IoT Readiness of BLE 5: Evaluation, Implementation and Improvements

HERGILS ÞÓRDARSON
KTH Royal Institute of Technology
School of Electrical Engineering and Computer Science

Degree project in Embedded Systems

IoT Readiness of BLE 5: Evaluation, Implementation and Improvements

Author: Hergils Pórdarson
Supervisor: Johanna Nordlóf, Tritech
Yuan Yao, KTH

Examiner: Prof. Zhonghai Lu, KTH
Abstract

The rapid enhancement of low-power short range wireless connectivity has been a driving factor of the pervasive adoption of Internet-of-Things (IoT). However, the lack of universal standard for such technologies causes compatibility issues and slows down innovation. The Bluetooth Low Energy (BLE) protocol has become the leading protocol that is most likely to be adopted as the standard over other compatible technologies and thus has to be studied thoroughly and all characteristics evaluated. Several major enhancements were introduced in the release of BLE 5 which makes the technology instantly more attractive in wider range of use cases than before. These enhancements bring additional complexity into the BLE architecture while allowing for more flexibility and configuration varieties to optimize each use case.

This thesis attempts to evaluate the benefits of new features in BLE for a specific device developed by Tritech Technologies and the possibility of utilizing several features to improve wireless performance. Additionally, the technology architecture is deeply studied, challenges in implementation identified and operational characteristics measured. Results of the literature review discusses how the scalability of BLE has significantly improved, new features provide more flexibility making the technology more attractive for all IoT and finally recommends further work in order to have a single standard when operating low-powered wireless communication. Moreover, test results of power consumption, possible range and throughput are summarized showing that the new features can bring significant benefits to certain products but massive drawbacks might occur in form of power consumed if not carefully implemented. To point out some notable test results acquired in this project, double the energy utility was achieved by utilizing high speed physical layer (PHY) in high throughput operation that reached data transfer rate of 1.37 MB/s. Using long range PHY with coding scheme of eight symbols per bit reached roughly 1 km range in Line-of-Sight (LoS) and improvement from about half-house to nearly full-house coverage. Furthermore, a method of dynamically switching PHYs was implemented and concluded not suitable for such an application due to high added power consumption.

**Keywords** — Bluetooth Low Energy, BLE 5, Internet of Things, Wireless Communication
Referat

Den snabba förbättringen av trådlös kommunikation med låg energiförbrukning har präglat utvecklingen av Internet-of-Things (IoT). Bristen på en universell standard för sådan teknik orsakar kompatibilitetsproblem och kan hämma innovation. Protokollet för Bluetooth Low Energy (BLE) har kommit att bli det ledande protokoll som förmodligen kommer att antas som standarden över andra kompatibla teknologier och måste därför granskas noggrant och alla dess egenskaper utvärderas. Flera anmärkningsvärda förbättringar introducerades i utgåvan av BLE 5 vilket omedelbart gör tekniken mer attraktiv i ett större användningsområde än tidigare. Dessa förbättringar ger ytterligare komplexitet i BLE-arkitekturen, samtidigt som detta möjliggör mer flexibilitet och konfigurationsvarianter för att optimera varje användningsfall.

Denna rapport försöker att utvärdera fördelarna med nya funktioner i BLE för en specifik produkt som utvecklats av Tritech Technologies och möjligheten att utnyttja flera funktioner för att förbättra den trådlösa anslutningen. Protokollarkitekturen är dessutom granskad, utmaningar i genomförandet identifierade och operativa egenskaper uppmätta. Resultaten från litteraturöversikten diskuterar hur skalbarheten hos BLE har förbättrats avsevärt, hur nya funktioner bidrar till flexibilitet vilket gör tekniken mer attraktiv för all typ av IoT och slutligen rekommenderar vidare arbete för att kunna uppnå en standard för trådlös kommunikation med låg energiförbrukning. Dessutom sammanfattas testresultatet av strömförbrukning, möjlig räckvidd och datahastighet, vilket visar att de nya funktionerna kan ge betydande fördelar för vissa produkter men att nackdelar kan förekomma i form av strömförbrukning om den inte är noggrant genomförd. BLE 5 jämfördes med tidigare versioner och resultaten från denna jämförelse visade på att fördubblad energy utility kunde uppnås genom att använda ett Physical Layer (PHY) med höghastighetsegenskaper och dataöverföringshastighet på 1.37 MB/s. Då ett PHY med lång räckvidd och datakodning på åtta symboler per bit användes kunde en räckvidd på cirka 1 km siktlinje uppnås och en förbättring kunde ses i en tvåplansvilla där täckningen ökade från cirka halva byggnaden till nästan hela byggnaden. Dessutom utvecklades en metod för att dynamiskt byta PHY under användning, och slutsatsen visade att denna metod ej är lämplig för den produkt som utreddes på grund av den ökade energiförbrukningen som då uppstod.

Nyckelord — Bluetooth Low Energy, BLE 5, Internet of Things, Trådlösa kommunikationer
Acknowledgment

I want to start by expressing my gratitude to my supervisor, Johanna Nordlöf, for providing me with guidance, helpful feedback and inspiration throughout the process. On the same note, I want to thank all colleagues at Tritech for a warm welcome from beginning, sharing ideas and resources, and in general making the project work fun and memorable.

I would like to thank Prof. Zhonghai Lu at KTH to take on the responsibility of examining this project and his helpful feedback.

Finally I want to thank my family, especially my girlfriend Högna, for their support and encouragement through my studies.

Stockholm, November 2018

Hergils Þórdarson
## Abbreviations

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>xvi</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>1.1.1</td>
<td>3</td>
</tr>
<tr>
<td>1.1.3</td>
<td>4</td>
</tr>
<tr>
<td>1.2</td>
<td>5</td>
</tr>
<tr>
<td>1.3</td>
<td>6</td>
</tr>
<tr>
<td>1.4</td>
<td>6</td>
</tr>
<tr>
<td>1.5</td>
<td>6</td>
</tr>
<tr>
<td>1.6</td>
<td>7</td>
</tr>
<tr>
<td>1.7</td>
<td>8</td>
</tr>
<tr>
<td>1.8</td>
<td>8</td>
</tr>
<tr>
<td>2</td>
<td>9</td>
</tr>
<tr>
<td>2.1</td>
<td>10</td>
</tr>
<tr>
<td>2.2</td>
<td>11</td>
</tr>
<tr>
<td>2.2.1</td>
<td>12</td>
</tr>
<tr>
<td>2.2.2</td>
<td>14</td>
</tr>
<tr>
<td>2.2.3</td>
<td>16</td>
</tr>
<tr>
<td>2.2.4</td>
<td>17</td>
</tr>
<tr>
<td>2.2.5</td>
<td>18</td>
</tr>
<tr>
<td>2.2.6</td>
<td>18</td>
</tr>
<tr>
<td>2.2.7</td>
<td>19</td>
</tr>
<tr>
<td>2.2.8</td>
<td>20</td>
</tr>
<tr>
<td>2.3</td>
<td>21</td>
</tr>
<tr>
<td>2.3.1</td>
<td>23</td>
</tr>
<tr>
<td>2.3.2</td>
<td>25</td>
</tr>
<tr>
<td>2.3.3</td>
<td>26</td>
</tr>
<tr>
<td>2.4</td>
<td>27</td>
</tr>
<tr>
<td>2.4.1</td>
<td>28</td>
</tr>
<tr>
<td>2.4.2</td>
<td>29</td>
</tr>
<tr>
<td>2.5</td>
<td>30</td>
</tr>
<tr>
<td>2.5.1</td>
<td>30</td>
</tr>
<tr>
<td>2.5.2</td>
<td>31</td>
</tr>
</tbody>
</table>
## Contents

2.5.3. Advertising Extension ............................................. 32  
2.6. Theoretical performance .................................................. 33  
2.6.1. Throughput .......................................................... 33  
2.6.2. Power Consumption ................................................... 35  
2.6.3. Covering Range ....................................................... 35  
2.7. Related Work ............................................................ 37  

3. Methods ................................................................. 39  
3.1. Research Methodology .................................................. 39  
3.1.1. Philosophical Assumptions .......................................... 40  
3.1.2. Research Method ..................................................... 40  
3.2. Preparation ............................................................. 41  
3.2.1. Hardware Description ............................................... 41  
3.2.2. Software Description ............................................... 43  
3.3. Measurements ........................................................... 44  
3.4. Data Analysis ........................................................... 46  

4. Implementation ......................................................... 47  
4.1. Product Background .................................................... 47  
4.2. Software Application ................................................... 48  
4.2.1. Central Device ....................................................... 48  
4.2.2. Peripheral Device .................................................... 49  
4.3. Evaluation Plan .......................................................... 51  
4.3.1. Power Measurements ................................................ 51  
4.3.2. Data Throughput Measurements ................................... 53  
4.3.3. Range Measurements ............................................... 53  
4.4. Competing technology .................................................. 55  
4.4.1. Zigbee ................................................................. 55  
4.4.2. Thread ................................................................. 57  
4.4.3. ANT/ANT+ ............................................................. 57  
4.4.4. Comparison Discussion ............................................. 58  

5. Results ................................................................. 61  
5.1. Power Consumption Results .......................................... 61  
5.2. Throughput Results .................................................... 65  
5.3. Range Results ........................................................... 66  

6. Summary and Conclusion .............................................. 69  
6.1. Implementation Challenges ............................................ 69  
6.2. IoT Readiness of BLE 5 ................................................... 70  
6.2.1. Scalability ............................................................. 71  
6.2.2. Low Power Characteristics ........................................ 71  
6.2.3. Range & Throughput ................................................ 72  
6.3. Conclusion .............................................................. 73
# List of Figures

<table>
<thead>
<tr>
<th>Figure</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.1</td>
<td>Typical range vs. throughput for various wireless technologies.</td>
<td>9</td>
</tr>
<tr>
<td>2.2</td>
<td>Bluetooth Core Specifications release highlights [11].</td>
<td>10</td>
</tr>
<tr>
<td>2.3</td>
<td>BLE protocol stack.</td>
<td>11</td>
</tr>
<tr>
<td>2.4</td>
<td>BLE channel division.</td>
<td>12</td>
</tr>
<tr>
<td>2.5</td>
<td>Link Layer state machine. Adopted from [14, Fig. 1.1]. * M and S denote master and slave respectively.</td>
<td>15</td>
</tr>
<tr>
<td>2.6</td>
<td>Link Layer bit stream processing on LE 1M and LE 2M. Adapted from [14, Fig. 3.1].</td>
<td>16</td>
</tr>
<tr>
<td>2.7</td>
<td>Link Layer bit stream processing on LE Coded. Adapted from [14, Fig. 3.2].</td>
<td>17</td>
</tr>
<tr>
<td>2.8</td>
<td>L2CAP structure.</td>
<td>16</td>
</tr>
<tr>
<td>2.9</td>
<td>Example of GATT Profile hierarchy.</td>
<td>20</td>
</tr>
<tr>
<td>2.10</td>
<td>Example of connectionless mode. Advertiser broadcasting short non-connectable packets containing useful data, while Scanner listens.</td>
<td>24</td>
</tr>
<tr>
<td>2.11</td>
<td>Example of simplified BLE connection establishment.</td>
<td>25</td>
</tr>
<tr>
<td>2.12</td>
<td>Five different BLE topology examples. Adapted from [13, Fig 4.2].</td>
<td>26</td>
</tr>
<tr>
<td>2.13</td>
<td>Packet format for LE Uncoded PHYs.</td>
<td>27</td>
</tr>
<tr>
<td>2.14</td>
<td>Packet format for LE Coded PHY.</td>
<td>28</td>
</tr>
<tr>
<td>2.15</td>
<td>Advertising channel PDU structure.</td>
<td>28</td>
</tr>
<tr>
<td>2.16</td>
<td>Data channel PDU structure.</td>
<td>29</td>
</tr>
<tr>
<td>2.17</td>
<td>Simplified data transfer mode using connections.</td>
<td>34</td>
</tr>
<tr>
<td>2.18</td>
<td>Relationship of path loss and distance.</td>
<td>36</td>
</tr>
<tr>
<td>3.1</td>
<td>Summary of research methods used in various parts of the project.</td>
<td>41</td>
</tr>
<tr>
<td>4.1</td>
<td>FSM describing basic Central Device functionality.</td>
<td>49</td>
</tr>
<tr>
<td>4.2</td>
<td>FSM describing basic Peripheral Device functionality. *Three advertising sets used when BLE 5 is utilized, one for each option of connecting(LE1M, LE Coded S=2, LE Coded S=8).</td>
<td>50</td>
</tr>
<tr>
<td>4.3</td>
<td>Jumper removal on Launchpad for clean BLE power measurements.</td>
<td>52</td>
</tr>
<tr>
<td>4.4</td>
<td>Test points indicated in test area.</td>
<td>54</td>
</tr>
<tr>
<td>5.1</td>
<td>Single connectable advertising event for each PHY able to advertise.</td>
<td>62</td>
</tr>
<tr>
<td>5.2</td>
<td>Single notification in a connection event for all PHYs.</td>
<td>63</td>
</tr>
<tr>
<td>5.3</td>
<td>Radio standby between connection events. A single VDDR recharge pulse can be seen scaled in time on the lower subplot.</td>
<td>64</td>
</tr>
</tbody>
</table>
### List of Figures

<table>
<thead>
<tr>
<th>Figure</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.4.</td>
<td>Difference between maximum data throughput of each PHY with and without data length extensions.</td>
</tr>
<tr>
<td>5.5.</td>
<td>House covering range of all PHYs compared.</td>
</tr>
<tr>
<td>5.6.</td>
<td>Map view of LOS measurements.</td>
</tr>
<tr>
<td>A.1.</td>
<td>Breakdown of advertising power profiles.</td>
</tr>
</tbody>
</table>
List of Tables

2.1. BLE PHY power classes based on output power........................................13
3.1. Power characteristics of CC2640R2F[40]...............................................43
3.2. RX Sensitivity of CC2640R2F.............................................................43
4.1. Comparison of wireless standards..........................................................59
5.1. Energy utility comparison of each PHY using different PDU size.............65
5.2. A summary of power consumption test results.......................................65
5.3. Data throughput of each PHY using different PDU size..........................65
5.4. Range test results, first column represents test points in the house, result set up as [A,B], where A answers if the connection was main-
tained at the test point and B answers if the connection could be initiated at the test point.................................................................66
Abbreviations

6LoWPAN .... IPv6 over Low Power Wireless Personal Area Network
AFH .......... Adaptive Frequency Hopping
ANT .......... Advanced and adaptive Network Technology
ATT .......... Attribute Protocol
BER .......... Bit Error Rate
BLE .......... Bluetooth Low Energy
BR ........... Basic Rate
BW ........... Bandwidth
CAD .......... Computer-Aided Design
CPU .......... Central Processing Unit
CRC .......... Cyclic Redundancy Check
CSMA/CA .... Carrier-Sense Multiple Access with Collision Avoidance
dB ............ Decibel
dBm .......... Decibel-milliwatts
DSSS .......... Direct Sequence Spread Spectrum
EDR .......... Enhanced Data Rate
FEC .......... Forward Error Correction
GAP .......... Generic Access Profile
GATT .......... Generic Attribute Profile
Gbps .......... Gigabit Per Second
GFSK .......... Gaussian Frequency Shift Keying
GPS .......... Global Positioning System
HCI .......... Host-Controller Interface
HVAC .......... Heating, Ventilation, and Air Conditioning
IEEE .......... Institute of Electrical and Electronics Engineers
IETF .......... Internet Engineering Task Force
IFS .......... Inter Frame Space
IIoT .......... Industrial Internet of Things
IoT .......... Internet of Things
IPv6 .......... Internet Protocol version 6
ISM .......... Industrial, Scientific and Medical
List of Tables

L2CAP ........ Logical Link Control and Adaptation Protocol
LL ............ Link Layer
LOS ........... Line Of Sight
LPD ........... Low Power Device
MAC ........... Multiple Access Control
Mbps .......... Megabit Per Second
MTU .......... Maximum Transmission Unit
OAD ........... Over-the-Air Download
OTA ........... Over The Air
PAN ........... Personal Area Network
PDU .......... Protocol Data Unit
PHY .......... Physical layer
PL ............ Path Loss
QoS .......... Quality of Service
RFID .......... Radio frequency identification
RTOS ......... Real-Time Operating System
RX ............ Receiver
SD ............ Secure Digital
SDU .......... Service Data Unit
SIG .......... Special Interest Group
SM ............ Security Manager
SNR .......... Signal to Noise Ratio
SoC .......... System on Chip
SRD .......... Short Range Device
sym/s .......... Symbol Per Second
TDMA .......... Time Division Multiple Access
TI ............ Texas Instruments
TX ............ Transmitter
UART ........ Universal Asynchronous Receiver-Transmitter
USB .......... Universal Serial Bus
WPAN .......... Wireless Personal Area Network
WSN .......... Wireless Sensor Network
Chapter 1.

Introduction

Bluetooth is a ubiquitous wireless technology invented by the Swedish telecommunication company Ericsson in 1994. Four years later, in 1998, the Bluetooth Special Interest Group (SIG) was established. Bluetooth SIG was formed by Ericsson, IBM, Intel, Nokia, and Toshiba, and the name Bluetooth was officially adopted. A year later the first specifications were released, Bluetooth 1.0 [1]. This technology was originally designed as a solution for short-range wireless point-to-point connectivity, such as wireless mouse/keyboard, small data exchange between devices and remote controllers. Significant improvements over the last decade has made the technology ubiquitous and nowadays Bluetooth connectivity can be seen in wide variety of applications.

This chapter introduces the background and research scope that will be addressed in this thesis report. A more thorough description of Bluetooth and BLE is carried out in Chapter 2. The specific focus, purpose, problem and goals will be discussed here along with limitations of this thesis. Finally this chapter will outline the structure and content of this report.

1.1. Background

Researches on systems that have the potential of connecting the physical world with the virtual world of the internet have been of big interest in both the academic society and industry the last two decades. In 1996 Xerox PARC started experiments involving this topic using RFID (Radio-Frequency Identification) tags with the vision of connecting objects, people, and things to the internet. This would eventually lead to a future where an internet search could reference a physical object in real time where it is possible to track its state and controlling functionality. Then in 1999 the phrase 'Internet of Things' (IoT) was emerging as a popular term to describe this concept [2].

The revolution of IoT is clearly visible in modern society as the number of connected devices is growing rapidly. Some key requirements concerning most of these devices
are low power, low cost, wireless connectivity, interoperability, and easy deployment. Thus there is a need for pushing wireless technology further every day in respect to those requirements. When Bluetooth SIG released the specification for Bluetooth 5, they stated that the new enhancements made on Bluetooth Low Energy (BLE) systems have the potential to revolutionize the IoT market. This makes BLE a likely candidate to overcome these challenges in IoT development.

Advancements made on the Bluetooth standard aim to make communication more efficient by achieving interconnectivity between any Bluetooth device regardless of brand or manufacturer while developing the technology to meet the growing demands of the IoT. Bluetooth has gained popularity and prosperity in the last 10 years especially for specific use cases concerning wireless audio streaming. Since the first release of the Bluetooth specifications, Bluetooth v1.0, significant enhancements have been seen in terms of increased throughput. Then in 2010, Bluetooth SIG released Bluetooth v4.0. This version of the specification had entirely different focus than the previous versions. This version addressed use cases that have the need for ultra-low power, while the previous version main focus was to increase the throughput of data transfer.

1.1.1. Bluetooth

Even though Bluetooth was invented more than 20 years ago it is still considered an evolving technology especially when the introduction of low energy features are considered. The focus of this thesis is specifically on Bluetooth Low Energy (BLE) and the new enhancement in the latest release of the specifications. In order to get a clear understanding of the technology, Bluetooth classic will be briefly explained.

Before diving deeper into Bluetooth discussion, it is important to note how different parts of the technology will be referred to in this report. The Bluetooth Core Specification defines two classifications of the technology and each version of the specification introduces changes and improvements for the communication protocol. These two classifications are as follows:

1. **Bluetooth Classic**, also known as Bluetooth BR/EDR (Basic Rate/Enhanced Data Rate), is the technology that ensured the prosperity of Bluetooth in wide range of applications. Improvements made on Bluetooth Classic are not considered relevant to this project, so the specific version will not be denoted when discussing Bluetooth Classic.

2. **Bluetooth Low Energy (BLE)** is the second classification of Bluetooth systems which adheres to v4.0 and higher versions of the Bluetooth specifications. These systems are simplified compared to Bluetooth Classic, and aim on lower cost and power consumption. The trade-off when using BLE systems can be seen in message capacity and maximum throughput, though devices intended
for this classification generally do not need high speed data transfer. The different versions of BLE will be denoted (‘BLE 5’ for the most recent version, and ‘BLE 4.x’ for earlier releases) whenever relevant.

It is worth noting that with the most recent Bluetooth specification, Bluetooth SIG has changed their brand guidelines to remove the use of ‘Bluetooth Smart’ brand used for earlier BLE devices. Additionally, they simplified the naming convention compared to former iteration of the standard, by using merely Bluetooth 5, unlike previous iterations that used .0 (followed by updated such as 4.1 and 4.2). From here on, the most recent specifications concerning Bluetooth Low Energy, will be referred to as BLE 5.

1. Introduction

1.1.2. Bluetooth Low Energy

Bluetooth Low Energy was first introduced in 2010 when the Bluetooth SIG released specification for version 4.0 [1]. This release addressed the market need for a ubiquitous solution for low-powered and short range devices. By using the same infrastructure as Bluetooth Classic in the design of BLE protocol stack, it has a significant advantage over other short range low power wireless technologies. This advantage can be seen in the form of wide spread, already existing applications that support Bluetooth, and is made cheap and simple to add BLE compatibility to currently Bluetooth Classic enabled devices. Furthermore, most centralized entities such as smartphones and laptops that were released after 2010 come with dual mode Bluetooth radio, supporting both Bluetooth Classic and BLE. This makes Bluetooth SIG able to fully exploit its ubiquity in BLE development as the compatibility is evident in most laptops and smartphones [5].

The latest Bluetooth specifications, version 5, were released in late December 2016. These core specifications claim to be able to transform the IoT market with new and improved features concerning BLE. The most mesmerizing upgrades can be seen in the form of double speed, 4x range and 8x data capacity, along with a mesh-based networking topology that was officially introduced several months later in mid-2017. Following is a brief summary of these enhancements and what the Bluetooth SIG claims to achieve with this new version [6], but a more thorough description of these features can be seen in Section 2.5.

- First of all, BLE 5 offers a new Physical Layer (PHY) variant with the ability to double the speed of transmission. This new PHY variant increases the bandwidth of data transfer from a maximum of 1 Mbps to 2 Mbps without the need to increase the power consumed. In fact, this new feature reduces the power consumption as the time for transmitting (TX) and receiving (RX) data has been reduced. This enhancement is really beneficial for solutions where speed of data transfer is a priority.
1. Introduction

- The **quadruple range** is achieved using another new PHY variant introduced in BLE 5, utilizing lower packet encoding of 125 kbps or 500 kbps. Then to further increase the range the TX power is increased to maximum of +20 dBm resulting in a potential of 4x range compared to BLE 4.x. This is especially beneficial for smart home systems, smart cities and networks with moving nodes.

- Another major benefit is **eightfold message capacity** of advertising messages. BLE works in the 2.4 GHz band and consists of 40 channels that have 2 MHz spacing. Three of those are used for advertising while the other 37 channels are allocated to genuine data transfer. The increased data capacity comes from advertising channel extension that makes it possible to increase the payload from 31 to 255 octets per transmission. This enhancement gives significant benefits to beacon development that only uses these advertising messages to broadcast data.

- Shortly after the release of the Bluetooth 5 specification followed the announcement of separate specifications on **Bluetooth mesh**, that has the potential of extending the Bluetooth ecosystem even further. As the name implies, this allows for using BLE (currently BLE 4.0) in a mesh based topology. This brings substantial benefits for many use cases. However, further description of Bluetooth Mesh is beyond the scope of this project as it does not utilize Bluetooth 5 and will thus not be described in more detail.

This project will focus especially on BLE 5, the enhancements that are briefly explained above, and how they create new opportunities in product development. These new features allow for a wide range of new application possibilities along with major improvement potential in most use cases. Moreover, BLE 5 and future versions could possibly fill a gap that ensures significant IoT evolution by efficiently linking smart phones with low-power sensors previously unsupported by other wireless standards.

1.1.3. Company Background

This project is carried out in collaboration with an embedded systems consultant company named Tritech Technology AB. Tritech offers consulting services to develop products all the way from idea phase to market launch. Their focus lies within the area of IoT systems, where wide competence in various parts of IoT development is desired. The company has to be able to offer expertise in various fields, knowing the state of the art, and being able to advise customers on significant design decisions. Therefore it is an interest within the company to gain competence on new exciting technology such as Bluetooth 5.
1. Introduction

1.2. Problem

The number of IoT devices in the world is increasing rapidly, and is predicted to exceed 20 billion devices by the end of 2020 (excluding smart phones, tablets, computers) according to predictions from Gartner [7]. This includes a significant range of applications that will increase congestion on the license free 2.4 GHz ISM (Industrial, Scientific and Medical) band. The communication protocols utilizing the ISM band need to coexist and preferably interoperate. This great increase in connected devices can also be considered problematic when considering power consumption. The vast majority of IoT devices run on small batteries and thus have very strict power requirements. Technology has advanced rapidly in the field of IoT and embedded systems during the recent decades, making higher demands on wireless connectivity, thus it has to be done efficiently, using ultra low power, to meet those demands. BLE 5 is coming up strong in that perspective and therefore its features and operation have to be studied thoroughly for the IoT readiness of the technology to be determined.

The introduction of several operating modes and PHY configurations in BLE 5 paves the way for new exciting use cases and improvement opportunities for BLE devices. Some promotions of BLE technology implies that it offers both longer range and increased throughput - but in fact, both features are not available simultaneously. This thesis focuses on investigating the possibility of making use of both the longer range and the higher throughput by dynamically adjusting the configuration of the connection. A product that is being developed by Tritech will be used as the potential use case for such an application and its functionality and requirements will be used as guidelines. Further description on this product and the actual implementation is introduced in Section 4.1.

Bluetooth 5 is relatively new on the market and requires both hardware and software updates in order to explore all new features that it introduces. Manufacturers can claim official Bluetooth 5 compatibility when fulfilling requirements set by the Bluetooth SIG. These requirements are presented in the Core Specifications [8] and state that support for only one of the three PHY variants, LE 1M, is mandatory and supporting the other two is optional. This can cause confusion and delays in product development where the aim is making use of these new features. Accordingly, a developer must ensure that the intended hardware supports the features that will be used, not only that it supports Bluetooth 5. Problems and issues mentioned above, along with the impact that BLE 5 can have on IoT development, will be addressed in this thesis during literature study and implementation, and backed up to some extent with measurement results.

The main research question defined for this project is the following:

- What benefits come from switching between PHYs dynamically by adjusting radio configuration parameters?
1. Introduction

1.3. Purpose

Bluetooth has become an important factor in wireless communication due to its simplicity, robustness and interoperability. Its omnipresence and low power capabilities makes BLE a true candidate to be a core component in the development of IoT. This makes it beneficial to conduct further research and push the technology towards further improvements.

The purpose of this project is to investigate how the new BLE enhancements could benefit a specific use case and propose improvements for BLE product development. Investigation of challenges that needs to overcome in order to have more optimized performance and to evaluate whether BLE 5 is in practice 'IoT Ready' along with speculations on how the technology compares to some of its competitors on the market today.

1.4. Goals

The main goal of this project is to identify challenges that may occur when utilizing new features of BLE and propose a method to improve robustness and reliability of BLE wireless connectivity. This will be done by presenting a specific use case following guidelines of a product developed by Tritech. This will aim on improving the efficiency and functionality of the product by utilizing more than one PHY during operation. The use case in mind is a hybrid smart watch designed for elderly people. This watch uses BLE 4.x to transmit an emergency signal to a smartphone when the user falls. More information about the product is found in Section 4.1. The hypothesis is that by introducing BLE 5 connection to this product, and utilizing more than one PHY, will make it possible to send important messages in a more robust and reliable way while spanning longer distance and further decrease power consumption during typical operation, without significant complications of the design. Furthermore, with both hands-on implementation and literature study the challenges and issues that may occur when updating a product from BLE 4.x to BLE 5 will be identified and analysed. Finally, the IoT readiness of BLE 5 will be concluded with results from literature study and implementation.

1.5. Method

A majority of the work in this project consists of both literature review and technology assessment. Bluetooth Low Energy will be thoroughly studied. Specific focus will be on understanding details of the most recent release of the specifications. Research within this topic and relevant related work will be studied. This information will be gathered through trusted sources such as Google Scholar, IEEE Xplore,
1. Introduction

ScienceDirect, Google Patents database, etc. This literature review is presented in Chapter 2.

The evaluation of the benefits that BLE could potentially bring to the development of IoT and how it compares to other competing technologies will be based on the empirical research method in addition to literature study. The empirical research methodology derives knowledge and information from experience and predictions while focusing on actual application and situations. It seeks to gain knowledge by getting proofs based on data from experiments, observations and experiences. Both quantitative and qualitative methods will be used to analyse and conclude this thesis project. More specific discussion on methods in direct context to this project are provided in Chapter 3.

The implementation will be built on top of knowledge acquired from the literature phase. Furthermore, testing qualifications provided in the Bluetooth specifications will be used to evaluate performance.

This is considered the most appropriate method for this project as it will consist of investigating and utilizing existing technology and knowledge to propose and implement the possibilities of new or improved use cases.

1.6. Sustainability and Ethics

The rapid development of technology, such as the IoT, automation and sensor networks, demands increased performance of wireless connectivity. Keeping that in mind it is important to strive towards the best or most suitable solution possible for each use case. The significant effort that has been put in decreasing power consumption of battery powered equipment can have drastic effects of power storage manufacturing. Thus it is of high importance to minimize power usage in general especially considering sustainability. A special focus is kept on energy expenditure in wireless communication throughout this thesis.

Ethical aspects of this thesis project is mostly aimed towards the presentation of knowledge. All information presented in this thesis that is derived from other sources shall be well cited and all credit given to original authors when applicable. All data and information concerning implementation and analysis shall be well documented in order for the results to be reproducible. Finally, all results and discussion shall be presented with full honesty and transparency in order to formulate an educated and correct conclusion.
1.7. Delimitations

This thesis project is carried out by one person and should include 20 weeks of work, equivalent of 30 credits. The limitations of this project have been specified, and this report does not cover the following:

- Delivery of any directly profitable product.
- Bluetooth Classic/Mesh research and development.
- Hardware manufacturing other than supporting circuitry for commercially available chipsets.
- Bluetooth software stack development.
- Experiments using other wireless protocol standards than Bluetooth.

1.8. Outline

This thesis report consists of six chapters. Each of these chapters addresses a specific part significant for this thesis work. This first chapter briefly introduces the subject and scope of this thesis. The second chapter introduces the technical aspects of BLE in more detail. The architecture is introduced where the functionality of each layer is described, potential and limitations of BLE discussed, other comparable technologies introduced and finally summarises the important characteristics of several popular radio modules supporting BLE 5. Following that is a description of the methodology used in this thesis discussed in chapter three. That discussion includes information about how the research was conducted, why the specific methods were chosen and how both implementation and evaluation is performed. The practical and technical information on implementation will then be described in chapter four. This is a thorough analysis of the chipset used for the implementation and what will be changed to improve the overall performance. Chapter five presents the tests conducted and their corresponding results. Finally, the last chapter concludes the thesis and presents discoveries made along the way, discusses the test results and suggests future works on this topic.
Chapter 2.

Theoretical Background

Wireless communication currently exists for many different use cases enabling developers to choose an optimal solution for a specific use case. These options typically differ in design goals, with some having data rates from a few Kbps (Kilobits per second) to several Gbps (Gigabits per second). Bluetooth Low Energy (BLE) focuses on low-cost and power consumption and therefore it is on the lower end of the data rate spectrum, and often referred to as WPAN (Wireless Personal Area Network) as seen in Figure 2.1, whereas Bluetooth Classic has considerably high data rate with all its enhancements since first introduced. Figure 2.1 additionally illustrates some widely known wireless technologies, as well as three other WPAN protocols with similar characteristics as BLE.

![Figure 2.1: Typical range vs. throughput for various wireless technologies.](image)

This chapter explains the brand name Bluetooth with special focus on BLE. The architecture and operation are explained in detail, theoretical performance is introduced, related literature are reviewed along with a brief introduction on competing technologies.
2. Theoretical Background

2.1. Bluetooth Fundamentals

Bluetooth is a global standard for wireless technology originally aiming to replace serial data cables that connects various devices. The design goals for the original Bluetooth were the following: worldwide operation, low cost, robust, short range, low power.

To achieve these goals, Bluetooth is implemented on the 2.4 GHz ISM (Industrial, Scientific and Medical) band that is license-free and can be adopted worldwide. However, there are a lot of downsides using the ISM band. This frequency band is heavily congested as several other widely used standards use it (e.g., IEEE 802.11, IEEE 802.15.4, etc.) along with the fact that it is really prone to noise from numerous devices such as street lights and microwave ovens. To compensate for these defects and enabling robust connection, Bluetooth Classic pioneered a mechanism called adaptive frequency hopping (AFH) \[10\] that is explained in more detail in section 2.2.

<table>
<thead>
<tr>
<th>Version</th>
<th>Release Date</th>
<th>Highlights</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0, 1.0a, 1.1, 1.2</td>
<td>Jul 1999-Nov 2003</td>
<td>1.0: Very first versions of Bluetooth. Aiming on replacing serial cable with wireless link. 1.0b: Minor updates and fixed some issues 1.1: Bluetooth ratified as IEEE 802.15.1 standard 1.2: AFH was introduced, eSCO links added to provide better voice quality</td>
</tr>
<tr>
<td>2.0, 2.1</td>
<td>Nov 2004, Jul 2007</td>
<td>2.0: EDR introduced to increase throughput (from 721 kbps to 2 Mbps). 2.1: Some minor updates and added SSP to simplify pairing mechanism and improve security.</td>
</tr>
<tr>
<td>3.0</td>
<td>Apr 2009</td>
<td>3.0: Significant increase in throughput by supporting multiple radio, referred to as AMP (throughput increased from 2.1 Mbps to 24 Mbps). Also included minor enhancements on some parts of the architecture. No major changes to Bluetooth Classic are made after this point.</td>
</tr>
<tr>
<td>4.0, 4.1, 4.2</td>
<td>Jun 2010 - Dec 2013</td>
<td>4.0: Market of low power devices addressed, and introduction of BLE. 4.1: BLE enhanced, devices allowed to act as both a hub and end point. Dual mode devices introduced and new topologies introduced to widen use case. Connected links added to increase reliability and security improved with private addresses.</td>
</tr>
<tr>
<td>5</td>
<td>Dec 2016</td>
<td>5: Marketing strategies changes as ‘Bluetooth Smart’ brand was abandoned and new version numbered as a single digit (e.g., 5 but not 5.0) Two new PHYs introduced aiming separately on higher throughput and longer range. Advertising extensions added to allow connectionless data transfer using larger packets.</td>
</tr>
</tbody>
</table>

Figure 2.2.: Bluetooth Core Specifications release highlights \[11\].

The Bluetooth standard has evolved and improved significantly since its first appearance in 1999. Figure 2.2 illustrates all releases of the Bluetooth Specifications and lists some notable changes in each version. It is worth noting that no major changes or improvements have been made to the Bluetooth Classic specifications since the release of Bluetooth 3.0 in 2009. It is also worth noting that the brand names 'Bluetooth Smart' and 'Bluetooth Smart Ready' have been abandoned. These brand names are now simply just branded as Bluetooth Low Energy. The Bluetooth Mesh specifications were released in July 2017, but are not included in Figure 2.2 as they
Bluetooth Low Energy (BLE) is a new and evolving technology originally introduced in June 2010. BLE is innovated from the prosperous Bluetooth Classic technology but addresses different design goals and market segments. One of the innovators involved in the development of BLE states that it is the lowest possible power wireless technology that can be designed and built [10].

The main focus of BLE are applications that only need to transfer small amounts of data upon request and typically run on strictly limited power. Therefore it can bridge the gap between smartphones and low-power sensors previously unsupported by wireless standards.

2.2. BLE Architecture

Bluetooth Low energy devices can be classified in two different types: dual-mode and single-mode devices. The dual-mode device consists of both support for Bluetooth Classic and BLE, therefore it can communicate with devices that support only one of these classifications or both. Single-mode devices consist of only BLE support and can therefore only communicate with other single-mode and dual-mode devices, but not with Bluetooth Classic-only devices.

Like Bluetooth Classic architecture, BLE is designed in a modular fashion. The protocol stack is based on three blocks, Application, Host and Controller, and has a layered architecture which is illustrated in Figure 2.3.

![BLE protocol stack](image-url)

*Figure 2.3.: BLE protocol stack.*
The Application block is only dependent on the use case of each Bluetooth device. The Host includes the so called upper layer functionality: Generic Access Profile (GAP), Generic Attribute Profile (GATT), Attribute Protocol (ATT), Security Manager and the Logical Link Control and Adaptation Protocol (L2CAP). Then the Controller includes the so called Physical Layer (PHY) and the Link Layer (LL) that is usually implemented on a small System-on-Chip (SoC). The communication between the Host and Controller is handled by the Host-Controller Interface (HCI) in a standardized manner that is pre-defined by the Bluetooth SIG. Finally on top of these blocks is the Application layer that represents the user interface [12].

2.2.1. Physical Layer

The Physical Layer (PHY) is the lowest layer of the protocol stack. It configures the physical parameters of the BLE radio, meaning that the PHY basically determines how a bit and its value is represented over the air.

Like Bluetooth Classic, BLE works on the 2.4 GHz ISM band. The frequency spectrum is divided into 40 channels in the case of BLE and 79 channels in Bluetooth classic. These 40 BLE channels are each 2 MHz wide. This is then further divided into three primary advertising channels and 37 Data channels (also called secondary advertising channels when advertising extension is used). Primary Advertising channels are used for device discovery, connection establishment and broadcast transmission while the data channels are used for bidirectional communication between connected devices, and when they are referred to as secondary advertising channels they are used for advertising extension. The channel structure of BLE is illustrated in Figure 2.4. As can be seen, the placement of the primary advertising channels is rather peculiar. This is done to minimize overlap with the commonly used standard IEEE 802.11.

![Figure 2.4: BLE channel division.](image)

To overcome interference on the congested ISM band Bluetooth uses a pseudo random frequency hopping paradigm called Adaptive Frequency Hopping (AFH). Frequency hopping is a well known method to transmit data on the radio spectrum while avoiding interference from other devices using the same channel. When data is
corrupted by noise or interference on a specific channel, then the retransmission is
done on another channel that is chosen in a pseudo-random manner with hopes on
hitting a channel with less noise and interference.

AFH is a variation of this method that improves immunity to interference and
decreases possibilities of causing disturbance to other devices using the same band.
The basic principle is that Bluetooth channels are classified into two categories, used
and unused. Thus the channels that have interference, causing data corruption, can
be marked as unused during connection. This results in fewer retransmissions and
therefore less energy usage and higher effective throughput. For all devices to know
which data channels to observe, a very simple algorithm is used. This algorithm
is based on a pseudo-random value defined by the master in the connection. Note that a channel map is built by the Link Layer to know which channels to be
used.

The modulation technique used in the physical BLE channels is called Gaussian Fre-
quency Shift Keying (GFSK) modulation. In this GFSK a binary one is represented
with a positive frequency deviation while a binary zero is represented with a negative
frequency deviation. Further details on modulation techniques are beyond the
scope of this project and are only provided here for reference.

There are certain transmission power level requirements that BLE devices must fulfil
according the Bluetooth Core Specifications. The maximum output power shall
not exceed +20 dBm while the minimum output power cannot be below -20 dBm.
Furthermore, BLE devices can be classified into power classes based on the highest
output power that the PHY can supply. These power classes are defined in Table
2.1. It is worth noting that the transmission power along with receiver sensitivity
are the most important features to reach maximum range in BLE communication.

<table>
<thead>
<tr>
<th>Power Class</th>
<th>Max Power $[P_{\text{max}}]$</th>
<th>Min Power $[P_{\text{min}}]$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>+20 dBm (100 mW)</td>
<td>+10 dBm (10 mW)</td>
</tr>
<tr>
<td>1.5</td>
<td>+10 dBm (10 mW)</td>
<td>-20 dBm (0.01 mW)</td>
</tr>
<tr>
<td>2</td>
<td>+4 dBm (2.5 mW)</td>
<td>-20 dBm (0.01 mW)</td>
</tr>
<tr>
<td>3</td>
<td>0 dBm (1 mW)</td>
<td>-20 dBm (0.01 mW)</td>
</tr>
</tbody>
</table>

All versions of BLE, prior to version 5, only used a single PHY for all communication.
That is the default LE 1M PHY. The Bluetooth Core Specifications v5 define two
additional PHYs that are available for the BLE radio. The possible PHYs to choose
from are the following:

- **LE 1M PHY** - Is the default PHY of BLE that was introduced in the first
version of BLE. LE 1M Provides raw data rate of 1 Msym/s using uncoded
modulation. This is the only mandatory PHY to include for BLE classification.
2. Theoretical Background

- **LE 2M PHY** - Introduced with Bluetooth 5. Provides data rate of 2 Msym/s using uncoded modulation while reaching 80% range of LE 1M using less time for TX and RX and thus using less energy. This is an optional PHY to support for BLE classification.

- **LE Coded PHY** - Also introduced with Bluetooth 5. Uses the core 1 Msym/s with two possible error correction coding schemes yielding to raw data rates of 500 kbps and 125 kbps gaining up to double and quadruple range respectively compared to the default LE1M PHY. This is an optional PHY to support for BLE classification.

By adding more options on the lowest layer gives BLE wider design space. It can be optimized further for a specific use case, or even use more than one of these PHYs in the same application dependent on operating conditions. The usage of these new features are described in more detail in Section 2.5.

### 2.2.2. Link Layer

The Link Layer (LL) is often said to be the single most complex part of the BLE architecture \[10\]. This layer defines the BLE state machine, state transitions, data and advertisement packet formats, and manages connections, packet timings and retransmission.

Figure 2.5 shows a simple state machine that describes the basic operation of the Link Layer. It is important to understand the basic concept of this LL state machine in order to continue to the packet structures and how they are used. So following is a brief description of each state and its functionality.

This state machine has five different states \[4\]:

1. **Standby State** - This is the default state of the link layer and can be entered from any other state. The LL remains in this state until the host layers have instructions to do otherwise. In this state there are no packets sent or received.

2. **Advertising State** - This state can only be entered from the Standby state. Here the LL transmits advertising packets but it may also listen for responds to advertising packets in this state. A Link Layer in this state is called 'Advertiser' and that term will be used from here on. This state is required for a device that wants to be discoverable or connectable. This state can either enter the standby state by stopping advertisement, or enter the connection state if an initiating device sends a connect request packet to the advertiser.

3. **Scanning state** - When a device enters the scanning state it listens for packets from an advertiser and may respond by requesting additional information. A Link Layer in this state is known as 'Scanner' and that term will be used from
2. Theoretical Background

![Link Layer state machine](image)

Figure 2.5.: Link Layer state machine. Adopted from [14, Fig. 1.1]; * M and S denotes master and slave respectively.

here on. This state can only be entered from the standby state when the LL decides to start scanning.

4. Initiating State - In this state the receiver is used to listen for packets from an advertiser requesting connection initiation. A Link Layer in this state is known as 'Initiator' and that term will be used from here on. If a connection request is received it moves into the connect state. Otherwise it will move back to the standby state.

5. Connection State - In this state a connection has been established. Two roles are defined in this state: Master and Slave. The device acts as a master if this state is entered from the initiating state, and acts as a slave if it is entered from the advertising state.

The link layer is usually implemented on the same chip as the PHY to avoid overloading the CPU that is responsible for the SW layers of the stack. This is due to computationally expensive operation that the Link Layer includes [15]. These operations are mainly to manage packet formats, such as Cyclic Redundancy Check (CRC) generation, preamble, access address and air protocol framing, data whitening, random number generation and Advanced Encryption Standard (AES).

It is safe to say that the Link Layer plays a big role in the protocol stack. Figure 2.6 and Figure 2.7 show an illustration of the sequence of steps that are carried out by the Link Layer when attempting to transmit data along with similar step sequence taken by the Link Layer on the receiving end. As mentioned in the previous section, there are three different PHYs available in BLE 5 (LE 1M, LE 2M, LE Coded) and the link layer uses additional steps when performing transmission with
LE Coded. These extra steps are denoted as FEC encoding/decoding and Pattern mapper/demapper in Figure 2.7.

The encryption/decryption stages are optional in BLE communication and are only done when the host requests encrypted message for increased security. Following that is the Cyclic Redundancy Check (CRC) which is a 24-bit checksum used to ensure bit error to enhance robustness. Then the whitening process is used to avoid long sequences of ones and zeros while transmitting and thus improving robustness of communication. Additionally in the LE Coded PHY two steps are added: FEC encoding/decoding and Pattern mapper/demapper. These steps are necessary to utilize the long range capabilities of LE Coded where the bits are modulated with modulation factor $S=2$ or $S=8$ as per the choice of the developer.

2.2.3. Host-Controller Interface

The role of the Host-Controller Interface (HCI) is simply to manage communication between the Controller and the Host. This includes providing a standardized communicational mechanism between the upper (host) and lower (controller) layers of the stack. Bluetooth specification define four transport layers that can be used as a physical interface between the host and controller: UART, three-Wire UART, USB or Secure Digital (SD). This standardized HCI brings several advantages. First the software development of the host and controller can be independent of each other. Another advantage is that a host and a controller can easily interoperate even though they are from different vendors. 

16
2.2.4. Logical Link Control and Adaptation Protocol (L2CAP)

The Logical Link Control and Adaptation Protocol (L2CAP) is a layer partly reused from the Bluetooth Classic protocol stack with some significant simplifications for BLE. It sits on top of the HCI and transfers data between the profiles that reside in the upper layers of the host. L2CAP is a protocol multiplexing layer that allows BLE to multiplex three different channels. The L2CAP is responsible for Quality of Service (QoS), routing, segmentation, fragmentation and reassembly of packets for higher level protocols (ATT, SM, etc.). Additionally, it includes segmentation and reassembly of packets that are larger than the radio can deliver and is used e.g. when transmitting IPv6 packets through BLE.

Figure 2.8 describes the architecture of the L2CAP. The Channel Manager is responsible for all internal signals, and signals for higher and lower layers of the architecture as well as providing the control plane functionality. The retransmission and flow control block provides flow control on each channel and error recovery using packet retransmission. The Resource Manager is responsible for providing a frame relay service to the Channel Manager and for coordinating the transmission and reception of packets related to multiple L2CAP channels over the facilities offered at the lower layer interface [16].

The Maximum Transmission Unit (MTU) is defined in the L2CAP layer. The MTU is an important parameter that is used to inform the other end of a connection link about the maximum size of the Service Data Unit (SDU) available. The minimum, and default, MTU for BLE is 23 octets. This means that all BLE devices must
2. Theoretical Background

support a packet size of at least 23 octets. In case that a transmitter sends a packet exceeding the predefined MTU of the receiver, the receiver responds with a special reject message.

2.2.5. Security Manager

The main purpose of the Security Manager (SM) is to encrypt and decrypt data packets and define procedures for pairing and authentication. Pairing is the process of attempting to trust another device by authenticating the other device. The SM also provides a security toolbox for generating hashes of data, generating confirmation values, and generating short-term keys used during pairing.

The pairing process used to establish secure connection with encrypted links is a three-phase process:

1. Pairing Feature Exchange.
3. Transport Specific Key Distribution.

Phase 1 and 2 are mandatory for pairing while phase 3 is optional [17]. Further details on SM and the types of encryption it provides is beyond the scope of this project and will not be described in more detail.

2.2.6. Attribute Protocol (ATT)

The Attribute Protocol (ATT) defines communication between devices using server-client architecture. In this relationship, the server exposes a set of attributes to the client and additionally it can notify or indicate the client about any changes in these attributes. The client can discover, read and write those attributes.

Firstly, an attribute is basically something that represents data, any data at any given time when a device is in any given state. In addition to containing the value of the data, an attribute has three properties associated with it: Attribute Type, Attribute Handle, Attribute Permission. The attribute type indicates what a particular attribute represents. This allows a client to know the purpose of that particular attribute. The attribute handle is used by the client in all operations with the server to identify the attribute. Finally an attribute permission determines the level of access that is permitted for that specific attribute. This is used by a server to determine whether a client has permission to read/write an attribute value.

The client or server role is determined by the GATT (further described in Section 2.2.7) and is independent of the master/slave role defined by the LL. The ATT is
designed to push or fetch attributes to/from a remote device. Additionally ATT also supports setting notifications and indications so that the remote devices can be alerted when that data changes.

The ATT defines six types of messages, where both client and server can initiate communication. These six types will not be described in detail, but are as follows:

1. Requests sent from client to server.
2. Responses sent from server to client in reply to a request.
3. Commands sent from the client to the server that have no response.
4. Notifications sent from the server to the client that have no confirmation.
5. Indications sent from the server to the client.
6. Confirmations sent from the client to the server in reply to an indication.

The service of the ATT is used by the GATT, which defines a hierarchy of services and characteristics using these attributes [10].

2.2.7. Generic Attribute Profile (GATT)

The Generic Attribute Profile (GATT) defines the types of attributes and how they are used. The GATT also defines how a device will discover, read, write, notify and indicate the characteristics. The GATT defines a hierarchy so that the attributes are grouped into primary and secondary services.

The main goal of the GATT is to establish and exchange profile information in a BLE link. These profiles are definitions of possible applications and specify general behaviour used during communication. Moreover, they define what type of data a BLE device is transmitting. This layer introduces the concepts of 'Services' and 'Characteristics' using the attributes as building blocks. An example of this GATT Profile data hierarchy can be seen in Figure 2.9. Immediately before connection, the GATT profile exposes its services and characteristics. They are defined in order to form a logical data structure.

A service is a collection of data and associated behaviours to accomplish a particular function or feature. A characteristic is a value used in a service and includes attributes used to communicate specific type of data.

As Figure 2.9 illustrates, a profile provides one or more services, a service provides one or more characteristics, and each characteristic includes its properties, value and optionally a descriptor that defines its functionality. A profile is composed of one or more services necessary to fulfil a use case [18].
To clarify the role of the GATT and ATT in the architecture, a simple analogy can be used. ATT defines a flat structure of attributes and relevant operations for those attributes. GATT then organizes those into profiles, services and characteristics. A profile could be thought of similar to a department in a large organization. These profiles are independent of each other. Each profile can provide one or more services. This could be considered to be services provided by each department of the large organization (payroll, training, etc.). Finally, each service could either contain sub-services or contain one or more characteristics. In this analogy, sub-services can be thought of as sub-departments where the characteristics would be the people who are providing the services [4].

To summarize, GATT groups similar attributes into structures which are easy to manage instead of large collection of attributes.

### 2.2.8. Generic Access Profile (GAP)

The main purpose of the Generic Access Profile (GAP) is to define the base definitions, recommendations and common requirements related to modes and access procedures that will be used by transport and application profiles during communication. Additionally the GAP describes how devices should behave in standby and connecting states in order to ensure that links and channels can always established between BLE devices.
There are four GAP roles defined for devices using BLE. A device may operate in multiple GAP roles at the same time if the LL supports that. The GAP roles are defined as follows:

- **Broadcaster** - A device that transmits non-connectable advertising events.
- **Observer** - A device that scans for advertising events from a broadcaster but cannot initiate a connection.
- **Peripheral** - A device that is an Advertiser, transmitting connectable advertising packets. Can accept the establishment of a BLE active physical link using any connection procedure. A device operating in the Peripheral role will be in the slave role when connected.
- **Central** - A scanner, that initiates the establishment of a BLE connection. A device operating as Central will be in the Master role when connected.

The GAP is the highest layer of the host, which directly interfaces with the application layer and thus the user. Requirements are therefore stated in the GAP about the generic terms that should be used on the user interface. These are useful when designing user interfaces, user manuals, documentations, and assists ensuring a uniform user experience independent of vendor, which is one of the main goals with Bluetooth.

Additionally, this layer provides privacy by the means of resolvable private addresses. This is intended for devices that are constantly advertising, but want to be private. Meaning that they will use a constantly changing random addresses while broadcasting. For the device to be discoverable, the GAP defines a resolvable private address, and how to connect to these private devices [10].

### 2.3. BLE Operation

BLE is often called a 'mostly off' technology, meaning that BLE devices typically send data only occasionally and stay in the standby state most of the time. This is the key to the ultra-low power consumption. However, BLE needs to establish connections really fast to compensate for this and remain robust. This is done by having three dedicated advertising channels that are used when initiating connection. This results in connection time less than 3 ms, or 20x faster than a Bluetooth Classic connection [4].

To fully understand the BLE operation and different connection modalities it is important to know the architecture well. BLE provides both connected mode of operation and connectionless mode. Before describing the different means of communication that BLE provides, several terms and parameters are introduced.
2. Theoretical Background

Advertising event is defined as advertising packet transmission on the advertising channels. At the start of each advertising event, the Advertiser sends an advertising packet. The corresponding Scanner receives this packet and depending on the type of advertising packet, it can send a request back to the Advertiser. The Advertiser then responds to that request within the same advertising event. There are two parameters that affect the time between two advertising events [14]:

- Advertising Interval (advInterval): an integer multiple of 0.625 ms in the range of 20 ms to 10485 s.
- Advertising Delay (advDelay): a random value that ranges from 0 to 10 ms after each advertising interval.

Thus the time between two consecutive advertising events (T_advEvent) is defined as the sum of advInterval and advDelay.

Connection event is a point of synchronization between a master and a slave. The start of a connection event is called an Anchor Point. At that point, the master transmits data channel PDU to the Slave. After that the master and slave send packets between each other during the connection event. The end of the connection event can either be upon request from the master or the slave. All packets within the same connection event are transmitted on the same physical channel. Channel hopping occurs at the start of each connection event. Similarly to the advertising event, the connection event has two parameters that affect the time between two connection events:

- Connection Event Interval (connInterval): the time between two successive anchor points. It is an integer multiple of 1.25 ms and in the range of 7.5 ms to 4.0 s.
- Slave Latency (connSlaveLatency): allows slave to use a reduced number of connection events. This parameter defines the number of consecutive connection events that the slave device is not required to listen for the master. This should be an integer in the

In addition to these, a parameter called Supervision Timeout (connSupervisionTimeout) is used by both devices in the link to detect lost connection. The Supervision Timeout is reset each time a packet is correctly received.

The advertising interval and connection interval are important parameters that impact the power consumption of a device significantly and have to be set properly. It is worth noting that these parameters are independent of each other. While advertising interval plays a role while establishing a connection and when operating in connectionless mode, connection interval plays a role during data transfer [4].
2. Theoretical Background

2.3.1. Connectionless Mode

The connectionless mode of BLE operation is often referred to as broadcasting or advertising. This is the most primitive way of transmitting data to more than one peer at the same time \[15\]. The limitations of this approach is lack of privacy so it is not suitable for sensitive data.

When operating in the connectionless mode, several types of advertising events are provided. These events are either connectable or non-connectable. Connectable events are used when establishing a connection, and is better described in next section. The non-connectable advertising events transfer data directly over primary advertising channels without establishing a connection. The new secondary advertising channels (data channels) can be used to broadcast larger data packets when the primary channels are not sufficient.

For certain advertising types (both legacy and extended), the Scanner can request additional information by responding to an advertising packet on the same primary advertising channel. This results in the Advertiser sending a scan response packet on the same advertising channel within the same advertising event.

When operating in the connectionless mode, there are two main classifications of advertisements:

1. **Legacy Advertisements** - Sends out advertisement packet, limited to 31 octets, on the primary advertising channels. This is the same advertisements as used in BLE 4.x, and can only use LE 1M PHY.

2. **Extended Advertisements** - Can be utilized for sending larger data packets than the legacy advertisements. Send out up to 255 octets large advertisement packets (also called auxiliary packets) on the secondary advertisement channels and can use any of the three PHYs (LE 1M, LE 2M, LE Coded).

In the case of non-connectable packets, data is included in the advertising packet sent over a primary advertising channel. This mode of communication consists of two types of participants, Advertiser and Scanner.

All advertising events begin on the primary channel. A typical legacy advertising event, with non-connectable packets, consists of the Advertiser bursting advertising packets to the all three primary advertising channels as shown in Figure \[2.10\]. The scanner listens to one of the channels each scan interval and then hops to the next channel with hopes of receiving data. The parameters shown in Figure \[2.10\] can all be modified to fit each application.

The data payload of each legacy advertisement is limited to 31 octets and the minimum time between non-connectable advertisement typically recommended to be 100 ms \[19\]. Therefore the maximum available throughput is limited to few kilo-bits.
2. Theoretical Background

Figure 2.10: Example of connectionless mode. Advertiser broadcasting short non-connectable packets containing useful data, while Scanner listens.

per second. To overcome this limitation and provide use cases that needed higher payload size, BLE 5 introduces extended advertising.

Extended advertising is a modified approach to the connectionless method with non-connectable advertising packets. To achieve this, secondary advertising channels are used for data transmission, but still without establishing a connection. Similarly to the legacy advertisement, the Advertiser sends short extended advertising packets in the three primary advertising channels. This extended advertisement packet includes a pointer to a secondary advertisement channel, chosen randomly from the 37 data channels, and the time offset for when data is transmitted on the secondary advertising channel. The Scanner shall then tune the receiver to that channel to receive data. The so called auxiliary advertisement packet is transmitted on the secondary channel when the advertising event ends according to a time offset.

Another valuable feature of the Extended Advertising is the so called Periodic Advertisements. This feature can be used to broadcast data at a defined period without establishing a connection. Periodic Advertisements is basically a clever way to implement Extended Advertisement. First, the Advertiser transmits a packet on a primary advertisement channel containing information such as time offset, PHY to use, and indication of where the next packet will be. Then the Advertiser sends another packet, on secondary advertisement channel, containing data needed to synchronize to the periodic advertisement packets that follow. This can be very useful, especially when attempting to stream data (e.g. voice or audio) through BLE. Although voice or audio streaming is not yet commercially available, the new LE 2M PHY might bring that benefit to certain applications.

Extended advertisement really expand the possibilities of connectionless BLE opera-
2. Theoretical Background

The payload size limit extends from the 31 octets up to 255 octet and the minimum time between advertisement events reduced to 20 ms [20].

2.3.2. Connected Mode

The connected mode is based on establishing a dedicated connection between devices to exchange data packets periodically. Figure 2.11 illustrates a simplified example of a connection establishment and packet transaction.

First, a peripheral device wants to establish a connection (Advertiser) by sending a connectable advertising packets to the advertising channels (see Figure 2.4 for channel map) periodically similarly to the connectionless mode, but with connectable packets. It is worth noting that this advertising procedure can be targeted, so that only specific device will respond to the advertising. The central device, at this point in time a Scanner, receives the advertisement packet and replies with a connection request packet (making it an Initiator) over the same channel. Once the connection is established, the peripheral device stops advertising and becomes the slave while the central device becomes the master. Now a bidirectional data transfer is possible between the devices. The data transfer is done on the same frequency channel during each connection event, but on each anchor point AFH occurs.

The Initiator (the master) is responsible for the first transmission and synchronization of connection and transmits the necessary configuration parameters. A connection is then terminated by either of the participants by acknowledging a termination command. A connection can also be terminated if a supervision timeout expires.
2. Theoretical Background

Figure 2.11 illustrates a data packet being sent after the connection has been established. A 31-octet data packet takes approximately 3 ms including connection establishment.

2.3.3. Topology

BLE network typically consists of a master and a slave, called a piconet. Each device can also play the role of both master and slave simultaneously in different piconets, thus forming a scatternet. In theory there can be infinite slaves connected to each master, but in practice this is not the case. The number of slaves connected to each master is typically specified by the vendor of a BLE module [21].

Figure 2.12 illustrates several examples of BLE network topologies: The first example, Figure 2.12 (A), shows one master device, A1, connected to slaves A2 and A3. Additionally, device A1 acts as the Initiator of a connection with device A4, which acts as an Advertiser transmitting connectible advertising packets. Figure 2.12 (B) illustrates a simple broadcasting topology, where device B1 acts as the Advertiser and devices B2 and B3 act as scanners. The scenario seen in Figure 2.12 (C) shows a simple point-to-point connection, a piconet with single master and slave connection. C1 is acting as the master and C2 as the slave. Figure 2.12 (D) shows two piconets forming a scatternet. Device D2 acts as a master connected to slave D1. Simultaneously, D1 acts as a master connected to slave D3. Finally Figure 2.12 (E) illustrates another scatternet. Here device E1 acts as a slave connected to two masters, E2 and E3. In addition to that, E1 acts as an Initiator starting a connection with Advertiser E4. When the connection has been established E1 acts as a master in that link.
Another network topology that was first introduced by the Bluetooth SIG in 2017 is Bluetooth Mesh. Bluetooth Mesh is built on top of BLE 4.0 LE 1M PHY and it can be implemented on any BLE 4.0 compliant radio by adding necessary software layers on top. However Bluetooth Mesh does not support any further improvements made in v4.x through v5 although it will likely introduce some of those improvements in later versions [22]. Bluetooth Mesh is a great addition to the Bluetooth ecosystem and is expected to revolutionize the IIoT (Industrial IoT) in the nearest future. A thorough description of all parts of Bluetooth Mesh are carried out by the Bluetooth SIG in [23].

2.4. Packet Format

Packets are fundamental building blocks of BLE communication. A packet is simply a labelled piece of data that is transferred from one device to another. The label on the data packet identifies the device that sent the data and optionally which devices should listen to it.

BLE uses a two types of basic packet structure. Common packet format is used for both uncoded PHYs (LE 1M and LE 2M). LE coded PHY uses a slightly modified packet format due to its error correction mechanism. All bit ordering used in BLE communication follows the Little Endian format [14].

<table>
<thead>
<tr>
<th>Preamble</th>
<th>Access Address</th>
<th>PDU</th>
<th>CRC</th>
</tr>
</thead>
<tbody>
<tr>
<td>1-2 octets</td>
<td>4 octets</td>
<td>2-257 octets</td>
<td>3 octets</td>
</tr>
</tbody>
</table>

Figure 2.13.: Packet format for LE Uncoded PHYs.

Figure 2.13 shows the packet format defined for LE Uncoded PHYs. This structure is used for both connectionless and connection mode communication. Each packet consists of four mandatory fields:

- **Preamble** - A fixed sequence of alternating 0 and 1 bits used by the receiver to perform frequency synchronization, symbol timing estimation, and Automatic Gain Control (AGC) training. The preamble is 8 bits when using LE 1M PHY and 16 bits when using the LE 2M PHY. The LSB of the preamble must be the same as the LSB of the Access Address.

- **Access Address (AA)** - Used as a correlation code by connected devices to prevent unrelated BLE devices using the same RF channel to be confused. The AA is a 32-bit value generated by the LL. Each AA shall be different for each LL connection between any two devices.
• **Protocol Data Unit (PDU)** - 2 to 257 octet long strictly dependent on type of communication. Divided into Advertising Channel PDU and Data Channel PDU, described further later in this section.

• **Cyclic Redundancy Check (CRC)** - A 24 bit checksum calculated over the PDU to check for bit-errors occurring during packet transmission.

The packet format defined for the LE Coded PHY can be seen in Figure 2.14 and is used for both advertising and data channel packets. The main difference between the two formats is that this one includes so called Forward Error Correction (FEC) blocks. FEC block 1 always uses \( S=8 \) coding scheme, and the Coding Indicator (CI) that is a 2 bit value indicating which coding scheme is used for FEC block 2. TERM1 and TERM2 are termination field that are 3 bit values and form a termination sequence used for the modulation. Remaining fields have the same functionality as the LE Uncoded format.

![Figure 2.14: Packet format for LE Coded PHY.](image)

### 2.4.1. Advertising Channel PDU

![Figure 2.15: Advertising channel PDU structure.](image)

The advertising channel Protocol Data Unit (PDU) has two main fields, header of two octets and a variable size payload. The PDU structure can be seen in Figure 2.15 where the 16-bit structure of the header is illustrated. It consists of the PDU type
simply defines the type of advertisement that the packet holds as there are several different types. The next bit of the header is Reserved for future use (RFU). Following that are Channel Selection (ChSel), Transmitter Address (TxAdd) and Receiver Address (RxAdd), which are all connected to a certain type of PDU and are not valid for all types of PDU. TxAdd and RxAdd are used to indicate whether the address contained in the payload is a public or a random address. The last eight bits of the header simply represent the length of the payload in octets.

The advertising payload field in Figure 2.15 can be up to 255 octet. This field always includes a 6 octet field for Advertiser device address (AdvA). The remainder of the payload varies between advertising types but is limited to 31 octets for traditional advertising (including active/passive scanning and initiation of connection). However the Advertising Extension utilizes the rest of the payload field, as it can contain up to 254 octets of data and uses the secondary advertisement channels (i.e. data channels) [14].

### 2.4.2. Data Channel PDU

![Data Channel PDU structure](image)

Similar to the Advertising channel PDU, the Data channel PDU also has a 16-bit field that represents the header further divided to five smaller fields as Figure 2.16 illustrates. Another addition in the Data Channel PDU is the Message Integrity Check (MIC) field that is an optional 4-octet field used to authenticate the PDU when a LL encryption is used.

The first field of the header is a 2 bit Logical Link Identifier (LLID) that determines the payload format contains data or control message. Next three header fields are the Next Expected Sequence Number (NESN), Sequence Number (SN), and More Data (MD), and they are all used for the LL flow control scheme where more than one consecutive data packet has to be sent. The SN bit is used to identify packets sent by the LL and the NESN bit is used by the peer either to acknowledge the last PDU sent, or to request retransmission. MD bit simply identifies if there is...
2. Theoretical Background

more data available. Finally the length field is an indication of the payload in octets [14].

Both data and advertising channel PDUs can have slightly more overhead than illustrated in Figures 2.16 and 2.15 due to operational dependent messages for higher level layers (L2CAP header, ATT header, etc.). This additional overhead typically occupy several octets at the LSB end of the payload.

2.5. BLE 5 Major Enhancements

The most recent version of the Bluetooth core specifications include several upgrades aiming to have significant performance improvements and introduce new features. The most mesmerizing enhancements seen in BLE 5 are two new PHYs, LE 2M and LE Coded. The former offering greater speed of transmission and the latter enabling longer covering range. It is worth noting that these new PHYs cannot be used simultaneously to achieve greater speed and longer range. Additionally a feature has been added that especially improves the connectionless operation mode, allowing advertising messages to include up to 255 bytes of data. These enhancements are thoroughly described in this section and example use cases that clearly benefit from each enhancement are introduced showing how it can be beneficial for various IoT applications.

2.5.1. Increased Speed

BLE 5 includes a new radio PHY, LE 2M, capable of transmitting data at twice the speed compared to prior versions (BLE 4.x). While the LE 1M PHY is able to transmit data at 1 Msym/s, the new LE 2M PHY transmits data at 2 Msym/s. As LE 1M and LE 2M PHYs signals are not modulated, a single symbol translates to a single bit (thus 1 sym/s = 1 bps). It is worth noting that these data rates represent the on-air data rate, meaning that it does not consider packet overheads, connection interval or IFS (Inter-Frame Space). The maximum effective throughput for LE 2M PHY can theoretically reach up to 1.4 Mbps, or roughly 1.7x higher than LE 1M, which can reach up to 800 kbps. This increased speed also means that the radio will need to operate for less time, providing another significant benefit of reduced power consumption. This difference in power consumption is measured in [24] and reported to be about 15% when transmitting the shortest packets possible. Therefore by using a maximum length BLE packet, the corresponding power savings could yield up to 40-50%.

Although the speed of 1 Msym/s is sufficient for most applications that utilize BLE, it can be desirable to use the new LE 2M. For instance, a wearable fitness tracker does not require high data rate, but benefits largely from the reduced power
consumption and thus requires less frequent charging. Another benefit for the same fitness tracker can be seen in the form of faster software updates resulting in improved user experience.

This feature requires a hardware update on the Controller part of a BLE module. Thus a considerable delay can be assumed until most devices can support this mode of operation.

2.5.2. Increased Range

The option of having increased range also introduces a new optional PHY called LE Coded. The Bluetooth SIG claims that this feature will be able to achieve quadruple the range of prior versions. To put that in context, the range of BLE 4.x has been reported to be around 50-100 m outdoors and unobstructed, while in a typical indoor environment it reduces to 10-20m [25]. This means that BLE 5 using LE Coded should in the worst case achieve up to 200 m outdoors and 40 m indoors.

To achieve this, LE Coded uses a raw data rate of 1 Msym/s like the LE 1M, on top of that is a lower packet encoding scheme. This coding scheme may use either of two spreading factors: $S=2$ or $S=8$. The spreading factor defines how many symbols are used to represent one bit, meaning that the data rates result in 500 Kbps for $S=2$ and 125 Kbps for $S=8$. By spreading several symbols over an increased tolerance for a weak Signal-to-Noise Ratio (SNR) is achieved. This coding scheme is mainly performed in hardware in the Controller part of the architecture, and therefore BLE modules need hardware updates to support this feature. The coding process is divided into two steps, that are illustrated in Figure 2.7 and includes Forward Error Correction (FEC) encoding/decoding followed by Pattern mapping/demapping. These steps provide improved receiver sensitivity seen in greater ability to fix errors in the received data without requiring retransmission.

BLE 5 offers a possibility to increase the available range even further by raising the bar of maximum transmission power from $+10$ dBm to $+20$ dBm. This is of course a drawback when aiming for ultra-low power, especially in terms of LE Coded as it requires far longer operation time of the radio for the same data size than LE 1M or LE 2M. However, this could be preferred for certain applications that do not have strict power requirements but still need BLE connectivity, e.g. mains powered devices in smart homes.

It is worth noting that this mode of operation is not suitable for applications requiring streaming data or transmitting large datasets. However, this operating mode aims at IoT applications where e.g. low-cost modules are placed through a building or open spaces to gather data (such as humidity, light, temperature, motion detection, etc.). In such a use case, it would be possible to reduce number of devices covering the same area drastically by upgrading from BLE 4.x to BLE 5.
Another application could be a wearable device. Consider a wearable bracelet/watch designed for elderly people, that transmits an emergency message to a smart phone when the user falls down. This situation might happen when the range between the wearable and smart phone is too large for the LE 1M. As the signal is critical, great benefits can be seen by transmitting messages over longer distances as the transmission speed or packet size is not of great concern.

To evaluate the maximum range of a given technology is a cumbersome task as there are many unpredictable parameters that can affect the results. In order to get a feeling of the range at this point, test results have reported up to 1.6 km range using 125 Kbps data rate \[26\]. Some of the parameters affecting the achievable range and how the maximum range is evaluated is described in detail in Section 2.6.

### 2.5.3. Advertising Extension

Another notable improvement seen with BLE 5 is the ability to extend broadcasting capacity when operating in the connectionless mode (advertising). As described in Section 2.3.1, broadcasting does not require a connection between devices. Messages are simply transmitted by an Advertiser and one or multiple scanners within range can pick up the messages. Advertising Extension provides devices ability to broadcast roughly 8x larger packets compared to prior versions. With BLE 4.x, it is possible to broadcast messages up to 31 octets, while BLE 5 offers message size up 255 octets. This enhancement is not backwards compatible with the Legacy Advertisements that is the only supported broadcasting mode in prior versions of the technology.

To summarize the advertisement extension process, first the Advertiser transmits an packet (\(\leq 31\) octets) containing device address and configuration parameters to notify Scanners about configurations to access the extended advertisement data. Next, data packets up to 255 octets can be transmitted on the secondary advertisement channels (data channels) for Scanners to receive without establishing a connection. Refer to Section 2.3.1 for details of the Advertising Extension process.

To ensure that devices which do not support this feature are not confused, the advertisement packet transmitted on the primary advertisement channel provides a header value informing these older devices to discard them. This feature can be supported without modifications of the radio hardware, it only requires chipset manufacturers to provide an updated software stack.

Advertising Extensions can have significant benefits in BLE beacon development. The common usage of beacons has increased rapidly since BLE was introduced. According to predictions, annual shipment of beacons is expected to surpass 565 million by 2021 where almost all are expected to use BLE 5 and future versions \[27\].
The message size of 31 bytes puts very strict limit on beacon broadcasting. To put this further in context, consider a use case where a beacon is broadcasting a URL for devices within range. Average size of URLs tend to be higher than 31 bytes \cite{28} forcing developers to find a way around this. This issue is resolved in BLE 5, enabling more substantial data to be transmitted in connectionless operation.

This improvement will also have meaningful benefits for the variety of beacon use cases. Beacons combined with proximity devices could automatically send all devices within a specific range localized information. This information can range from being restaurant menus, traffic data, special offers, promotions, etc. Furthermore, as this option only requires software update, it has a great advantage as the market delay is decreased as most existing smart devices can support this feature after a software stack update.

### 2.6. Theoretical performance

As the theoretical framework of BLE has been introduced, it is ideal to discuss how its performance can be evaluated. The performance of a Bluetooth device does not only depend on the version of Bluetooth it supports but is strictly dependent on how it is operated and the hardware design itself. Thus many performance parameters are different between chip vendors and of course operation scheme. The theoretical performance of BLE 5, in terms of throughput, power consumption evaluation and covering range will be introduced in this section.

#### 2.6.1. Throughput

The achievable throughput is an important benchmark of each wireless technology. In the case of BLE, there are several factors that determine the actual data throughput that can be expected from an application. However, this may not resemble real life environment as if any device in a connection, master or slave, receives two consecutive packets where CRC check cannot be validated, the connection event ends. Meaning that the data will not be retransmitted until the next connection event using another data channel. This scheme might decrease the effective throughput in areas with much interference, depending on connection interval, but at the same time it prevents waste of energy when a certain channel introduces high bit error rate. This is one of many details that has been implemented to minimize the power consumption of BLE communication.

First of all, there are three different PHYs available in BLE 5, and four possible air data rates that affect the throughput drastically. These are LE 2M at 2 Mbps, LE 1M at 1 Mbps, and LE Coded at 500 kbps (S=2) or 125 kbps (S=8). However, it is impossible to reach these data rates as this is the rate of which the symbols are sent
2. Theoretical Background

and there are several factors that delay the data transfer. The radio is limited to a number of packets per connection interval, Inter Frame Space (IFS) delay between packet is a constant of 150 $\mu$s, and packet overhead in the form of headers and configuration parameters is evident meaning that not all octets in a packet are usable data.

To calculate the maximum data throughput with each PHY, consider a connected operation mode where largest possible data packet is being sent (255 octets). Figure 2.17 illustrates one complete transmission period between connected devices, where the slave sends a data packet in response to a poll from the master (packet containing no data). Between all packets there is a constant IFS specified by the Bluetooth SIG. To calculate the data throughput, the usable 255 octets of data are simply divided by a single transmission period.

![Figure 2.17: Simplified data transfer mode using connections.](image)

When operating on LE 2M, transmitting at 2 Mbps, the first packet contains 11 octet (as seen in Figure 2.13) and takes 44 $\mu$s. Then the data packet contains 255 octets of usable data and 11 octet of overhead, and takes 1064 $\mu$s to be transmitted. With that said, the application data throughput can be calculated as: $T_{2M} = 1.45$ Mbps.

Then when set to LE 1M, the first packet contains only 10 octets, as the preamble is shorter, and takes 80 $\mu$s to transmit. The data packet is 255 octets of usable data and 10 octets of overhead, taking 2120 $\mu$s to transmit. So the maximum application data throughput for LE1M is calculated to be $T_{1M} = 816$ kbps.

The packet format for LE Coded is slightly different, refer to Figure 2.14. Here the same amount of data is sent, 255 octets. But the empty packet sent first is considerably larger, or 20 octets and takes 462 $\mu$s and 720 $\mu$s for coding S=2 and S=8 respectively. The IFS stays the same, but the data packets will take much longer to transmit. For S=2 it is 4541 $\mu$s and for S=8 it takes 17040 $\mu$s to transmit the 255 octets of data. This leads to application data throughputs of $T_{S2} = 384$ kbps and $T_{S8} = 115$ kbps.

This model does not consider parameters that can have significant effects on the throughput such as connection interval, slave latency, maximum packets per connection interval, device limitations or BER (Bit Error Rate), and RAM available to buffer the data. Another notable approach to model the throughput in a BLE link is
carried out in [29], where an older version of BLE is investigated and effects of BER is considered.

2.6.2. Power Consumption

As the name implies, the main goal of BLE is to establish wireless connection by using as low power as possible. It is nearly impossible to state average power consumption for a low power wireless standards, since it is really dependent on several hardware and software characteristics such as operating mode, hardware design, power class, etc. To evaluate the power consumption of BLE, a specific hardware module and operating mode have to be considered. Then it is necessary to evaluate the average current draws during the active phase of operation, as well as the peak current as that can affect battery operated devices significantly. For the rest of the operation, during standby mode, the power consumption is nearly constant around 1 µA using 3V reference voltage [2].

To get better perspective of the energy utility of BLE, and how significantly that can vary on test condition and hardware used, some notable results and analysis from other studies is reviewed. In both [30] and [31], detailed power analysis is done on both BLE and 802.15.4 based protocol. The former study is using BLE 4.0 and the latter BLE 4.2. It is reported in [30] that for a connected mode of operation using CC2540 SoC from Texas Instruments, the energy utility roughly exceeds 500 KB/J (Kilobyte/Joule) using optimal connection interval, packet size and slave latency. In comparison they report that the energy utility for Wi-Fi can reach up to 240 KB/J and for Zigbee they measure it to be limited to 300 KB/J. In [31], an identical SoC is used for both BLE and 802.15.4 measurements (CC2650 from TI). It reports that the energy utility using BLE in connection mode, sending packets of 39Bytes at output power of +2 dBm, results in 2.1 MB/J while the same setup using 802.15.4 results in 780 KB/J. It is evident that the result vary quite a lot between studies, but it is safe to say that BLE provides promising results in terms of power consumption.

2.6.3. Covering Range

As with most performance characteristics, the covering range is highly dependent on operating environment. Real usage scenarios include reflections, obstructions and RF interference that adds up and determines if a link can be established.

A common term to represent the achievable range of radio communications is Link Budget. It describes the ratio of the transmit power and the sensitivity level as seen in [2.1]. The link budget defines how much path loss is acceptable for the transmission
2. Theoretical Background

to be successful. The correlation between covered distance and path loss can be described with equation 2.2 [10].

\[
\text{Link budget} = \frac{TX \text{ output power}}{RX \text{ Sensitivity level}}
\]

\[\text{path loss} = 40 + 20 \log(d)\]  \hspace{1cm} (2.1)

Where \(d\) represents the distance between the transmitting and receiving antennas. Figure 2.18 illustrates the relationship of the path loss and the distance. It is worth noting that this is an optimistic estimation that is only applicable with isotropic antennas and does not consider losses in the Tx/Rx systems.

\[\begin{aligned}
\text{Distance}[\text{m}] & \quad \text{Path Loss [dB]} \\
0 & \quad 40 \\
100 & \quad 50 \\
200 & \quad 60 \\
300 & \quad 70 \\
400 & \quad 80 \\
500 & \quad 90
\end{aligned}\]

\[\begin{aligned}
\text{Distance}[\text{m}] & \quad \text{Path Loss [dB]} \\
0 & \quad 40 \\
100 & \quad 50 \\
200 & \quad 60 \\
300 & \quad 70 \\
400 & \quad 80 \\
500 & \quad 90
\end{aligned}\]

Figure 2.18.: Relationship of path loss and distance.

To be able to calculate the possible range, the sensitivity and output power need to be known. The Bluetooth SIG specifies that a receiver sensitivity must be better or equal to -70 dBm (lower is better). As stated in Table 2.1, the maximum output power is +20 dBm. For example, using these numbers for the output power and sensitivity level, the link budget can be calculated as +90dB. This leads to a range of 100 m.

Another interesting feature that is possible in BLE communication is to evaluate the distance between connected devices. This is done by the means of Received Signal Strength Indicator (RSSI). Numerous studies have tried to model the relationship of RSSI and distance between nodes, [32] proposes a model that approximates the
distance directly from the RSSI and is described in equation \(2.3\), where \(N\) is a constant assumed to be one, \(d\) is the distance in meters and \(a\) is the RSSI at one meter distance.

\[
RSSI = -10 \cdot N \cdot \log(d) + a
\]  

(2.3)

Such estimations can be especially beneficial for use cases such as positioning systems and keyless entry systems. This approach can be used for approximating the distance between devices and dynamically change PHY configuration of BLE connection and thus avoid link termination.

### 2.7. Related Work

Numerous studies have been carried out to evaluate and improve BLE. These previous work includes case studies to evaluate the technology, surveys to compare technologies and RF electronics design considerations. Some literature that is reviewed throughout this project will be summarized in this section.

It has become a difficult task to evaluate the effects of a specific wireless technology in the field of IoT and WSN (Wireless Sensor Network). Following the release of BLE 4.2, [2] studied if BLE would be able to efficiently link smartphones and low-power sensors, filling the gap between wireless standards and low power consumption. Want et al. emphasized that the supporting ecosystem of a given technology must be mature enough for its value to be really significant. They concluded that BLE might need few years of development to be considered the solution to enable pervasive adoption of IoT and WSN, while still having high potential.

A notable study that focuses on BLE devices deployed in a dense IoT environment is presented in [33]. An investigation is done on the scalability of BLE where many devices are operating in a small area and this results in high collision rates and thus wasted energy. Furthermore, this paper reports that BLE certainly has a potential to revolutionize IoT technology, but the blind use of it in a densely deployed environment will hinder any realization of this vision. For BLE to widen the adoption of IoT, some effort has to be put into routing in dense networks. They propose a method called Opportunistic Listening, that extends the ability of scanning response for a specific scenario. The results show that this approach outperforms active scanning in the environments tested.

Another notable research on integrated SoC for BLE can be found in [34] where ultra low power consumption and high performance is of main interest. This design employs a sliding-IF architecture to achieve both low power consumption and high performance. They state that this SoC achieves the lowest current consumption, for both RX and TX, of all published product-level SoCs using 65 nm CMOS process supporting BLE 4.2 and prior versions.
2. Theoretical Background

Many other studies have been carried out regarding specific parts of the BLE technology with the aims of identify new challenges and opportunities and expand the BLE ecosystem further. One of which has been done by the Internet Engineering Task Force (IETF) in [35] where techniques on how IPv6 can be transported over BLE networks are introduced. This can benefit BLE enabled products significantly as it opens up the possibility of communicating directly to the internet where each BLE device could have its own IP address removing the reliance on smartphones. Furthermore, IPv6 over BLE was utilized in [36] to adjust communication performance at run-time using a custom designed open source BLE stack. This introduces an IPv6 over BLE stack that adds tuning knobs to control energy usage and timeliness of BLE devices that can ensure several QoS metrics. Additionally, Spörk et al. state that they have developed the first open-source stack enabling full support for IPv6 over BLE while providing performance optimizations during runtime.

Other studies worth noting is firstly an interesting approach aiming on maximizing the lifetime of a BLE network that is arranged as a large-scale capillary network [37]. This study focuses on establishing mesh networks using the heterogeneous characteristics of BLE devices. Results of the custom built routing algorithm that considers a metric defined as Role Suitability Metric (RSM) results in 20-40% improved network lifetime according to simulations. Secondly, there are several interesting papers evaluating effectiveness of BLE and how it compares to other technologies. Some of those results are presented in Chapter 4, Section 4.4, where similar competing technologies are analyzed.

Most of the studies referenced here have been carried out where the host block of the BLE architecture is of main interest, while the controller block, LL and PHY, is treated as a black box. The forthcoming of BLE 5 brings new opportunities of BLE studies, as new features offer increased configuration possibilities of the physical radio parameters. Additionally this makes room for new use cases and improved performance that needs to be studied and evaluated thoroughly.
Chapter 3.

Methods

The purpose of this chapter is to provide information on how this study was conducted, to give rationale for the methods chosen and to introduce the implementation done to acquire the desired results. This will begin on general assumption early in the process and describe the research methods used. Next there is a discussion on tools and resources used for the practical implementation and finally a description about measurements and data collection.

3.1. Research Methodology

Research methods and methodologies can be described as processes and approach to assure the quality of results in a research project. A significant part of every research is the decision of what methodology is used to reach the desired conclusion. The methods used are essential to plan and conduct the work needed to achieve proper well-founded results.

In the literature review in Chapter 2, several technologies with similar purpose as BLE were introduced. To evaluate how BLE compares to its prior versions and other wireless technologies intended for the competing world of IoT, both quantitative and qualitative methods are used. Both approaches are needed as some aspects of wireless connectivity can be clearly represented with quantities, such as throughput, range, latency and power requirements. Furthermore, the benefits of upgrading a specific product from BLE 4.x to BLE 5 can be represented quantitatively. When utilizing the additional PHYs introduced in BLE 5 for a given application there are some essential characteristics that have to be quantified. Thus quantitative research methodology is well suited to report results concerning these aspects.

However, to determine if BLE 5 is in fact ‘IoT Ready’ is not as simply described using numerical values and measurement results. Several aspects have to be considered, that would make a technology ready to overcome challenges in IoT, and motivation of why the technology has the potential of spreading through the wide varieties of applications seen in IoT. Moreover, both comparison with other technologies and
migration issues have to be supported with qualitative methods. As the numerous technologies intended for the IoT have different design goals and optimal use cases, the quantitative results do not tell the whole story. It is important to consider scalability, availability, interoperability, etc. with qualitative approach to get a better understanding of the state of the technology. Additionally, when migrating a specific application from BLE 4.x to BLE 5 it is important to identify challenges and qualitatively address when, why and if there is clear benefit in upgrading a product to use BLE 5.

3.1.1. Philosophical Assumptions

There are several core philosophical assumptions in research methodology that are described in [9], and they are: Positivism, Realism, Interpretivism, and Criticalism. This project explores two of these assumptions, Positivism and Interpretivism, for different parts of the project.

Positivism assumes that the reality is objectively given and independent of the observer and instruments. Here a conclusion is drawn from quantifying measures of variables to test hypotheses [9]. The Positivism assumption is a recommended approach for testing performances as done in a part of this project where performance of BLE 5 is evaluated in contrast to BLE 4.x in the same application.

Interpretivism is used to understand phenomena by exploring richness, depth and complexity in an inductive manner. This approach will be used to evaluate the position of BLE 5 towards the IoT. This concept is also relevant when using new features of BLE. The improvements stated by the Bluetooth SIG are interpreted with perspective of an application that has strict power requirements but would benefit from both higher throughput and increased range.

3.1.2. Research Method

Choosing a comprehensive research method is important in order to work efficiently, accomplish the goals and to eventually get a well-founded result. This project is primarily based on two research methods: Empirical Research method and Experimental Research method. The former one is defined to rely on knowledge from actual experience and observations. It forms a body of knowledge by involving collection and analysis of data to characterize performance and in this case to evaluate how BLE 5 compares to other wireless technologies in terms of power, range, speed, throughput etc. Furthermore, to evaluate if the technology is ready to overcome challenges regarding IoT compatibility, the Empirical method is well suited as the literature review forms a body of knowledge from previously conducted studies to support deep discussion on the matter. The latter method, Experimental Research, studies causes and effects in general. In its definition it can manipulate one variable
and keep the other variables constant to observe how changes affect results. This methodology is used to see effects of dynamic change of connection parameters during BLE 5 operation in specific situations.

To summarize, both quantitative and qualitative methods are used to reach the desired results. This includes the philosophical assumptions of Positivism and Interpretivism while using both Experimental and Empirical research methods. The different methods are applied on different parts of the projects, and is summarized in Figure 3.1.

![Figure 3.1: Summary of research methods used in various parts of the project.](image)

### 3.2. Preparation

Prior the actual implementation, several aspects had to be considered. First off, the BLE protocol had to be deeply studied and along with writing Chapter 2 the required knowledge was acquired to take decisions regarding hardware platform and appropriate software. Additionally, limitations and requirements had to be determined, and finally hardware platform and software application had to be decided and outlined.

#### 3.2.1. Hardware Description

The decision of hardware usage is critical to most embedded system application. For the purpose of the implementation done in this project, an MCU with RF features supporting BLE 5 was needed. Furthermore, it must support all new PHYs introduced...
3. Methods

in BLE 5 and have similar power and memory characteristics as the one aimed to compare to, which is described in Section 4.1. Other aspects that affected the choice of hardware platform were availability, unit price, technical support from vendor, and the ability of having a standalone RF core for possible further development. By considering these aspects and investigating the market for possible hardware, several MCUs were identified to be suitable for the task. There were namely three SoC that were further investigated, all with support for all PHYs and similar power characteristics:

- nRF52840 from Nordic Semiconductor. Based on ARM Cortex-M4F, 64MHz clock speed, 1MB Flash, 256kB RAM [38].
- ERF32MG12 Mighty Gecko from Silicon Labs. Based on ARM Cortex-M4, 40 MHz clock speed, 1MB Flash, 256kB RAM [39].
- CC2640R2F from Texas Instruments. Based on ARM Cortex-M3, 48MHz clock speed, 128kB Flash, 20kB RAM [40].

The hardware platform chosen for the project was the CC2640R2F from Texas Instruments. This platform is a complete SoC solution combining a 2.4 GHz RF transceiver, 128kB programmable flash memory, 20kB SRAM, and includes a full range of peripherals. This SoC has two cores, one main ARM Cortex-M3 CPU and additional radio core based on ARM Cortex-M0. Even though the memory of this platform is a lot less than the other comparable platforms, it is considered sufficient as the application will not require large memory. Additional argument for this choice of platform is the unit price\(^1\) as the CC2640R2F costs 30% less the other two platforms.

The main core is responsible for everything from the application layer down to the Link Layer in the BLE protocol. It is designed to meet system requirements of low memory footprint, and low power consumption, while still delivering excellent computational performance.

The RF core interfaces the analog RF and base-band circuitries, handles all data transfers to and from the system side, and assembles the data in the BLE packet structure. It is capable of autonomously handling time critical high priority tasks of the BLE protocol, and thus offloading the main CPU, leaving more resources for the user application.

Additionally, the MCU includes a Sensor Controller block that provides extended low-power ability as it is capable of controlling data acquisition and external communication (SPI, I\(^2\)C) independent of the main CPU. The CC2640R2F is equipped with a power-management system that is able to efficiently power down the device during extended periods of inactivity, positioning it perfectly for battery operated applications. The power characteristics of the CC2640R2F are summarized in Table

\(^1\)Pricing from Mouser, as of May 2018.
3. Methods

3.1 where the current measurements assume ambient temperature of 25°C and supply voltage of $V_{DDS} = 3.0V$.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>MIN</th>
<th>TYP</th>
<th>MAX</th>
<th>Unit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supply Voltage</td>
<td>1.8</td>
<td>3.0</td>
<td>3.8</td>
<td>V</td>
</tr>
<tr>
<td>Reset state</td>
<td>100</td>
<td></td>
<td></td>
<td>nA</td>
</tr>
<tr>
<td>Shutdown mode</td>
<td>150</td>
<td></td>
<td></td>
<td>nA</td>
</tr>
<tr>
<td>Standby mode*</td>
<td>1.1</td>
<td></td>
<td>3.0</td>
<td>µA</td>
</tr>
<tr>
<td>Idle mode</td>
<td>550</td>
<td></td>
<td></td>
<td>µA</td>
</tr>
<tr>
<td>Active mode</td>
<td></td>
<td></td>
<td>1.45 mA +</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>31 µA/MHz</td>
<td></td>
</tr>
<tr>
<td>Radio RX **</td>
<td>5.9</td>
<td>6.1</td>
<td></td>
<td>mA</td>
</tr>
<tr>
<td>Radio TX, 0dBm power</td>
<td>6.1</td>
<td></td>
<td></td>
<td>mA</td>
</tr>
<tr>
<td>Radio TX 5dBm power</td>
<td>9.1</td>
<td></td>
<td></td>
<td>mA</td>
</tr>
</tbody>
</table>

*Depending on retention selection
**Depends on Single-ended or Differential RF mode

This hardware platform provides excellent RF characteristics, including TX power range of -21 dBm to +5 dBm and low spurious emissions. The RX sensitivity changes according to the PHY being used and can be seen in Table 3.2.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>LE 1M</th>
<th>LE 2M</th>
<th>LE Coded S=2</th>
<th>LE Coded S=8</th>
<th>Unit</th>
</tr>
</thead>
<tbody>
<tr>
<td>RX Sensitivity</td>
<td>-97</td>
<td>-92</td>
<td>-101</td>
<td>-103</td>
<td>dBm</td>
</tr>
</tbody>
</table>

3.2.2. Software Description

The software used to control the behavior of the hardware platform was developed using an integrated development environment (IDE) called Code Composer Studio (CCS). CCS is based on the widely used Eclipse environment. The software developed in this project utilizes a Software Development Kit (SDK) produced by TI. The specific SDK used is v1.50.00.71 supporting BLE 5 stack v1.01.00.71. This stack is the only one that supports the usage of all PHYs introduced in BLE 5, both while advertising and when connected, and the usage of advertising extensions. However, this SDK is tagged for evaluation only as it lacks testing and certificates to be used for an actual product. This project is done with focus on improvements and done
3. Methods

with educational purposes, thus the absence of certification in this BLE stack is not of high concern.

The BLE SDK used for the CC2640R2F consists of an application image using an the TI-RTOS kernel, TI drivers, and a BLE profile using the stack image that implements the BLE protocol. This project includes development of the application image to be able to perform the intended tasks. Additionally, the BLE profile was modified to achieve dynamic configuration of advertising and connection parameters.

A significant part of the software architecture is the TI-RTOS kernel, that operates as a real-time, preemptive, multi-threaded operating system that provides tools and drivers for synchronization and scheduling. The RTOS kernel manages four distinct context levels in a priority based scheduling paradigm. The priority between these different levels cannot be modified. These levels are the following with the highest priority to the lowest: Hardware Interrupts, Software Interrupts, Tasks, Idle Tasks.

The Hardware Interrupt (Hwi) threads, typically called ISR (Interrupt Service Routine), have the highest priority in a TI-RTOS application and are used to perform time critical tasks that have hard deadlines. These Hwi threads are triggered in response to interrupts that occur in the real-time environment and ensure that BLE protocol stack meets RF time-critical requirements. Software Interrupts (Swi) provide additional priority levels between the Hwi and Task threads. Swi threads have time constraints which prevents them from being run as a normal high priority task. Swi threads are allocated only enough memory to save the context for each preempted Swi priority level. Tasks however differ from Swi in that way that they can be blocked during execution until a resource is available. Furthermore, tasks need separate stack for each thread, and use mechanisms like semaphores, events, message queues, and mailboxes for inter-task communication. Finally the Idle Tasks execute at the lowest priority and are executed one after another in a continuous loop.

Further description of the software application implemented for this project can be seen in Section 4.2.

3.3. Measurements

Several measurements were done to carry out the evaluation of the application implemented for this project. The evaluation metrics includes throughput, range and power measurements.

Low power consumption is the single most innovative characteristic of BLE technology. Since BLE communication has several different modes of operation and devices
3. Methods

typically spend most of its time in standby mode it is important to be fully aware of the state of the application while measuring power output. The measurements that were done evaluate the average current consumption during the active phase of each relevant operating mode while the voltage is kept constant. The instantaneous power is then calculated as the product of the instantaneous current and the constant voltage. To finally get the average power, the instantaneous power is integrated over the time of interest. These power measurements are carried out using an expansion board from STMicroelectronics called X-Nucleo-LPM01A [41]. This board is designed as a power supply source with advanced power consumption measurements, capable of measuring current ranging from 1 nA to 200 mA with 2.2 Msps sampling rate. The power measurement data was collected through STM32CubeMonitor software tool and further analysed using various Matlab scripts.

Range testing is done by physically using the hardware running the application software. Utilizing both BLE 4.x and BLE 5 separately, two types of range tests were performed. Firstly a measurements in a two floor house with a balcony and a large garden, and secondly a LoS range measurement. When operating in the house, which can be considered a typical environment for this use case, distance measurement is done using a blueprint of the house and surrounding area. Distance measurements on the blueprint were done using Autocad CAD software with estimated precision of about 0.5 meters. The distance in the LoS measurements was measured using GPS coordinates and compared to simple step measurement to validate certainty of measured values. The range tests uses the alarm service where the peripheral device sends an alarm signal to the central device with pre-determined time intervals. The connection is considered lost when two consecutive alarm message are not received on the central side. Similar range measurements are done for connection initiation as that is a more fragile process that is more sensitive to interference and packet loss. All range measurements were repeated several times until a consistent result is achieved.

Finally, the throughput measurements are done to evaluate the benefits that can be seen when utilizing the LE 2M PHY. This is done in similar manner as an OAD (Over-the-Air Download) [42]. Unfortunately the limitations of the BLE Stack used for this project prevents the traditional OAD operation as it is implemented by TI. As this is only an evaluation of how the LE 2M PHY variant can improve a firmware update or data streaming, it is assumed that the OAD can be performed at the maximum data throughput reached with the device. To reach the maximum throughput, a large data stream is transmitted at the optimal connection interval with all power saving options disabled. After ten successful packet transmission the throughput is calculated. A software timer is used to measure the duration of the data transmission and calculate the data throughput. Each measurement is carried out 100 times sending a total of 1000 packets for each throughput result. Devices are set up 0.2 m apart for all measurements, transmit power set to +5 dBm and the transmission is configured to send without response to maximize throughput.
3. Methods

Further details of the test setup and configuration of test parameters are described in Section 4.3.

3.4. Data Analysis

The implementation part of this thesis project requires some data analysis to evaluate various results. The testing is mainly done on three characteristics, range, throughput and power consumption. The range and throughput measurements only require very limited amount of analysis that is done manually. However the power measurement data will need additional analysis with the help of software tools.

As explained earlier, the power measurements are done by sampling current consumption data of the target device. To calculate the power dissipation over time and the average power, Matlab is used. A numerical method called Trapezoidal Method is used to approximate the integral of the instantaneous power. The approach of this method is to break the vector data down into trapezoids for simpler area calculations, which is then added to approximate the integral of the data over the specified time interval. Finally the data samples are presented in an intuitive illustrations where the power consumption of each operating mode can be observed.
Chapter 4.

Implementation

The implementation carried out in this thesis project is mainly to evaluate the benefits of using BLE 5 as the means of wireless connection for a specific use case. This chapter aims to explain the use case used as guideline, describe the software developed during the process, outline the test scenarios set up for the evaluation, and finally discussion and comparison of several technologies with similar focus as BLE.

4.1. Product Background

A specific use case was decided to be used as guideline for the implementation part of this project with the intention of improving the wireless activity of that product. This is a product named BellPal Watch, designed by a team from Tritech for a company named BellPal. This is a hybrid smartwatch designed specifically for elderly people with high risk of severe injury when they fall down. The BellPal watch contains an accelerometer using algorithms that can detect a fall of the user. When the watch detects a fall, an alarm event is sent via BLE to a smartphone, given that the device is within range. The BellPal watch is equipped with a CC2640 SoC from Texas Instruments and uses BLE 4.x for all wireless communication. The software application is built on top of the TI-RTOS in the form of a state machine. The BLE activity part of this application will be used as guidelines for the software developed in this project.

To back up literature study, attempt to answer research question, reach project goals, and additionally propose improvements to the functionality of the watch, BLE 5 will be implemented by utilizing all PHY variants presented in BLE 5. The LE 2M PHY with increased throughput will be used mainly for the OAD both to improve power consumption during update, and it could enhance the user experience. The LE Coded PHY will be used both to establish a connection and to maintain a connection when the distance between devices is too great for the LE 1M to handle. An attempt is made to gain benefits from all these new features without user interaction. The
performance of each operating mode is then monitored to get a measure of the possible benefits that BLE upgrade would bring.

4.2. Software Application

The application developed in this project consists of one central device, and one peripheral device. These applications will all run on the CC2640R2F development board during data acquisition and measurements.

The central device would typically be in the form of a smartphone, or other similar device, and the peripheral device is used to emulate the BellPal watch. The peripheral application is designed to be able to emulate the watch using both BLE 5 and prior version with limited flexibility. The BLE 4.x utilizes a single PHY and static configuration parameters for advertising and connection. When the application is configured to support new BLE 5 features, several connection parameters are change manually. The BLE 5 part of the application emulates the watch and adds option of dynamic configuration of the PHYs used for both advertising- and connection events.

4.2.1. Central Device

The central device is used to emulate a smartphone application with a GATT client functionality. The application is built in the TI-RTOS environment using BTool (PC application developed by TI) as a user interface. The basic functionality of the central device can be described with a simple state machine seen in Figure 4.1.

Scanning State is the initial state of the central device. Scan configurations ensure that the central device detects connectible advertising packets regardless of what PHY is used. When a specific peripheral device is detected, using the UUID as an identifier, a connection is initiated. The central device is configured to only have one active connection at a time, just for convenience of this particular task. When a connection has been established, there are four state transitions possible. Three of these states can be triggered from the user interface.

An Over-the-Air Download (OAD) can be requested by the user. The OAD state is designed to evaluate the improvements that increased throughput might have on the operation of this application. The software developed in this project however only emulates such a data transmission without actually updating the firmware. When OAD state is entered, connection parameters are reconfigured and set to transmit without response. This enables the connection to reach highest possible throughput and discover the maximum benefits of high speed data transmissions using BLE.
4. Implementation

4.2. Peripheral Device

The peripheral application is built to emulate the BellPal watch product with the aim of comparing the results of using BLE 4.x and then BLE 5. The application is designed to support two variants of operations, only older BLE configurations enabled, and then all BLE 5 related features enabled. The actual connection parameters that are used on the BellPal product are used in this application in order to make the results realistic and closest to the actual product. Figure 4.2 shows an FSM describing an abstract functionality of the peripheral device. Note that the ‘Set PHY’ state only applies for when the peripheral device is utilizing the BLE 5 functionalities.

When only BLE 4.x features are enabled, the peripheral application emulates the same BLE functionality as BellPal watch. Other abilities such as accelerometer readings and factory reset, that is present on the BellPal watch, are disregarded in this implementation as it does not affect the results of BLE tests. The initial state of the application is Advertising. There a connectible advertising packet is activated and when a peripheral device is detected, it will connect to the peripheral device and initiate an OAD state. From there, the peripheral device will go through different states until the connection is terminated either manually via the user interface, or if the peripheral device is out of range or not powered. This results in the central device going back to the Scanning state where it will stay until a peripheral device is detected or it is powered off.

Figure 4.1.: FSM describing basic Central Device functionality.

Alarm Handling state has the highest priority and is reached when an alarm is received from the peripheral in the form of a notification. Continuous alarm message is received from the peripheral until the user acknowledges the message, thus restarting the alarm and going back to the Connected state. Finally the connection can be terminated either manually via the user interface, or if the peripheral device is out of range or not powered. This results in the central device going back to the Scanning state where it will stay until a peripheral device is detected or it is powered off.
transmitted until the central initiates a connection. Upon connection establishment, the connected state is reached where there are three possible transitions. First of all there is the Alarm Handling state, which emulates a fall detection of the BellPal watch. This state is simply triggered with the push of a button on the launchpad, and uses a custom built GATT service to send alarm message to the central using BLE notifications. This state is of highest priority and is only left when the alarm is reset from the central device, connection is lost or power is turned off. The OAD state is really a high throughput mode where the focus is maximizing the data throughput, thus emulating an efficient OAD. This state is reached when a message from the central initiates high throughput mode, and starts blasting data at highest possible data rate. Finally, the connection can be terminated manually from either the central or the peripheral, or when the distance between devices gets too large.

When utilizing the new features of BLE 5, the application has the same basic functionality but with the addition of dynamic PHY switching capabilities. This includes an extra state in the basic FSM that determines which PHY is used for communication. To automatically determine the best suitable PHY for operation the RSSI value is used. A weighted average of RSSI values is reported to the central device to determines a the best suited PHY. The threshold that decides which PHY should be used was decided by manual inspection. The RSSI value was observed in several scenarios and finally decided to be as follows:

- LE 2M shall be used when RSSI < -40 dB and when OAD is performed.
- LE 1M shall be used when -40 dB < RSSI < -80 dB.
- LE Coded S=2 shall be used when -80 dB < RSSI < -95 dB.
4. Implementation

- LE Coded S=8 shall be used when RSSI > -95 dB

4.3. Evaluation Plan

The tests carried out in this implementation will consist of power, range and throughput measurements. These tests will be done using two CC2640R2F launchpads where one acts as the central device, emulating a smartphone, and the other acts as the peripheral device, acting as the watch. All tests where the covering range is not of concern will be performed in a typical office environment. The covering range is then tested in two separate parts, in a typical home environment, and a Line-of-Sight (LoS) range test where no objects are in between the two devices.

During testing, the central device will be hooked up to a PC where BTtool will be used as an interface to control connection parameters and verify data transmissions in addition to the central application. This makes it convenient to track the connection establishments and terminations in real time. The peripheral will be powered by a 3.3V coin cell battery and LEDs will indicate state of device, which PHY is used, and if the connection is terminated. It is worth noting that all I/O peripherals and external flash memory will be disabled when measuring the power consumption. These features are not necessary for this application and allows for a lower standby current. This forces only the mandatory RF operations will to be active when nothing else is needed and allows for a clean power measurement of the BLE activity.

All tests aim on measuring the performance of the BLE link focusing on the different capabilities of the new BLE 5, and comparing results to the older versions. Meaning that tests are done using older version of BLE, capable of only LE 1M PHY and without data length extensions (where maximum PDU is 27B), the same BLE functionality as the current BellPal Watch. Then tests are done in the same condition expanding the low layer configurations using the new available PHYs and increasing the PDU gain higher data throughput in order to see how that affects the systems power consumption. Each of the three test categories are explained in more detail further in this section.

4.3.1. Power Measurements

This test will collect data on power consumed during all states of interest while advertising and in connected mode. The measurements are done using an X-Nucleo-LPM01A expansion board from STMicroelectronics which allows for a real time dynamic current sampling of the device. During the test, the DUT is powered by the X-Nucleo expansion using its programmable output power set to 3V. The power consumption will be evaluated in several parts: during active advertising, alarm
message transmission in connected state, maximum throughput connection and in standby mode which happens between BLE activities.

To get a clean current measurement of only the BLE activity, the jumpers shown in Figure 4.3 are removed. This is done as the additional features that are present on the launchpad, but should not be included in the final product, such as JTAG, LEDs, programming and debug capabilities. These features introduce additional and unnecessary current consumption and noise seen in the power readout.

The power consumed while advertising is significantly affected by several properties that have to be decided while advertising. As described in Chapter 2, the advertising interval, TX power level, advertisement data length, number of advertisement channels used and advertising PHY are all factors that drastically impact the power consumption. For the tests conducted, the only parameter listed here that is changed is the advertising PHY. The advertising interval is set to 400 ms, all three advertisement channels are used, and TX power is set to 5 dBm. The advertisement data contains 7 bytes of advertising data with additional overhead that is necessary. The advertisements are configured to be connectible, scannable undirected advertising events. Apart from the PHY used, another difference in the advertising measurements is a feature called Advertising Extensions (AE) that was introduced with BLE 5. When using coded PHY, it automatically uses the AE. The main difference in the default Legacy advertisement and using the AE, is that the former transmits and listens consecutively for response on the same channel. When the AE is used, it transmits data that includes a pointer to a secondary advertising channel to all primary advertising channels, and then transmits data and listens for requests.

Power consumption is again measured when connection has been established and alarm message is sent periodically as a notification when manually triggered. The current consumed is then measured for a single transmission of an alarm message. This test is done for all PHY variants, keeping all connection parameters constant for comparable measurements. However, the majority of the time during a single connection event consists of standby, the standby power consumption is measured.
between two consecutive connection events. There are number of ways to optimize connection parameters to a certain application, but in this case it was decided to use the same basic connection parameters as configured on the BellPal watch. The connection interval was set to 50 ms, slave latency set to 20 intervals and connection timeout to 6 s. A single packet sent during alarm state is only 9 bytes with additional 4 bytes of overhead reaching a total of 13 bytes.

For the maximum throughput, the power consumption is expected to be significantly higher than for all other modes of operation. This is due to the device being constantly transmitting/receiving data to achieve the highest data rate possible. For this part of the tests, a feature called energy utility is measured for all cases. This property is considered a good measure of power consumption as it describes data sent per each unit of energy, and can thus be directly compared to other studies such as [30] and [31]. Connection properties are modified here in order to achieve the highest throughput possible, meaning the slave latency is set to zero, timeout is irrelevant and connection interval can be optimized for a specific packet size and symbol rate. In this case, a connection interval of 100 ms is chosen.

4.3.2. Data Throughput Measurements

Even though BLE is not intended for transmitting large data sets with high speed, it is still an advantage to be able to increase the speed of transmission when desired. High throughput is desirable in scenarios such as when a device needs OAD, or when it needs to send big data sets occasionally. This test is done in order to test what the actual data rate for each PHY can be achieved when utilizing the full connection interval for data transmissions.

The test is done using variable PDU to be able to compare how Data Length Extension (DLE) impacts the throughput. First, the PDU will be fixed at 27B, which is the maximum size before DLE was introduced in BLE, and is used in BLE 4.1 and prior. Secondly, the PDU will be set to 251B, which is the maximum PDU size after DLE is enabled. Measurements will be taken using all PHY variants with the goal to see how beneficial the high speed 2M PHY is for when large chunks of data needs to be transmitted.

4.3.3. Range Measurements

These measurements are done to evaluate how significant improvements can actually be seen using long range PHY variant. The maximum distance achieved between the devices with each PHY variant is then compared. These range tests are divided into two separate parts, typical house covering range and LOS range where an open area is used to test the range. The Peripheral device is powered with a 3.3V coin cell battery through the range test and connection properties are kept constant for
4. Implementation

all PHY variants to get comparable results. The connection interval is set to 50 ms, slave latency set to 10 and the connection timeout is decreased to 1 s. This is done in order to set more strict restriction on when the connection is terminated. This makes it possible to get better readings on the actual limit of the connection. Furthermore, while determining the maximum range, the peripheral device is held close to the body with one hand, similarly as a watch would be worn. This approach takes into account the large interference that the human body can have on RF signal.

The house covering range is tested in an average sized two floor house whose blueprint can be seen in Figure 4.4 along with test points inside and outside the house. This is a concrete house with only thick concrete walls, which is considered a relatively difficult environment for an RF signal to pass through. However, the amount of additional RF interference is relatively small and comes mainly from WiFi signals present in the house, although no formal measurements are done on the RF interference. These tests are supposed to resemble a scenario where the central device (in most cases a mobile phone) is stationary in one room of the house while the user has the peripheral, acting as the BellPal watch, moving around the house. The test is carried out using all available PHY variants while maintaining connection and establishing a connection. During measurements a continuous alarm message is transmitted from the peripheral to the central until connection is terminated. The test is performed a total of 5 times at and around each test point to get clear and consistent results. All distance measurements are done through a blueprint of the house using software tools to get accurate distance readings.

![Figure 4.4: Test points indicated in test area.](image)

To test the LOS range of the connection, a large open area is selected. A straight road with almost no traffic just outside the city is selected to be the testing site. As
with the previous test, all PHY variants are used to test the connection range in order to compare the maximum distance achieved. To carry this test out, the central device is kept stationary while the peripheral device is moved further away simply by holding it and walking in a straight line while the devices have LOS. The distance between the devices is measured using GPS coordinates, which is considered to have sufficient accuracy to evaluate the distance between devices.

4.4. Competing technology

As the field of IoT is rapidly growing, covering a wide variety of applications in different environments and serving diverse purposes, it is important to choose the optimal wireless connection standard. It can be a challenging task to choose the right wireless technology for a specific application as numerous low-power wireless standards are available. This section will briefly describe several standards, aiming on use cases such as home and building automation, health, sport and fitness, HVAC systems, wireless sensor networks and potentially automotive field. The desired characteristics for a technology supporting these use cases are namely small data payload, low latency and ultra-low power consumption. Other characteristics like data throughput, scalability and covering range are additional benefit that can be used to expand the ecosystem of a given technology.

BLE is relatively new on the market of low-power wireless technologies. Other technologies with similar focus have been available for many years. Several such technologies will be discussed in this section. These are: Zigbee, Thread and ANT/ANT+. These technologies were chosen for several reasons, such as they all have similar use cases as BLE, similar operation characteristics and all these standards occupy the highly congested ISM frequency band. The discussion of this section includes power consumption, data throughput, covering distance, interoperability, scalability, omnipresence and why these protocols might be attractive for the field of IoT. All performance data that is presented is according to other published papers or technical specifications from vendors.

4.4.1. Zigbee

Zigbee is an open standard that is designed and maintained by a group called Zigbee Alliance, similarly to Bluetooth SIG, formed by many companies from different industries. Zigbee is one of the earliest released low power standards, with Zigbee Alliance established in 2002, aiming to assist the development of home and building automation. Like BLE, Zigbee is classified as a low-power, short range, low data rate and close proximity wireless ad hoc network [43].
Zigbee is based on IEEE 802.15.4 link layer and like BLE, it operates in the 2.4 GHz ISM band. Its networking operation layer has been designed with mesh based topology in mind from the ground up, providing significant scalability through multihop operations, as well as increased reliability as it can take multiple paths through the mesh. Zigbee has similar layered architecture as Bluetooth. The lower layers of Zigbee architecture are based on the IEEE 802.15.4, and its protocol stack consists of PHY and MAC (Medium Access Control) layer. A set of layers above the lowest layer are then specified by the Zigbee Alliance. The channel access used in Zigbee is CSMA/CA (Carrier-Sense Multiple Access with Collision Avoidance) as opposed to AFH in BLE. Furthermore, the air data rate in Zigbee is only 250 Ksym/s compared to 2 Msym/s in BLE. Zigbee uses 16 channels on the ISM band that are 2 MHz wide and are separated by 5 MHz, thus it is rather spectrum inefficient due to its unused allocation.

The layers of Zigbee make use of star, mesh and tree topologies. A Zigbee network consists of three possible device types: Coordinator, Router and End Device. The Coordinator is the most capable device, it forms the root of the network tree and can possible act as a gateway to other networks. There is only one coordinator in each Zigbee network, and it stores all necessary information about the network. The Router acts as an intermediate router passing on data through the network. Then the End Device is the most resource constrained device and contains just enough functionality to perform its specific action and connect to routers or coordinators.

To overcome interoperability issues from different manufacturers, Zigbee provide a complete solution. This approach enables true device interoperability between devices regardless of their origin. Furthermore, the Zigbee protocol suite includes standard commissioning, security, network and device management procedures. This means that various device types can join the network, and be decommissioned in an interoperable way, ensuring end-to-end device interoperability [5]. However, a significant limitation for Zigbee is that it has not been included by the mobile device industry, that limits its usage and deployment.

Zigbee is designed to use ultra low power. For a given scenario, it needs more energy than BLE but less than ANT [44]. The power consumption is however strictly dependent on hardware modules, operation mode and environment. The scalability of Zigbee is also very promising as it is designed for mesh networking topology using really effective routing algorithms. Theoretically a single device can connect to 254 other devices, and a Zigbee network can be contain up to 65535 nodes [45]. The protocol is widely adopted in ready home automation, but not supported by the biggest player of the consumer electronics market, the smartphone, making it less appealing to IoT developers compared to BLE.
4.4.2. Thread

In 2014 the Thread Group was formed by Google, Samsung and numerous silicon vendors that were aiming for direct connection from low-power IoT devices to IP networks. The main goal of the Thread Group was to define a standard that ensures device interoperability in smart homes and is specially designed for wireless device-to-device communications.

The Thread stack is an open standard that is based on collection of existing standards defined by IEEE (Institute for Electrical and Electronics Engineers) and IETF (Internet Engineering Task Force). The lower layers are based on the 802.15.4 MAC and PHY for the radio transceiver and then the internet protocol is based on 6LoWPAN (IPv6 over Low Power Wireless Personal Area Network). This adapts some advantages from these standards such as low-power operation, IPv6 addressability and mesh networking capabilities. This IPv6 addressability provides a significant advantage as it allows devices simpler access to the internet while eliminating the need for a special gateway. Thread operates on the ISM band and provides on-air data rates up to 250 Kbps and can support up to 250 nodes in a single local mesh network [5].

Thread achieves high reliability through its self-healing mesh topology that avoids a single point of failure. Several device types are defined in Thread communications: Border Routers (gateways), Thread Routers, Router-Eligible End Devices (REEDs), Leaders, End Devices and Sleepy End Devices. With clever implementation of these device types, the Mesh Link Establishment (MLE) provides this self-healing mechanism by dynamically reconfiguring the network in response to any failures without any user interaction. The main use case for Thread devices are smart home system, although it can be expanded to a wider variety of use cases [46].

Like the other compared protocols, Thread is designed for ultra low power consumption and has similar power characteristics, point-to-point covering range and throughput as Zigbee, as both technologies are based on the same lower layers. The scalability of Thread protocol is also considered to be really good as the technology is designed for mesh networking topology using effective routing algorithms that can theoretically support unlimited number of nodes. Thread is an open standard, using IP based stack and is relatively new on the market. It is aiming on home automation, and is predicted to have wide prosperity in the next several years as Google are the main innovators behind the standard [47].

4.4.3. ANT/ANT+

ANT (Advanced and adaptive Network Technology) is another protocol that is designed for WPAN (Wireless Personal Area Networks) aiming for low-power, low data rate and short range. The ANT wireless protocol was launched in 2003 and in
4. Implementation

2004 the ultra-low power wireless standard ANT+ was created. ANT+ are device profiles implemented on top of ANT, managing sessions and application layers to provide data and device interoperability. The ANT+ definitions are called profiles, and play a similar roles as the BLE profiles. The protocol was designed and is maintained by the the ANT+ Alliance, an open special interest group combined by members from various companies. Its primary applications are in the field of health monitoring [48].

Like BLE, ANT operates in the licence free ISM band and uses 125 channels where each one is 1 MHz wide. ANT provides on air data rate of 1 Msym/s. The modulation scheme used in ANT is the same as in BLE, GFSK. The ANT protocol operates using master and slave roles, where a master transmits messages and a slave receives them. For bidirectional communication, each node has both roles simultaneously. The data packets used in ANT are defined as 8 bytes that are transmitted on a 150 µs (or less) frame. ANT can reach maximum effective throughput of 60 Kbps [49].

ANT has several advantages such as the simplicity of the protocol provides an ultra low power and robust communication, minimum packet overhead, and offers different kind of network topologies (P2P, star, tree, mesh). However, its availability in smart phones and other commercial central devices is not as ubiquitous as BLE, which is a significant advantage that BLE has over this and other wireless protocols.

Similarly to the other protocols mentioned, ANT is designed for ultra low power consumption. But for a given scenario, it needs more energy than BLE and Zigbee [44]. The power consumption is however strictly dependent on hardware modules, operation mode and environment. This protocol can support large networks, up to 65k nodes per shared channel and can use 8 shared channels simultaneously. This is not as ubiquitous as Bluetooth, but is supported by some android devices such as Samsung phones and tablets, and can be found in a variety of commercial health and fitness products.

4.4.4. Comparison Discussion

It can be cumbersome to compare different wireless protocols head-to-head as the wide variety of available technologies spans a wide range of use cases each having different advantages and disadvantages. However, by gathering data from numerous sources that evaluates each technology it is possible to compare some important characteristics. Table 4.1 compares BLE with the three protocols that have been described, with additional comparison to Bluetooth Classic. It is evident that comparing these technologies, BLE is capable of saving most power during operation according to [44], but these numbers vary significantly between RF modules and operation condition. Another comparison on these protocols, with several additional
4. Implementation

protocols are presented in [50] where it is reported that BLE consumes least power, with ANT+ following closely while Zigbee and Thread require most power for operation.

<table>
<thead>
<tr>
<th>Table 4.1.: Comparison of wireless standards.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bluetooth Classic</td>
</tr>
<tr>
<td>Max bit rate</td>
</tr>
<tr>
<td>Max Data throughput</td>
</tr>
<tr>
<td>Covering distance</td>
</tr>
<tr>
<td>Max nodes</td>
</tr>
<tr>
<td>Power use</td>
</tr>
<tr>
<td>Smartphone support</td>
</tr>
</tbody>
</table>

*Bluetooth Classic can reach far higher throughput using AMP mode.
**BLE has been proven to reach far longer in optimal operating condition using LE Coded.

Another notable performance metrics are robustness and co-existence. Interference from nearby radios, suboptimal transmission environment, or deliberate frequency jamming can all cause corrupted transmission. The transmitter will then keep trying until the packet has been successfully delivered causing excessive power consumption at the expense of the battery life. Moreover, the immunity to interference caused by nearby radios if referred to as coexistence.

All these protocols use some methods to assist coexistence and improve robustness by avoiding congested channels. As described in Section 2.2, BLE uses AFH to enable each node to map the channels to avoid frequently congested channels in future transmissions. ANT provides TDMA (Time Division Multiple Access) to mitigate congestion. This is an isochronous scheme that subdivides its channels to timeslots, providing advantages for large networks. In contrast to this, Zigbee uses a DSSS (Direct Sequence Spread Spectrum) method, where the signal is mixed with a pseudo-random code at the transmitter that is then extracted at the receiver side [51]. These specific methods are however beyond the scope of this thesis and will not be discussed further.
Chapter 5.

Results

This chapter presents test results and brief description of the key findings and characteristics. The tests performed are described in Section 4.3 where all configurations and test setup is discussed. The tests that were performed can be divided into three main categories, power measurements, range testing and throughput tests. All tests are done using both the new BLE 5 and BLE 4.1 to be able to compare its performance in exactly the same conditions and scenarios.

5.1. Power Consumption Results

Power consumption of a BLE link changes significantly between the different operating modes and configuration parameters. By using the STMicroelectronics Power consumption breakout board that is briefly described in Chapter 3, the power consumption was measured for the several different operating conditions that is evident in this implementation. The test results can be divided into the following main parts:

- Advertising - using all PHY variant that allow advertising.
- Connected - sending notifications using all PHY variants.
- High throughput using all PHY variants.
- Standby mode between connection and advertising events.

As explained in Chapter 2, BLE 5 introduces the possibility to advertise using the LE Coded PHY allowing greater range while initiating a connection. The application implemented in this project is configured to advertise using all possible PHY variants. Figure 5.1 illustrates the current consumption profile of a single advertising event. All three advertising events contain the same advertising data, scan response data, advertising interval and TX power. As can be observed, significantly higher time and power is spent while advertising using the LE Coded PHY variants, as it is traded for higher covering range of connection initiation. Furthermore, it can be observed that the legacy advertisement and LE Coded advertisements use the same
5. Results

time in preparing the radio, or about 1.5 ms. After the radio preparation, the Legacy advertisement transitions to TX on the first primary advertising channel, then transitions to RX as it listens for scan request or connection initiation, and so on. This is different when using LE Coded PHY for advertising. As explained earlier, LE Coded advertisements automatically use Advertising Extensions (AE) and thus transmit information for auxiliary pointer in order for the central device to know which data channel to listen to and send scan/initiation request. For a single

![Graphs of BLE power consumption for Legacy Advertising, Coded S=2 Advertising, and Coded S=8 Advertising](image)

**Figure 5.1.: Single connectable advertising event for each PHY able to advertise.**

Legacy Advertisement, the average current consumption measured was 3.48 mA and consuming average power of 11.51 mW using a total of 57.56 µJ of energy. When using Coded advertisement, with S=2 coding scheme, the average current consumption was measured to be 4.86 mA, with corresponding average power consumption of 16.06 mW and using a total of 120.43 µJ. The last advertising type, LE Coded with S=8 coding scheme, had average current draw of 5.86 mA, consuming average power of 19.34 mW and using a total of 203.11 µJ.

Figure 5.2 shows current consumed during a single connection event when alarm notification was enabled. The figure shows four different profiles, one for each PHY variant, where each contains the same data being sent with same configuration parameters where the only difference is the PHY variant used. As the data being sent
is really small, only two bytes of PDU with several additional overhead bytes, the difference in the radio on-time is not significant. As can be observed, the connection event begins on radio preparation, then starts RX mode (around 6 mA consumed current) as the master always sends the first packet in a connection event, as described in Chapter 2, and then proceeds on transmitting the alarm message. Using the 1M PHY, the average current for a single connection event sending a notification was measured to be 2.16 mA, consuming average power of 7.16 mW and using 35.8 \( \mu \)J of energy. Same connection event using the 2M PHY had average current draw of 1.92 mA, consuming average power of 6.36 mW and using 31.8 \( \mu \)J of energy. Coded PHY with S=2 coding scheme had average current draw of 4.45 mA, corresponding average power of 14.51 mW and using 73.54 \( \mu \)J of energy. Finally with S=8 coding scheme, a single notification had average current draw of 4.80 mA, average power of 15.87 mW and 79.33 \( \mu \)J energy expenditure.

\[ \text{Figure 5.2.: Single notification in a connection event for all PHYs.} \]

BLE gains its ultra low power characteristics by utilizing an extremely low standby current as it is intended to operate with the radio in standby mode the majority of its lifetime. Between each advertising event and connection event, the hardware platform goes to complete standby mode where it consumes very little power. However, during the standby mode, a VDDR recharge pulse is necessary for the device to have the clocks powered and retain the RAM for operations due during next scheduled wake-up. Thus the standby power will here be defined as the ultra low power consumed in between the connection/advertising events including the VDDR recharge pulses. The frequency of the recharge pulses is variable and depends on the connection parameters such as advertising/connection interval, slave latency and SCA (Sleep
5. Results

Clock Accuracy). Figure 5.3 illustrates a standby current profile between connection events where a recharge pulse is also shown. The low current between the pulses and connection/advertising events is extremely low or around 100 nA and can go down to 70 nA. The X-Nucleo power measurement board that is used is capable of measuring down to 100nA, meaning that readings below that value can be skewed. To get more precise readings on the actual standby current a more advanced measurement setup is required. The test result show average current consumption during standby mode to be 0.997 \( \mu \text{A} \) with average power consumption of 3.29\( \mu \text{W} \). It should be noted that this number can change considerably depending on when the measurements are done, as the recharge pulses are dynamically configured according to the time required in standby. So directly when the DUT is reset, it needs more recharges between events, but after several cycles it goes down to an optimum value of recharge pulses.

![Figure 5.3](image)

*Figure 5.3:* Radio standby between connection events. A single VDDR recharge pulse can be seen scaled in time on the lower subplot.

BLE is not optimal for use cases that require high throughput for the majority of its operating time. However, many applications need to be updated or transmit/receive large amount of data occasionally. When BLE is used to gain high throughput its power consumption increases significantly accordingly. These test results measure the energy utility on a BLE link of the slave device in connected mode, while it is constantly transmitting using +5 dBm output power. This is done by measuring the energy required to transmit a single packet. This is done for two sizes of packets, maximum PDU with and without DLE (27B and 251B). Test results in Table 5.1 show how the energy utility improves with bigger data packets and shows clearly that LE 2M PHY is the far best option for high speed data transmission.
5. Results

Table 5.1.: Energy utility comparison of each PHY using different PDU size.

<table>
<thead>
<tr>
<th></th>
<th>LE 2M</th>
<th>LE 1M</th>
<th>LE Coded S=2</th>
<th>LE Coded S=8</th>
</tr>
</thead>
<tbody>
<tr>
<td>PDU = 27B</td>
<td>2.28 MB/J</td>
<td>1.12 MB/J</td>
<td>0.41 MB/J</td>
<td>0.21 MB/J</td>
</tr>
<tr>
<td>PDU = 251B</td>
<td>4.70 MB/J</td>
<td>2.57 MB/J</td>
<td>1.16 MB/J</td>
<td>0.35 MB/J</td>
</tr>
</tbody>
</table>

A summary of the power consumption test results can be seen in Table 5.2, where some of the measured characteristics can be compared. As can be seen, the high throughput test results provide different units of measure, this is done as the amount of data per a unit of energy is considered a more relevant characteristic at this point. Furthermore, a breakdown of each part of the power profile for advertising event, can be seen in Appendix A.

Table 5.2.: A summary of power consumption test results.

<table>
<thead>
<tr>
<th>Test case</th>
<th>LE 1M (BLE 4.x)</th>
<th>LE 2M S=2</th>
<th>LE Coded S=2</th>
<th>LE Coded S=8</th>
</tr>
</thead>
<tbody>
<tr>
<td>Advertising event [mW]</td>
<td>11.51</td>
<td>-</td>
<td>16.06</td>
<td>19.34</td>
</tr>
<tr>
<td>Single TX Alarm event [mW]</td>
<td>7.16</td>
<td>6.36</td>
<td>14.51</td>
<td>15.87</td>
</tr>
<tr>
<td>Standby mode [µW]</td>
<td>3.29</td>
<td>3.29</td>
<td>3.29</td>
<td>3.29</td>
</tr>
<tr>
<td>Max Throughput PDU=27B [MB/J]</td>
<td>2.28</td>
<td>1.12</td>
<td>0.41</td>
<td>0.21</td>
</tr>
<tr>
<td>Max Throughput PDU=251B [MB/J]</td>
<td>4.70</td>
<td>2.57</td>
<td>1.16</td>
<td>0.35</td>
</tr>
</tbody>
</table>

5.2. Throughput Results

Table 5.3.: Data throughput of each PHY using different PDU size.

<table>
<thead>
<tr>
<th></th>
<th>LE 2M</th>
<th>LE 1M</th>
<th>LE Coded S=2</th>
<th>LE Coded S=8</th>
</tr>
</thead>
<tbody>
<tr>
<td>PDU = 27B</td>
<td>388.4 kB/s</td>
<td>288.9 kB/s</td>
<td>101.5 kB/s</td>
<td>29.3 kB/s</td>
</tr>
<tr>
<td>PDU = 251B</td>
<td>1366.4 kB/s</td>
<td>780.8 kB/s</td>
<td>175.7 kB/s</td>
<td>58.6 kB/s</td>
</tr>
</tbody>
</table>

As discussed thoroughly in Chapter 2, the maximum data throughput possible in a BLE connection can never reach the actual symbol transmission rate. This test attempts to reach the maximum throughput that can be achieved for each PHY using the test platform. More detailed description of the connection configuration and how the maximum throughput is achieved is described in Section 4.3. Two different results are presented for each PHY variant, where one uses a PDU of 27 bytes (BLE 4.1 and earlier), and the other utilizes data length extensions with a PDU of 251 bytes.
5. Results

Maximum data throughput with/without data length extension

<table>
<thead>
<tr>
<th>LE 2M</th>
<th>LE 1M</th>
<th>LE Coded S=2</th>
<th>LE Coded S=8</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>200</td>
<td>400</td>
<td>600</td>
</tr>
<tr>
<td>800</td>
<td>1000</td>
<td>1200</td>
<td>1400</td>
</tr>
</tbody>
</table>

Figure 5.4.: Difference between maximum data throughput of each PHY with and without data length extensions.

5.3. Range Results

As discussed in Chapter 4, the range measurements are done in two different scenarios, home covering range and LOS range. First, the range is observed in a typical two floor concrete house where test points are marked all around the house as can be seen in Figure 4.4. For this test both connection initiation, and maintaining an already established connection, while sending alarm message to the peripheral, were tested. Section 4.3 states all relevant connection parameters describes the test area and setup. Measurements on each test point is done a total of 5 times for each PHY and in almost all cases, the results were the same. Meaning that the measurements and connection was consistent while doing the tests. The results from these tests can be seen in Table 5.4, where the remarks column states any notable description of the area or whether the connection was inconsistent. Unfortunately, no special RF

Table 5.4.: Range test results, first column represents test points in the house, result set up as [A,B], where A answers if the connection was maintained at the test point and B answers if the connection could be initiated at the test point.

<table>
<thead>
<tr>
<th>#TP</th>
<th>LE 2M</th>
<th>LE 1M</th>
<th>LE Coded S=2</th>
<th>LE Coded S=8</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Y, -</td>
<td>Y, Y</td>
<td>Y, Y Y, Y, Y, Y</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Y, -</td>
<td>Y, Y</td>
<td>Y, Y Y, Y, Y</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Y, -</td>
<td>Y, Y</td>
<td>Y, Y Y, Y, Y</td>
<td>Distance only about 12 m, many large walls between</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>N, -</td>
<td>Y, Y</td>
<td>Y, Y Y, Y, Y</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Y, -</td>
<td>Y, Y</td>
<td>Y, Y Y, Y, Y</td>
<td>Directly under the central device</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>N, -</td>
<td>Y, N</td>
<td>Y, N Y, Y, Y</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>N, -</td>
<td>N, N</td>
<td>N, N Y, Y, N</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>N, -</td>
<td>N, N</td>
<td>N, N N, N, N</td>
<td>Many concrete walls + fridge and freezer causing interruption</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>N, -</td>
<td>Y, N</td>
<td>Y, Y Y, Y, Y</td>
<td>Limit of LE1M connection initiation</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>Y, -</td>
<td>Y, Y</td>
<td>Y, Y Y, Y, Y</td>
<td></td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>Y, -</td>
<td>Y, N</td>
<td>Y, Y Y, Y, Y</td>
<td></td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>N, -</td>
<td>N, N</td>
<td>Y, Y Y, Y, Y</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
communication analyzer was available to get further readings on the BER or other specific characteristics of the connection to evaluate the reliability of the connection. Figure 5.5 further illustrates the covering range of each PHY variant at the test site.

![Figure 5.5: House covering range of all PHYs compared.](image)

The second part of the range test was to identify the LOS range for each PHY. This characteristic is very dependent on the PHY variant used, TX power settings, hardware platform used, and testing area. The test setup, connection parameters and test area is described in detail in Section 4.3. For this test, the same alarm message was sent from the peripheral to the central when the connection had been initiated. Figure 5.6 shows actual marked locations on a map where the test was carried out.
Figure 5.6.: Map view of LOS measurements.
Since its origin about 20 years ago, Bluetooth has kept evolving and adapting to technology advancements. With innovative new functionalities such as BLE and Bluetooth Mesh, the technology has a real potential of being the main wireless protocol used in IoT communications for decades to come. This statement can be supported by looking at studies of comparable technology, literature review, recent BLE improvements, and the fact that Bluetooth enabled devices can be found everywhere, meaning that the infrastructure for worldwide usage is partly evident.

Furthermore, the new features introduced in BLE 5 expand the ecosystem of BLE devices as it open the doors for use cases that require even lower power consumption, greater range or higher throughput. These features cannot all be utilized simultaneously, but could all be used on the same product for more efficient functionality by dynamically switching PHY variants and other connection properties.

During this project, the BellPal watch was aimed at as the use case. Data was acquired for comparison by implementing similar BLE activity as the actual product uses. The results included data that used connection properties limited to prior versions than BLE 5, as well as the new features. These new BLE 5 features consist of utilizing high throughput, long range and decreased power consumption. The benefits that are evident when utilizing new features of BLE 5 will be discussed within this chapter while aiming on answering the research questions proposed early in this thesis.

6.1. Implementation Challenges

During development of BLE application it is important to be aware of the low level functionality of the device. Throughout this project several obstacles and challenges were faced when attempting to perform the desired functionality. This section briefly discusses the problems that had most impact on the work done during this project.
6. Summary and Conclusion

and how they could have been prevented. The purpose of this part of the discussion is to emphasize the importance of detailed planning and effective literature study, both academic and practical.

The Software Development Kit (SDK) that was originally used for the software development, is not the full official release of this SDK but an evaluation version, caused relatively more problems than expected prior to the implementation. A large amount of time went into searching for defects and finding workarounds, and support from the manufacturer was minimal as this was not the official release of the SDK.

Another challenge was identified while verifying data transmissions and connection parameters. It can be hard to verify what packets contain when working with wireless connectivity. By having a proper BLE sniffer to be able to analyze the content of each packet and measure packet loss would improve measurement results quality significantly while offering more time efficient tests and wider analysis possibilities. Unfortunately this product does not exist within a reasonable price range for this project.

The original idea of designing an algorithm that is enabled to make use of all the new features present in BLE 5 did not succeed as hoped. This is mainly due to the tactic used to decide which PHY to use. The approach used was to make use of RSSI report values to determine suitability of connection parameters. As the specific use looked at in this project reports so rarely to the central device in daily use, this caused too large excess power consumption. With better planning and analysis before implementation this might have been prevented and a better approach could have been implemented.

6.2. IoT Readiness of BLE 5

The goals of this project were to study BLE 5 in depth and collect information regarding its capabilities to standardize IoT communication that require ultra low power consumption. This thesis summarized information that was collected during the project work while containing several test scenarios that evaluate the benefits of updated BLE technology for a given use case. Three important characteristics were aimed at during the implementation of this project, power consumption, covering range and throughput, of a CC2640R2F hardware platform. Other important features such as in-depth functionality, scalability, omnipresence and infrastructure was evaluated through literature study.
6. Summary and Conclusion

6.2.1. Scalability

The size of an IoT network can be a limiting factor of a system especially in the field of IIoT. This can be defined in two ways, large network containing immense amount of nodes communicating, and a network that requires longer distance between nodes. In some cases these networks demand a technology providing ultra low power consumption such as BLE.

Although the Bluetooth Mesh technology is not of main interest throughout this project, it is worth noting some features that it might bring to the world of wireless technology. Bluetooth Mesh could be an ideal solution within control, monitoring or automation systems. These systems often contain large-scale device network that need to communicate reliably with one another while using ultra low power. Although Bluetooth Mesh could be utilized for industrial grade applications, it could also bring significant benefits to personal systems such as home automation. Bluetooth Mesh has some advantages over other low power wireless technologies supporting mesh topology (such as ZigBee and Thread). These advantages are mainly the already available infrastructure as most interface devices, such as laptops and smartphones, already support Bluetooth.

Furthermore, by using IPv6 over BLE seamlessly while consuming acceptable power could revolutionize the world of IoT even further. This approach has been studied by various sources but is not yet widely supported by the market today.

6.2.2. Low Power Characteristics

Power consumption plays a big role when designing a low power system utilizing BLE. The trade-off in range and power consumption between the different PHYs can have significant impact of the power consumption in a BLE link and thus it has to be thought of in every design process. The results of existing literature provides a range of power measurements where the results seem to vary relatively much, and do not accurate consumption during different modes of operation. Test results of this project aim on including accurate power consumption measurement for all operating modes. The results are summarized in table 5.2 and are discussed here below.

The power profile of the application implemented in this project can be divided into several steps that are repeated during typical operation. First there is advertising mode which occurs when the slave device wants to connect to a master, and then again at specified periods when a connection with the master is lost. The result show power usage for advertising event using three configurations, each using a different PHY variant while transmitting the same advertisement data. For this application, the advertising state is not intended to be operating often but should
6. Summary and Conclusion

however be considered when evaluating the total power consumption. As expected, there is a notable difference between the power consumption where the two new PHY variants using LE Coded exceed the LE 1M by 40% and 68% respectively. The power consumption of each coding scheme is not proportional to the data rate due to the implementation of packet structure and different advertising events as discussed in Chapter 2.

When the device establishes a connection to a master, it stops advertising and transitions to connected mode. During daily usage, no important BLE data transition takes place. The only relevant BLE communication that was measured is transmission of alarm message and large data exchange that represents an OAD. When the alarm is triggered, a notification alarm is set to transmit message every second. This message is considerably small and only carrying several bytes of data. The power profile during this was measured for all available PHY variants. As expected, the PHY capable of the highest data rate needs the least power for each connection event and the one using the lowest data rate consumes most power.

The standby power consumption is one of the most important characteristics for BLE enabled applications. As mentioned earlier, BLE is designed to be a mostly off technology, meaning that it spends most of its time in standby mode. This characteristic varies a lot between hardware platforms and implementation. The test results obtained in this project showed extremely low average power consumption while in sleep mode. This value depends highly on the number of recharge pulses needed to keep the connection alive, thus the connection properties have some impact on this measure. Average standby current was measured to be around 100 nA for the application implemented yielding to a theoretical lifetime of roughly 500 years on a 500 mAh 3V coin cell battery when only operating in standby mode.

BLE 5 brings significant benefits to applications that require large data transmissions occasionally or when OAD is needed. By using the LE 2M PHY the energy utility can be almost doubled when utilizing DLE as shown in table 5.1.

6.2.3. Range & Throughput

The long range PHY variant, LE Coded, that BLE 5 introduced can bring significant benefits if used with caution. The greater range is traded for increased power consumption. Meaning that a device, such as the BellPal watch could utilize this option occasionally and only when necessary. This would mean that the communication would be more robust and giving the application wider covering range. A significant improvement can be seen when connecting over greater distances while devices are in LoS. Results show that the distance can reach up to 1 km while still maintaining connection. It is worth noting that all range tests were performed using output power of 0 dBm by mistake, while the maximum for this hardware platform is +5 dBm. This means that the longest possible range could potentially be even greater for
6. Summary and Conclusion

this device. This distance exceeds the range that has been reported for comparable technologies, as discussed in Section 4.4.

When the test results for the house covering range are observed, it is evident that the LE Coded offers wider range as expected. However, this range is not significant and cannot cover all corners of the house. Obstacles such as thick concrete walls, large electrical devices causing EMI and other interference significantly decreases the quality of the BLE link and does impacts the achievable range. Meaning that the using only long range PHY for application needing full house coverage might not be the most power/range efficient trade-off.

6.3. Conclusion

A literature study and hands-on implementation is summarized in this report aiming on answering the research question and reaching the goals of this project. The literature study included in-depth analysis of BLE architecture and functionality while the implementation part attempted to evaluate and measure benefits of new features included in BLE 5.

While expanding the possibilities of BLE enabled devices, the new functionalities increase its complexity levels considerably much. This additional complexity is not seen from the user perspective in a commercial product, but can cause increased challenges from design and development perspective. This allows for more flexibility and makes the technology attractive for wider range of use cases.

The most extensive improvements of BLE 5 were reported to be doubled transmission speed, quadruple range and eightfold message capacity. The former two characteristics were measured during the implementation phase of the project for a specific application and then the results presented in Chapter 5. It has been shown by the test results that it is possible to achieve almost double data rate using the LE 2M PHY variant. The results however do not reach the quadruple range compared to the default LE 1M PHY. The maximum range was reached using the LE Coded PHY variant with coding scheme as $S=8$, and achieved almost 1 km range or double the range of what is possible using older versions of BLE (LE 1M PHY). This range might be further increased if the hardware platform would support the new maximum TX power of $+20 \text{ dBm}$. The eightfold message capacity is not dependent on implementation or hardware platform and is just an architectural improvement that is evident in all BLE 5 enabled devices. That brings significant benefits to applications that use one way topology of broadcasting such as beacons.

An application such as the BellPal watch would benefit in several different areas by upgrading its wireless communication scheme to BLE 5. As this use case is intended to be in standby mode the majority of its lifetime, thus consuming extremely little current, the combination of decreased power consumption and increased data rate
when using LE 2M PHY variant can be neglected in typical operation and would only decrease its covering range. However using this PHY when performing an OAD would be greatly beneficial, consuming roughly half the power of prior versions of BLE, while completing the transmission in roughly half the time, as can be observed in test results concerning energy utility.

When operating such a device in an open area, the long range feature would at least double the possible range. This however is not a likely situation for this use case, and as it adds roughly double power consumption during transmission, this change would not be optimal on its own. However, by using the long range feature only when a connection is terminated due to weak received signal strength, a long range mode could be used to improve the robustness of connection, trading it off for added power consumption.

The most desired long range scenario of such a device is full-house coverage. This is challenging as the construction and size of houses varies greatly and RF interference is really unpredictable. The tests performed in this project included fairly large house with thick concrete walls providing difficult condition for clean BLE signal. However, the results show that by using the LE Coded PHY it is possible to increase the coverage reasonably much. Obviously this increases the power consumption and when the range is closing in on its limit, the number of retransmitted packages increases significantly causing even more power consumption. The retransmissions could unfortunately not be measured during this project due to equipment limitations. With that said, the long range feature can be beneficial to improve coverage but has to be implemented carefully as it might affect the lifetime of the device.

All the benefits listed here above could theoretically be achieved simultaneously for a specific use case by dynamically switch between PHYs, modifying maximum PDU size, connection and advertising intervals, and other critical connection parameters. This requires delicate design and implementation as using the RSSI value alone is not efficient for this task. The RSSI value needs to be sent frequently between BLE devices to get any consistency as it is very unstable and unreliable, thus consuming a lot of power causing negative effects. This could be solved by introducing a mesh repeaters to a system, or by implementing a low power AI, that would learn to interpret results from RSSI reports optimally based on environment.

When considering low-power short range wireless technologies, the Bluetooth SIG are definitely gaining more prosperity with BLE 5 and Bluetooth Mesh. If these parts of the technology will work seamlessly together, be widely supported by manufacturers and reach all expectations of Bluetooth SIG, this could definitely become the industry standard for low power wireless devices.
6.4. Future works

There are still some significant challenges in bringing BLE to the industry standard of low power wireless technology. Some recommendations and thoughts found during this thesis are listed in this section. These recommendations concern both work to be done by enterprises as well as individual researchers and developers to further understand the effective range of application where BLE could be the optimal wireless technology at hand.

- Evaluate the retransmission rate with respect to distance between devices, thus gaining more inside of actual power increments when utilizing BLE to its range limits.
- Introduce seamless IPv6 over BLE as attempted in [35].
- Investigate how power consumption varies between different BLE IC vendors when performing the same task.
- Propose a method to efficiently gain information dynamically on optimal connection parameters.
- From the market standpoint, investigate IoT readiness of the technology. This can be done by evaluating if the value proposition of the technology compensates for investment cost, development time, usability and maintenance cost to finally gain pervasive adoption within IoT.
Bibliography


[42] Texas Instruments, Over the Air Download (OAD) - BLE5-Stack User’s Guide 1.01.00.00, 2016.


Appendix A.

**Additional Test results**

This chapter includes some extra figures and explanations of test results that are not considered necessary for the report. This is still good additional information about power profiles and detailed description of various parts of the test results.

### A.1. Power profile breakdown

**Figure A.1.: Breakdown of advertising power profiles.**

Figure A.1 shows the power profile of a single advertising event of each PHY variant available for advertising. The profile can be broken down to several steps that are necessary for an advertising event. The Legacy advertisement power profile can be explained as follows:

- **1a** - Pre processing and radio preparation. It takes about 1500 µs with average current draw of 3.1mA

- **2a** - TX on primary advertising channel no. 37, broadcasting advertising data. It takes about 200 µs with average current draw of 9 mA (+5dBm TX power).
A. Additional Test results

- **3a** - RX on primary advertising channel no.37, listening for scan request or connection initiation request. It takes about 140 μs with average current draw of 6.1 mA.

- **4a** - RX to TX transition including channel hopping, as next transmission is performed on another advertising channel. It takes about 200 μs drawing on average 3.3 mA.

- **5a** - TX on primary advertising channel no. 38, broadcasting advertising data. It takes about 200 μs with average current draw of 9 mA (+5dBm TX power).

- **6a** - RX on primary advertising channel no.38, listening for scan request or connection initiation request. It takes about 140 μs with average current draw of 6.1 mA.

- **7a** - RX to TX transition including channel hopping, as next transmission is performed on another advertising channel. It takes about 200 μs drawing on average 3.3 mA.

- **8a** - TX on primary advertising channel no. 39, broadcasting advertising data. It takes about 200 μs with average current draw of 9 mA (+5dBm TX power).

- **9a** - RX on primary advertising channel no.39, listening for scan request or connection initiation request. It takes about 140 μs with average current draw of 6.1 mA.

- **10a** - Radio shutdown and post-processing. It takes about 600 μs with average current draw of 2.5 mA.

Advertisements while using LE Coded PHY automatically uses extended advertising, meaning that it uses the primary advertising channels to transmit a pointer (known as Aux_Ptr) to a secondary advertising channel and then finally transmits the advertising data and listens for scan/connection requests on that same channel. Both profiles b) and c) on Figure A.1 have the same profile descriptions:

- **1b,c** - Pre processing and radio preparation. It takes about 1500 μs with average current draw of 3.1mA

- **2b,c** - TX on primary advertising channel no. 37, broadcasting pointer to a secondary adv. channel. It takes about 560 μs and 1160 μs respectively, with average current draw of 9 mA (+5dBm TX power).

- **3b,c** - TX to TX transition including channel hopping, as next transmission is performed on another advertising channel. It takes about 460 μs for both profiles, drawing on average 2.7 mA.

- **4b,c** - TX on primary advertising channel no. 38, broadcasting pointer to a secondary adv. channel. It takes about 560 μs and 1160 μs respectively, with average current draw of 9 mA (+5dBm TX power).
A. Additional Test results

- 5b,c - TX to TX transition including channel hopping, as next transmission is performed on another advertising channel. It takes about 460 $\mu$s for both profiles, drawing on average 2.7 mA.

- 6b,c - TX on primary advertising channel no. 39, broadcasting pointer to a secondary adv. channel. It takes about 560 $\mu$s and 1160 $\mu$s respectively, with average current draw of 9 mA (+5dBm TX power).

- 7b,c - TX to TX transition including channel hopping, as next transmission is performed on a secondary advertising channel. It takes about 460 $\mu$s for both profiles, drawing on average 2.7 mA.

- 8b,c - TX on a random secondary advertising channel selected by the frequency hopping scheme, broadcasting advertising data. It takes about 740 $\mu$s and 1820 $\mu$s respectively, with average current draw of 9 mA (+5dBm TX power).

- 9b,c - RX on the same secondary advertising channel as step 8, listening for scan request or connection initiation request. It takes about 500 $\mu$s for both, with average current draw of 6.1 mA.

- 10b,c - Radio shutdown and post-processing. It takes about 600 $\mu$s with average current draw of 2.5 mA.