bluetooth connection is explained.

BLEDevice

```
#include "BLEDevice.h"

BLEDevice  ble;

void disconnectionCallback(Gap::Handle_t handle, Gap::DisconnectionReason_t reason)
{
    ble.startAdvertising(); // restart advertising
}

int main(void)
{
    ble.init();
    ble.onDisconnection(disconnectionCallback);
 ...
    ble.startAdvertising();

    while (true) {
...
            ble.waitForEvent();
...
    }
}
```

Figure 16. This shows the declaration of BLEDevice, the init() function and the other methods explained below [16]

In figure 16 above, there is an init() method that must be called before using the BLE-Device object. The startAdvertising() method is called to advertise the device's presence allowing other devices to connect to it.

onDisconnect() is used to set up and event handler prompting a callback function which restarts advertising when the connection is terminated.

The method, waitForEvent() is called whenever the main thread is done doing any work. This hands the control over to the protocol which helps in saving power. Whenever there is an interruption, this causes an event callback to be initialized. In this program, the ticker object is setup to call a function every second and whenever the ticker ticks, the periodicCallback() is called and the waitForEvent() return which resumes the execution in the main[16]

Interrupt to trigger periodic actions

```
void periodicCallback(void)
{
    led1 = !led1; /* Do blinky on LED1 while we're waiting for BLE events */

    /* Note that the periodicCallback() executes in interrupt context, so it is safer to do
     * heavy-weight sensor polling from the main thread. */
    triggerSensorPolling = true;
}

int main(void)
{
    led1 = 1;
    Ticker ticker;
    ticker.attach(periodicCallback, 1);
...
```

Figure 17. This shows the periodicCallback() method and the triggerSensorPolling explained below [16]

In figure 17, the periodicCallback() is called in only interrupt context and should not engage in heavy tasks to avoid the system being unresponsive. triggerSensorPolling is used to mark some activity as pending and to be handled in the main thread.

BLEDevice offters APIs to setup GAP for connectivity and GATT for services. GATT services may be composed by defining characteristics and attributes seperately

Service setup

```
/* Setup primary service. */
uint8_t hrmCounter = 100;
HeartRateService hrService(ble, hrmCounter, HeartRateService::LOCATION_FINGER);

/* Setup auxiliary services. */
BatteryService           battery(ble);
DeviceInformationService deviceInfo(ble, "ARM", "Model1", "SN1", "hw-rev1", "fw-rev1", "soft-rev1");
```

Figure 18. This shows the setting up of the connectivity and other advertisement packets [14]

Setting up GAP mostly has to do with configuring connectivity and payload contained in advertisement packets. This can be seen from figure 18.

```
/* Setup advertising. */
ble.gap().accumulateAdvertisingPayload(GapAdvertisingData::BREDR_NOT_SUPPORTED | GapAdvertisingData::LE_GENERAL_DISCOVERABLE);
ble.gap().accumulateAdvertisingPayload(GapAdvertisingData::COMPLETE_LIST_16BIT_SERVICE_IDS, (uint8_t *)uuid16_list, sizeof(uuid16_list));
ble.gap().accumulateAdvertisingPayload(GapAdvertisingData::GENERIC_HEART_RATE_SENSOR);
ble.gap().accumulateAdvertisingPayload(GapAdvertisingData::COMPLETE_LOCAL_NAME, (uint8_t *)DEVICE_NAME, sizeof(DEVICE_NAME));
ble.gap().setAdvertisingType(GapAdvertisingParams::ADV_CONNECTABLE_UNDIRECTED);
ble.gap().setAdvertisingInterval(1000); /* 1000ms */
```

Figure 19. This shows the general discoverable, the id and the name of the device methods are declared [16]

In figure 19, the first line is compulsory for Bluetooth smart and says that this device only supports Bluetooth low energy. The GENERAL_DISCOVERABLE is used to make it discoverable by other devices in order to connect. Next is the ID for the heart rate sensor and the name of the device.

After the payload is set, the code sets the advertising type and the advertising interval. In Bluetooth smart timing, values are multiples of 1000ms.[16]

5 Applications of Bluetooth

Bluetooth is a popular and widely used technology and we encounter it every day of our lives. Some of the applications of Bluetooth include:

5.1 Transfer of files

Figure 20. Bluetooth file transfer between a phone and a laptop [17]

Figure 20 shows the transfer of files between a laptop and a phone. This is arguably the most popular use of Bluetooth technology. Although it might be slower than a cable transfer or by using let's say a flash drive or a hard drive, this can be really useful if you forget your devices at home or you are in a place where you cannot access your storage device. With two Bluetooth enabled devices, you can always transfer files between them wirelessly. [18]

5.2 Home Security/Smart Home Control

The picture below shows the use of smart phone to control door security

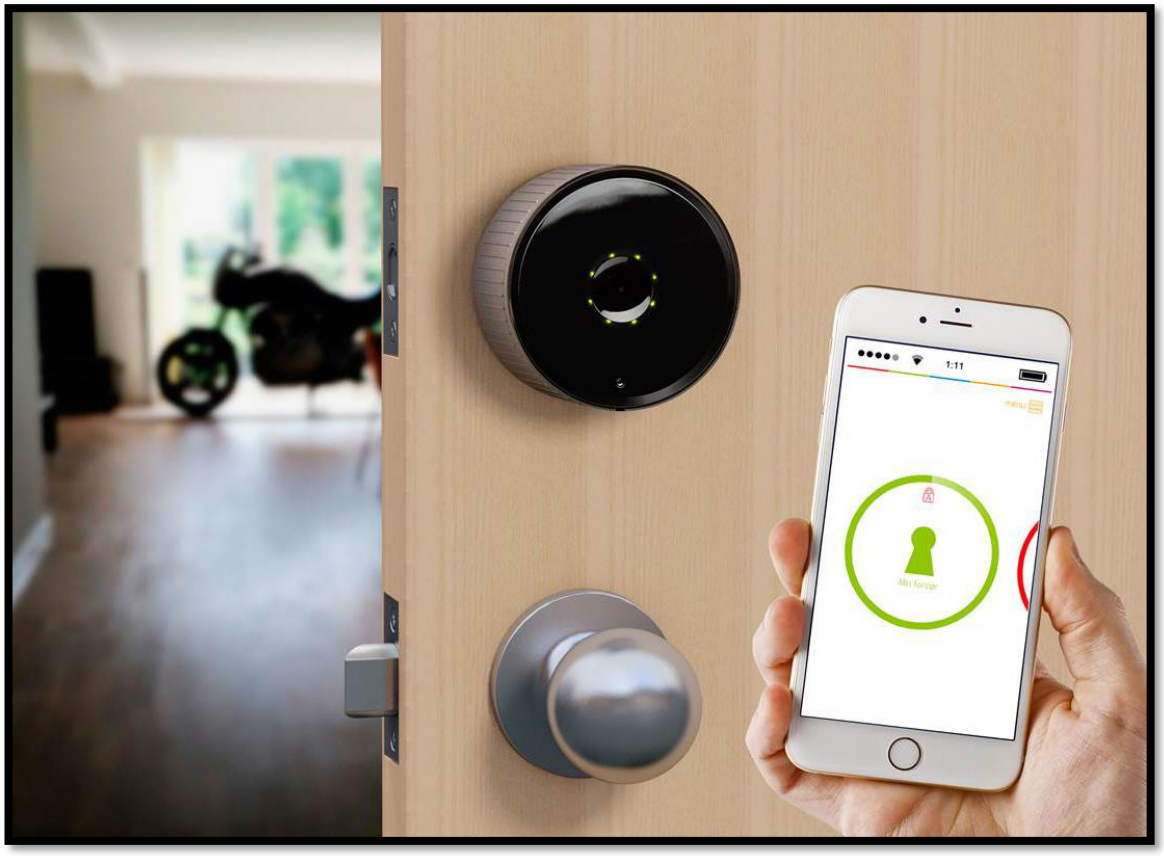

Figure 21. Bluetooth home security control [19]

Security doors can be controlled with a Bluetooth enabled smartphone as seen in figure 21. This is one of the most important use of Bluetooth. Some security locks these days come with Bluetooth support so you can control your security lock wirelessly without the need of your key. It can come in handy if you forget your key so with this, you can easily access your home or your work place without any trouble.

Aside from security, there are numerous things that can be controlled wirelessly. You can control your light, home assistant device like Google home, Amazon home, Apple homepod etc, TV, air conditioner etc. It makes controlling your home devices very convenient as you can control anything wirelessly by using Bluetooth from your phone.

5.3 Connecting Different Devices

There are numerous devices that can share information with each other by simply connecting them with Bluetooth. These devices include headphones, game controllers,

printers, keyboards etc. Figure 22 shows a sample connection between a headphone and a laptop.

Figure 22. connecting headphone to laptop [20]

5.4 Bluetooth Tethering

This is a surprising feature as you can share internet from your phone to your pc or other devices by Bluetooth. This is an important feature and it is very useful to have.

6 Bluetooth Security, Advantages/Limitations Of Bluetooth

6.1 Bluetooth Security

Security is a very important aspect of any wireless system and Bluetooth is no exception. The increasing number of hackers who can gain access to wireless system is increasing and this makes Bluetooth security very important as any device can be spied on or is open to access without security. Through the various updates on Bluetooth down the years, the security has been updated as well and is being updated often. Bluetooth security is not limited in the software alone, it is also implemented in the hardware.

Bluetooth security is provided in these means:

- **Authentication**: Authentication involves the verification of the device that is trying to communicate [21]

- **Confidentiality**: This makes sure that only the devices which are intended to communicate can gain access to device data [21]

- **Authorisation**: This makes sure that the device is given permission to use a service before it can be enabled to do so [21]

6.1.1 Bluetooth security modes

There are four security modes in which a device can operate on.

- **Security mode 1**: This is a non-secure mode. Devices operating in this mode do not have any way to prevent other devices from connecting to them. The good side of this mode is that it is very easy to establish connection between two Bluetooth-enabled devices but while it can be easy to establish connection, the authentication is also easily bypassed. This kind of security mode was supported upto 2.0 backwards.

- **Security mode 2**: In this mode, there is a manager that helps in controlling access to certain services and devices and also helps in maintaining rules for access control and interfaces with other protocols and device users.

  There is possibility on applying different trust levels and rules to limit access for applications which have varying security requirements even as they as work in parallel. There is also possibility to give permission to some services and not other services. This idea of authorisation was initiated in this mode. By making use of this, it is possible to know if a certain device has the permission to some services. [22]

- **Security mode 3**: In this mode, security procedure is initiated before establishing any link. Also, validation and encryption are used for the connections going to or coming from the device

  A separate link key which is secret, is shared by devices that has been paired

  This mode is only available on devices which have 2.0 + EDR and backwards. [22]

- **Security mode 4:** This is the most recent security mode used by most devices. This mode was introduced in Bluetooth update 2.1 + EDR**.**

  In Bluetooth Security Mode 4 the security procedures are initiated after link setup. Secure Simple Pairing uses what are termed Elliptic Curve Diffie Hellman techniques for key exchange and link key generation.

  The security requirements for services protected by Security Mode 4 are as below:

  - Authenticated link key required
  - Unauthenticated link key required
  - No security required

  Whether or not a link key is authenticated depends on the Secure Simple Pairing association model used. Bluetooth Security Mode 4 is mandatory for communication between v2.1 + EDR devices. [22]

6.1.2 Bluetooth security issues

- **Bluebugging**: This is a type of a security issue which occurs when a hacker or attacker accesses a mobile phone commands using Bluetooth and does not notify the phone's user. The attacker can do numerous things with the Bluetooth enabled device like make phone calls, send messages, change phonebook contacts and can even connect to the internet. [23]

- **Bluejacking**: This is a method in which an attacker can send messages (anonymously) to other Bluetooth-enabled devices in a certain range. This is not as severe as bluebugging because the attacker is limited to only text messages but it is still a security issue

- **Bluesnarfing**: This involves the stealing of information from Bluetooth device. The attacker can steal information such as contacts, text messages, calendar etc and will not leave any trace of attack so the owner of the device will not be away of any attack.

- **Car whispering**: In this security issue, a hacker can use a software to send and receive audio to and from a Bluetooth enabled car stereo system [23]

6.2 Advantages of Bluetooth

The list below shows the benefits of Bluetooth technology

- It requires low power [24]

- It has very minimal interference

- It can be used to answer phone calls and doing other things while driving

- It is also used for voice and data transfer

- It has a very good range especially when compared with infrared communication [24]
- It is popular and used in many products such as controllers, phones, keyboards etc
- Most Bluetooth devices are very cheap [24]
- Bluetooth radiation know as microwave radiation can penetrate through objects and that means that Bluetooth connections cannot usually be interfered by walls, human beings etc
- Bluetooth does not interrupt cellular network like wifi

6.3 Disadvantages of Bluetooth

These are the most common limitations of Bluetooth

- The bandwith is low especially when compared to WiFi
- Although Bluetooth uses lower power, it still consumes battery more when compared to when Bluetooth is not used [24]
- Bluetooth security is somewhat questionable because it can be vulnerable to attacks
- It can lose connection in certain conditions

7 Summary

Bluetooth is a technology that has been in existent since 1995 when it was developed by Haartsen and his partner Sven Mattison. It was named after a Danish king called Herald who had a “blue/dead” tooth because he united several parts of Scandinavia together since Bluetooth is used for creating communication between devices. The famous logo of Bluetooth came from the combination of letter “H” and “B” written in runes which were used by Vikings in the ancient times.

Since the discovery of Bluetooth, it has seen so many updates via different versions. First was Bluetooth 1.0 & 1.0b which were released in July 1999 and then version 1.1 and 1.2 which were released on February 2001 and November 2003 respectively. 1.1 and 1.2 fixed some issues experienced in previous versions such as authentication problem. Version 2.0 was released on November 2004 and this saw the introduction of EDR (Enhanced Data Rate) that helped to increase speed. Version 2.1 was released on July 2007 and version 3.0 was released 2 years later, on April 2009. In 2009, 2013 and 2014, version 4.0, 4.1 and 4.2 were released respectively and there were some improvements such as speed to 2.6x faster, improved connectivity and range. The latest version of Bluetooth is 5.0 and this was released on December 2016 which introduced features such as dual audio, low energy for wireless headphones.

Like in most technologies, security is arguably one of the most important things to focus on. Bluetooth has its security and that has been improved since release. Bluetooth security involves authentication which is the verification of the device trying to communicate, confidentiality which makes sure that only the devices trying to communicate has access to the data and authorisation which makes sure the device is given permission to use a service before it can be allowed to do so. There are also different security modes that Bluetooth devices must have. A device must operate on one of the security modes to ensure safety when connecting to another device. Security mode 1, 2 and 3 being the oldest and not used by current devices. Security mode 4 is the latest and most improved mode which was introduced in Bluetooth 2.1 + EDR. Although there are good security measures in Bluetooth devices, there are still some security issues to worry about. Bluebugging, Bluejacking, Bluesnarfing and Car whispering are all security issues which can be experienced by any Bluetooth enabled device. Bluebugging occurs when hacker has

access to a mobile phone command without the owner knowing. Bluejacking occurs when a hacker can send text messages. Bluesnarfing occurs when a hacker steals information from a Bluetooth device such as contacts, text messages etc. Car whispering is when a hacker can use a software to send and receive audio to and from a Bluetooth enabled car stereo system.

Bluetooth is a widely used technology and it has so many applications such as transferring of files between Bluetooth enabled devices, Home security or smart home control, for connecting different devices such as phone and a Bluetooth headphone, Bluetooth tethering etc.

Although there are other wireless technologies, Bluetooth has some advantages over those technologies. Some of the advantages are: minimal interference, can be used for voice and data transfer, does not interrupt wifi, requires low power etc. There are some disadvantages of Bluetooth such as: low bandwith, questionable security, can lose connections in certain conditions etc.

In conclusion, Bluetooth is a technology that is very useful and has made the connectivity and exchanged of information between devices easier and better.

.

References

1 Bright. *Nederlandse Bluetooth-uitvinder in Hall of Fame*, 6 April 2015. [online] Available from: https://www.bright.nl/nieuws/artikel/3998512/nederlandse-bluetooth-uitvinder-hall-fame [Accessed 6 March 2019]

2 Adam. *The History of Bluetooth*, 2 August 2017. [online] Available from: http://www.mobileindustryreview.com/2017/08/the-history-of-bluetooth.html [Accessed 25 Nov 2019]

3 Steemit. *The modern technology called Bluetooth was named after a powerful Viking king called herald Bluetooth*, [no date] Available from: https://steemit.com/technology/@blinks/the-modern-technology-called-bluetooth-was-named-after-a-powerful-viking-king-called-harald-bluetooth [Accessed 10 March 2019]

4 Stewart. *Feeling blue: A history of Bluetooth and the story behind the Bluetooth logo*, [13 March 2018]. [online] Available from: http://fabrikbrands.com/bluetooth-history-and-the-bluetooth-logo/ [Accessed 11 March 2019]

5 Walmart. *EEEKit usb Bluetooth 4.0 CSR4.0 Adapter dongle for pc laptop Win XP VISTA 7 8 10*, [no date]. [online] Available from: https://www.walmart.com/ip/EEEKit-USB-Bluetooth-4-0-CSR4-0-Adapter-Dongle-For-PC-Laptop-WIN-XP-VISTA-7-8-10/134130167 [Accessed 13 March 2019]

6 Bragi. *The Headphone-connect The Headphone Via Bluetooth*, [no date]. [online] Available from: https://support.bragi.com/hc/en-us/articles/115000129149-The-Headphone-Connect-The-Headphone-via-Bluetooth?mobile_site=true [Accessed by 10 March 2019]

7 Microchip. *Bluetooth Low Energy Connection Process*, [no date]. [online] Available from: http://microchipdeveloper.com/wireless:ble-link-layer-connections [Accessed 14 March 2019]

8 gc. *Establishing connections in Bluetooth, [18 Feb 2013].* [online] Available from: http://www.tutorial-reports.com/wireless/bluetooth/establishingconnections.php [Accessed 25 Nov 2019]

9 Yasir. *Secure Device Association Trends and Issues*, [2010]. [online] Available from: https://www.researchgate.net/figure/Bluetooth-pairing-process_fig2_295703327 [Accessed 7 March 2019]

10 Elprocus. *How does Bluetooth Work?*, [no date]. [online] Available from: https://www.elprocus.com/how-does-bluetooth-work/ [Accessed 30 March 2019]

11 *Specifications,* [no date]. [online] Available from: http://blue-tooth.50webs.com/bluetooth1_and_1.0b.html [Accessed 25 Nov 2019]

12 Margaret. *Sniff subrating*, [Feb 2008]. [online] Available from: https://search-mobilecomputing.techtarget.com/definition/sniff-subrating [Accessed 30 April 2019]

13 Marc. *Bluetooth versions*, [6 July 2017]. [online] Available from: https://www.rtings.com/headphones/learn/bluetooth-versions-comparison-profiles [Accessed 25 March 2019]

14 Arm. *Nordic NRF51-DK*, [no date]. [online] Available from: https://os.mbed.com/platforms/Nordic-nRF51-DK/ [Accessed 6 Nov 2019]

15 Bay. *The first usage of NRF51-DK*, [no date]. [online] Available from: https://www.instructables.com/id/The-First-Usage-of-NRF51-DK/ [Accessed 4 Nov 2019]

16 Arm. *Bluetooth Low Energy/OS 2 BlE_HeartRate*, [2019]. [online] Available from: https://os.mbed.com/teams/Bluetooth-Low-Energy/code/BLE_HeartRate/ [Accessed 27 Nov 2019]

17 Alphr. *How to transfer files from pc to android phone using wifi*, [2 Oct 2018]. [online] Available from: https://www.alphr.com/computing/1000231/how-to-transfer-files-from-pc-to-android-phone-using-wi-fi-manage-your-media [Accessed 8 March 2019]

18 Karrar. *6 uses of Bluetooth other than wireless audio*, [1 May 2016]. [online] Available from: https://www.maketecheasier.com/uses-of-bluetooth/ [Accessed 26 March 2019]

19 Ais. *3 Ways in which smart door locks improve home security*, [19 March 2016]. [online] Available from: https://www.aishalcyon.org/3-ways-in-which-smart-door-locks-improve-home-security/ [Accessed 12 March 2019]

20 Avantree. *Avantree How to-connect Bluetooth headphones with Macbook (Audition Pro)*, [8 Sept 2016]. [online] Available from: https://www.youtube.com/watch?v=VJwMpcI_Rio [Accessed 20 March 2019]

21 Ian. *Bluetooth security basics*, [no date]. [online] Available from: https://www.electronics-notes.com/articles/connectivity/bluetooth/security.php [Accessed 28 March 2019]

22 Electronics note. *Bluetooth Security,* [no date]. [online] Available from: https://www.electronics-notes.com/articles/connectivity/bluetooth/security.php [Accessed 30 May 2019]

23 Curt. *How Bluetooth works*, [28 June 2000]. [online] Available from: https://electronics.howstuffworks.com/bluetooth4.htm [Accessed 28 March 2019]

24 RF wireless world. *Advantages of Bluetooth/Disadvantages of Bluetooth*, [2012]. [online] Available from: http://www.rfwireless-world.com/Terminology/Bluetooth-advantages-and-disadvantages.html [Accessed 2 April 2019]