VAASAN AMMATTIKORKEAKOULU
UNIVERSITY OF APPLIED SCIENCES

Robin Snellman

WIRELESS COMMUNICATION USING BLE

Technology and Communication
2021

VAASAN AMMATTIKORKEAKOULU
UNIVERSITY OF APPLIED SCIENCES
Information Technology

ABSTRACT

Author	Robin Snellman
Title	Wireless Communication Using BLE
Year	2021
Language	English
Pages	42 + 1 Appendix
Name of Supervisor	Gao Chao

Wireless technology is becoming more popular in the industry each year. A few advantages of wireless communication are flexibility, mobility, scalability and wireless. Because of the advantages, the client company wants to implement such a technology in a future product.

In the theory part, different short range wireless technologies are researched, to find the most suitable one for the client company. The literature sources used are technical specifications, books, research papers and blog posts. The practical part is an evaluation of the chosen technology and hardware that supports the technology. The evaluation was necessary to ensure that the technology and hardware is good enough for the intended purpose.

The tested device is the BlueNRG-M2SA module, which is manufactured by ST Microelectronics. The application code used in the testing was an example code provided by the manufacturer that was modified to provide data of interest. The conclusion of the research was that BLE is a good technology to use for this purpose. The test showed that BLE and the tested hardware is a good option to be used in a future product.

Keywords Wireless communication, Bluetooth, BLE

VAASAN AMMATTIKORKEAKOULU
UNIVERSITY OF APPLIED SCIENCES
Information Technology

ABSTRAKT

Författare	Robin Snellman
Titel	Trådlös kommunikation med BLE
År	2021
Språk	Engelska
Sidantal	42 + 1 Bilaga
Handledare	Gao Chao

Trådlös kommunikation blir vanligare inom industrin varje år. Några fördelar med trådlös kommunikation är flexibilitet, mobilitet, skalbarhet och trådlös. Tack vare fördelarna som finns, ville klientföretaget utforska möjligheten att använda en sådan teknologi i en framtida produkt.

I teoridelen undersöks olika trådlösa teknologier avsedda för kortdistanskommunikation; för att hitta den som passar bäst för detta syfte. Literaturkällorna är tekniska specifikationer, böcker, forskningsrapporter och blogginlägg. Den praktiska delen består av en utvärdering av den valda teknologin och hårdvaran som stöder teknologin. Utvärderingen var nödvändig för att försäkra att teknologin och hårdvaran uppfyller klientföretagets krav.

Den valda Bluetooth-enheten, vilken också testades, var BlueNRG-M2SA, som tillverkas av ST Microelectronics. Applikationskoden som användes under testen var en exempelkod av tillverkaren, den modifierades för att få ut intressant data. Slutsatsen av undersökningen var att BLE är den mest lämpliga teknologin att använda i det här fallet. Baserat på testen konstaterades att BLE och den valda hårdvaran är redo att användas i en framtida produkt.

Nyckelord Trådlös kommunikation, Bluetooth, BLE

CONTENTS

ABSTRACT

ABSTRAKT

1 INTRODUCTION 10

2 RESEARCH 11

2.1 Bluetooth 11

2.1.1 Interference 13

2.1.2 Range 13

2.1.3 Security 14

2.1.4 Available Hardware 15

2.2 WirelessHART 15

2.2.1 Interference 17

2.2.2 Range 18

2.2.3 Throughput 19

2.2.4 Security 19

2.2.5 Available Hardware 20

2.3 ZigBee 21

2.3.1 Devices 21

2.3.2 Interference 22

2.3.3 Range 23

2.3.4 Security 24

2.3.5 Bit rate 25

2.3.6 Power Consumption 25

2.3.7 Available Hardware 25

2.4 Research Summary and Conclusion 25

2.5 Hardware Research 27

3 HARDWARE AND TECHNOOLGY EVALUATION 28

3.1 Brief Explanation of the BLE Stack 28

3.2 Testing code 29

3.3 Testing and Result 31

3.4 Result analysis 35
3.5 Problems 37
4 SUMMARY 39
REFERENCES 40

APPENDIX

LIST OF FIGURES AND TABLES

Figure 1. Wireless enabled module and related ecosystem. 10

Figure 2. Bluetooth piconet. 12

Figure 3. Bluetooth mesh network. 12

Figure 4. WHART mesh network. 16

Figure 5. Interference in 2.4 GHz frequency band. 17

Figure 6. Greater distance with mesh. 18

Figure 7. Object avoidance and redundancy in mesh. 18

Figure 8. The ZigBee superframe structure. 23

Figure 9. ZigBee Star, Tree and Mesh topology. 23

Figure 10. BlueNRG-M2SA. 27

Figure 11. BLE stack. 29

Figure 12. Code snippet from the master device. 30

Figure 13. Sample output from C# application. 31

Figure 14. Object setup in the corridor. 32

Figure 15. Corridor, without object test result. 32

Figure 16. Corridor, with object test result. 33

Figure 17. Outside, without object test result. 33

Figure 18. Outside, with object test result. 34

Figure 19. Ventilation room. 34

Figure 20. Ventilation room test result. 35

Table 1. Research summary. 25

Table 2. BlueNRG-M2SA characteristics. 27

Table 3. Distance of disconnection. 36

LIST OF APPENDICES

APPENDIX 1. Flow chart of the master device when it receives data.

LIST OF ABBREVIATIONS AND ACRONYMS

AES	Advanced Encryption Standard
ATT	Attribute Protocol
BER	Bit Error Rate
BLE	Bluetooth Low Energy
BR/EDR	Basic Rate / Enhanced Data Rate
CAP	Contention Access Period
CFP	Contention Free Period
CRC	Cyclic Redundancy Check
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
dBm	Decibel-milliwatts
EOL	End-of-Life
FHSS	Frequency-Hopping Spread Spectrum
GAP	Generic Access Profile
GATT	Generic Attribute Profile
GFSK	Gaussian Frequency Shift Keying
GHz	Gigahertz
GTS	Guaranteed Time Slot
HART	Highway Access Remote Transducer Protocol
HCI	Host Controller Interface
IEEE	Institute of Electrical and Electronics Engineers

I/O	Input/Output
ISM	Industrial, Scientific and Medical
Kbps	Kilobits per second
L2CAP	Logical Link Control and Adaptation Layer Protocol
LL	Link Layer
MAC	Medium Access Control
mAh	Milliampere hours
Mbps	Megabits per second
MHz	Megahertz
MIC	Message Integrity Check
MITM	Man-In-The-Middle
NFC	Near Field Communication
OOB	Out of Band
PAN	Personal Area Network
PHY	Physical layer
RAM	Random Access Memory
RSSI	Received Signal Strength Indication
RX	Receive
SM	Security Manager
TDMA	Time Division Multiple Access
TX	Transmit
USB	Universal Serial Bus

1 INTRODUCTION

This project was commissioned by a calibration company that sees potential in implementing a wireless technology in a future device. The report shows the research that was done to find the most suitable short-range wireless technology to be used in a calibrator, as well as choosing the right technology and hardware. The process of testing the technology and the chosen hardware is also shown, together with the test analysis.

Figure 1 shows the calibrator that is currently being developed as Wireless enabled module. It will communicate with either a calibrator or a mobile application, this communication makes up Link 1. Link 2 is used when the mobile application or calibrator communicates with a calibration management software. The aim of the project was to find the technology to be used in Link 1, and hardware to be used in the wireless enabled module. Therefore, Link 2 is out of scope of this report.

The wireless enabled module will send small packets irregularly, to be processed and shown on the calibrator or in the mobile application. Because of the irregular communication, the ability to sleep is wanted to reduce the power consumption. The communication over Link 1 is not going to be time critical.

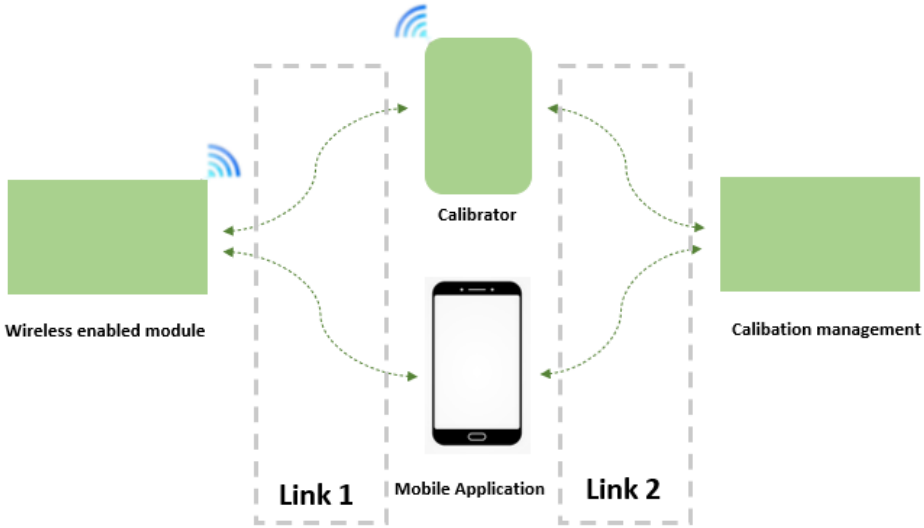

Figure 1. Wireless enabled module and related ecosystem.

2 RESEARCH

The researched technologies are Bluetooth, ZigBee and WirelessHART. The aim of the research was to find the most suitable technology to use in the future device, according to the following criteria:

- Energy consumption. The device is expected to run at least two workdays on a 4200 mAh battery.
- Sufficient data rate, neither too low nor too high. The maximum data rate of the module is specified as 400 kbps.
- Good security.
    - Authentication: Ensures that only wanted devices connects.
    - Integrity: Ensures that the received data is not changed.
    - Confidentiality: Ensures that the data is not readable by an unauthorized third party.
- Sufficient range. The estimated use case is maximum 10 m.

2.1 Bluetooth

Bluetooth is a wireless technology designed for short distance. It was introduced in 1989 with the first consumer device launched in 1999 /1,2/. The Bluetooth standard is maintained by the Bluetooth Special Interest Group (SIG), consisting of over 36,000 companies /3/. Bluetooth is designed to be backwards compatible with older Bluetooth versions, meaning a device using the newest Bluetooth version can communicate with a device that uses an older version. Bluetooth has five major versions; versions one to three are referred to as Bluetooth classic and versions four and five are called Bluetooth Low Energy.

Initially Bluetooth only supported piconets, where point-to-point connections are used to communicate between two devices. Figure 2 shows how a piconet looks like, where there is one central device , called master, connected to all other devices in the network, called slaves. Since BLE was launched, mesh networks with up to 32,767 nodes has been possible /4/. Figure 3 illustrates a mesh network, where the nodes are interconnected. This enables messages to be forwarded by intermediate devices to its destination, which makes it possible for two devices to

communicate even though they are not in range of each other. Devices work both as an intermediate device and a node that generate its own traffic.

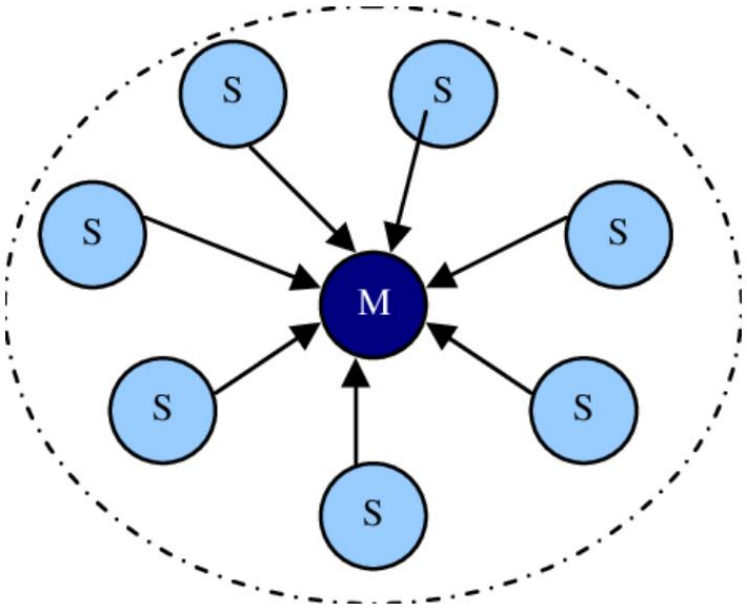

Figure 2. Bluetooth piconet /5/.

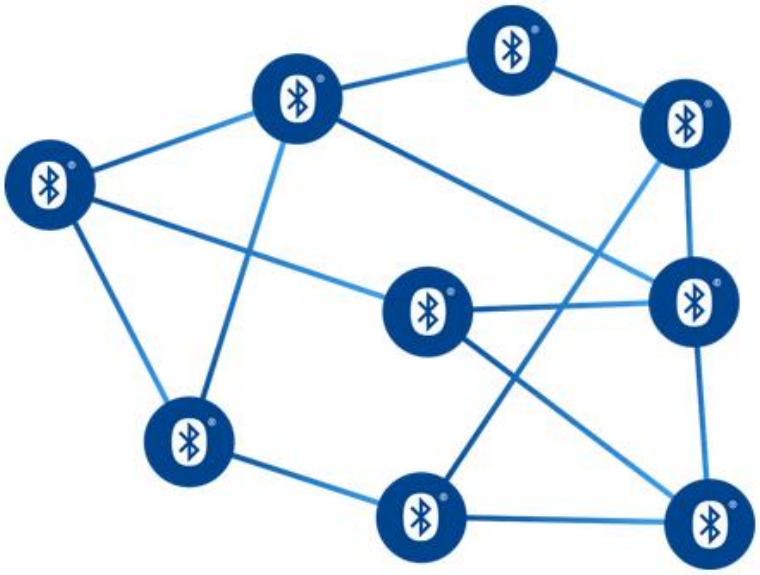

Figure 3. Bluetooth mesh network /6/.

2.1.1 Interference

Bluetooth utilizes the free ISM radio spectrum at 2.4 GHz. This is shared by several short distance wireless technologies, for example, Wi-Fi, ZigBee and WHART. The use of shared frequency band makes it prone to interference, this is shown in Figure 5. To prevent that, Bluetooth uses small packets that are transferred fast. When compared to low-power mesh technologies that uses the 802.15.4 standard, Bluetooth typically has half the packet size and is transmitted four times faster /7/.

Bluetooth also uses adaptive frequency hopping (AFH) to avoid interference, which is a form of frequency-hopping spread spectrum (FHSS). This divides the frequency spectrum into smaller channels and hops between the channels, using a predetermined hopping sequence, when transmitting data. Bluetooth classic, also referred to as BR/EDR, uses 79 channels, each one MHz, while BLE uses 40 two MHz channels. Channels that are used a lot or are very noisy, are tracked and avoided, called blacklisting. /7/

To avoid loss of data if interference occurs, packet acknowledgement is implemented. When a packet is successfully received, the receiver replies with an acknowledgement. If the transmitter does not receive an acknowledgement in a specified time, it assumes the packet or part of the packet was lost and retransmits the whole packet. /7/

In mesh networks, waiting for acknowledgements is not optimal. Since there might be several hundred receivers, it would be very time-consuming to wait for all the acknowledgements. Therefore, BLE mesh offers a feature called automatic retransmission where the transmitter rapidly sends multiple copies of the message. With this feature, the probability of successfully receipt is dramatically increased. /7/

2.1.2 Range

The range in wireless communication is determined by how far away a receiver can be from a transmitter and still interpret the received signal. The range depends on several factors; radio spectrum, modulation technique, receiver sensitivity,

transmit power, antenna gain and path loss /8/. BLE 5.0 provides longer range, up to 400 m, compared to the range of up to 100 m for BLE 4.0 and BR/EDR /9/.

The modulation technique used, commonly called PHY, greatly affects the range. Bluetooth uses the GFSK modulation scheme where a central frequency, frequency carrier, is selected. The frequency is shifted up or down from the frequency carrier with a frequency deviation to represent a 1 or a 0. Upshift represents a 1 and downshift represents a 0. Before Bluetooth 5, only 1M PHY was available, where the frequency deviation 185 kHz is used. In 2M PHY, which was introduced in Bluetooth 5, the frequency deviation is 370 kHz, this allows for higher throughput and less radio time at the expense of the range. Bluetooth 5 also introduced Coded PHY, which enables two times the distance of 1M PHY with a throughput of 500 kbps or four times the distance with a throughput of 125 kbps. /8/

The more sensitive the receiver is, the greater the range is going to be. Bluetooth devices must be able to receive signals of -70 dBm with a maximum BER of 0.1%. However, this is usually exceeded and signals with less power are received. /8/

The transmit power used in Bluetooth is between -20 dBm and +20 dBm and might be a tradeoff between range and power consumption. Path loss is the signal attenuation in air, which happens constantly with wireless signals, but the path loss is increased when there are obstacles in the signal path or when the signal is reflected of an object. The last factor, the antenna gain tells how well the antenna directs a signal in a certain direction, which intensifies the signal strength in that direction. Bluetooth antennas typically achieves a gain of -10 dBi to +10 dBi, this equals to 10% to 1000% of the original signal /27/. /8/

2.1.3 Security

Bluetooth has a security model consisting of the following five distinct features: /10/

- Pairing: A process for creating the shared secret key(s).
- Bonding: Storing of the shared secret key(s) for use in subsequent connections to form a trusted device pair.

- Device authentication: Verifies that the two connected devices have the same key.
- Encryption: Message confidentiality.
- Message integrity: Protects against message forgery.

There are four association models used to pair devices. The I/O capabilities of the devices determine what association model is used:

- Numeric Comparison: Both devices have I/O capabilities
- Just Works: One or both devices does not have I/O capabilities.
- Out of Band: The two devices exchange the connection information, not using Bluetooth.
- Passkey Entry: One device has input capabilities and the other has output capabilities.

2.1.4 Available Hardware

There are two different Bluetooth chips available, single-mode and dual-mode. Dual-mode chips integrates both BLE and BR/EDR and single-mode chips only integrates one of them. Bluetooth hardware is available from many manufacturers and they are usually very inexpensive. Most of them are certified by required authorities. Bluetooth is also widely integrated in smartphones today, which is a big benefit. An example BLE module is BlueNRG-M2SA. This has a current consumption of 10.73 mA during TX using +4 dBm transmit power, with +8 dBm it is 14.78 mA. During RX, 7.55 mA is consumed and during sleep mode 0.9 µA /23/.

2.2 WirelessHART

The HART specification is owned by FieldComm Group, who oversees the development of the technology. WirelessHART, hereby referred to as WHART, is designed to add wireless capabilities to the already established HART technology. Thus, it must be compatible with the wired HART protocol. It is designed to be a mesh network, where every device routes traffic through the network. This way devices do not need to communicate directly with the destination but can forward messages to the closest device. This leads to extended network range, it also provides redundancy, which is important in industrial environments. Figure 7 shows how mesh networks are redundant. WHART is self-configurable and self-healing,

which makes it easy to use. It includes the PHY of the IEEE 802.15.4 standard. Figure 4 shows an example setup of a WHART network.

A WHART network includes the following elements:

- Field devices: Devices that can be connected as an adapter to the HART-enabled sensors in a plant, or it can be integrated into the sensor. They are interconnected, which provides redundancy.
- Gateways: Devices that enable communication between the field devices and the host application. They are connected to the backbone network in the plant.
- Network Manager: An application that is responsible for network configuration, schedule communications between devices, route determination and network health monitoring. It can be integrated into a host application, gateway or process automation controller, or it can be a standalone device.
- Security Manager: An application that manages the security resources and monitors the security status in the network. Manages the encryption keys.
- Host Application: Receives the data from the plant and presents it to the user.

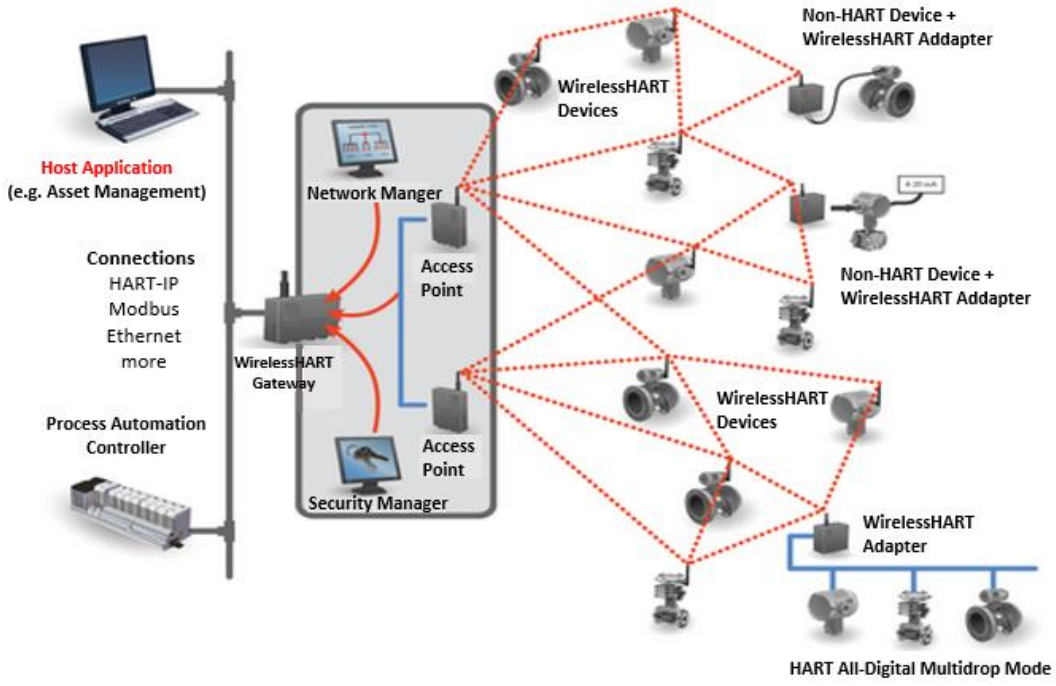

Figure 4. WHART mesh network /12/.

2.2.1 Interference

Like Bluetooth and ZigBee, WHART also uses the ISM radio band. Figure 5 shows how the different technologies using 2.4 GHz interfere with each other. For example, IEEE 802.15.4 channel 11 uses the frequency spectrum 2404 to 2406 MHz. The same frequency spectrum is used by BLE channels 0 and 1, Wi-Fi channel 1 and third, fourth and fifth channels in BR/EDR.

To enable co-existence, WHART uses FHSS on its 16 channels, low power and assigned time slots of 10ms with TDMA. In TDMA devices communicate in their own time slot, this way, not all devices communicate simultaneously. The risk is reduced even more by blacklisting channels that have a high probability of interference. Mesh networking further reduces the risk of errors caused by interference. /13/

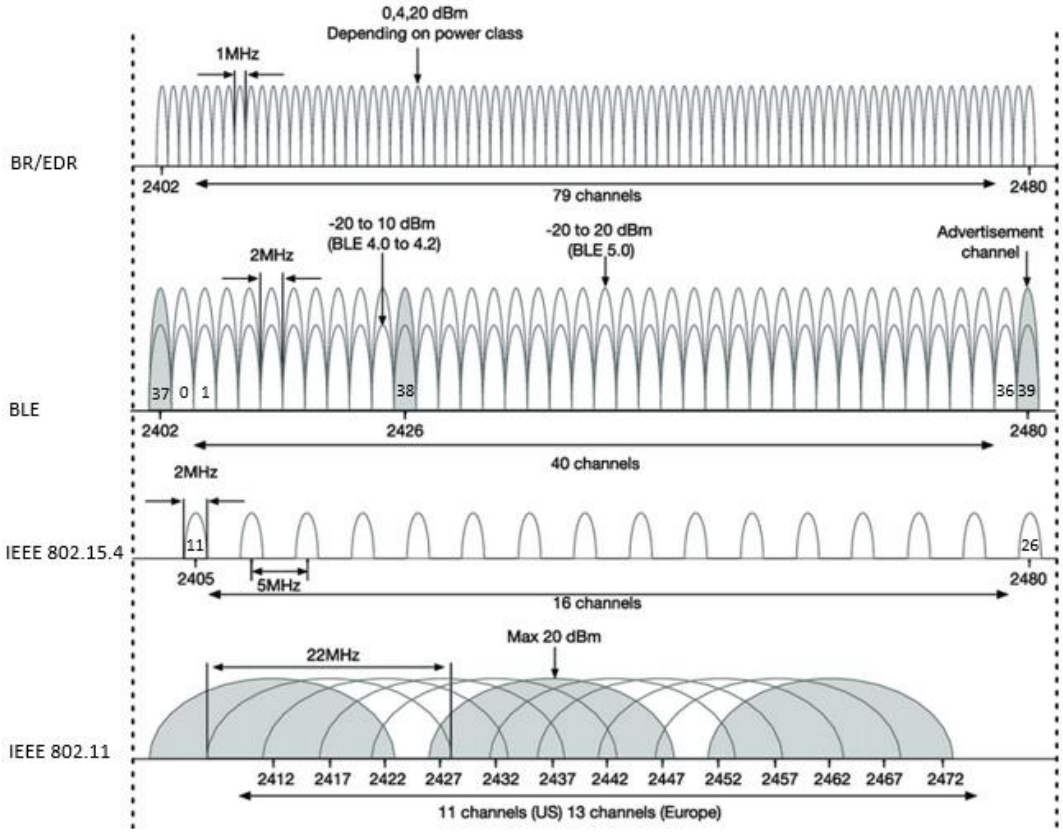

Figure 5. Interference in 2.4 GHz frequency band /30 (modified)/.

2.2.2 Range

Since WHART is a mesh network technology, the range is not necessarily determined by how far the signal can travel line of sight. However, the line-of-sight range depends on the same factors as explained in Chapter 2.1.2, it is estimated to be approximately 225m. Mesh networking enables a message to be sent a great distance by hopping between nodes in a network, at every hop, the signal is sent out with full transmit power. There can be up to 250 nodes per network. Figure 6 illustrates how the range is extended in mesh networks. Figure 7 shows how the use of mesh topology also reduces the impact of an object between two nodes. If the transmitter does not receive an acknowledgement of the transmitted data, it can be re-transmitted using another route.

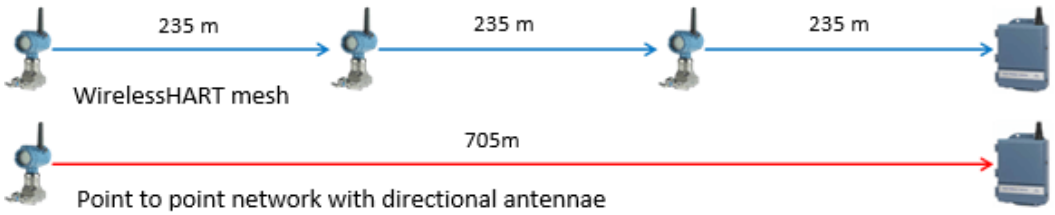

Figure 6. Greater distance with mesh /14 (modified)/.

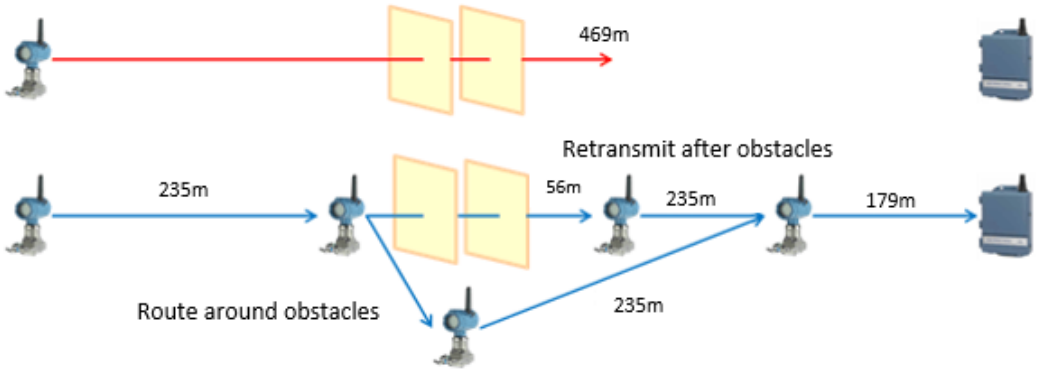

Figure 7. Object avoidance and redundancy in mesh /14/.

2.2.3 Throughput

Throughput is defined as number of correctly received bits in a fixed time. In mesh networks, the throughput is dependent on how many nodes are in the network. The more nodes, the less time each node is able to transmit, because of TDMA. This leads to less throughput the more nodes there are in a network. If two networks are so close that they create interference to one other, they share the available channels to avoid interfering with each other. This ultimately leads to less throughput. Since WHART uses the PHY and data link layer from the IEEE802.15.4 standard, the maximum bit rate is 250 kbps. The throughput is not as high as the bit rate, since there are usually some bits that are not received correctly.

2.2.4 Security

Because of the level of sensitivity data can have in an industrial environment, the security is of high priority. The security in WHART is always on and cannot be disabled. However, it was designed in a way that it would provide ease-of-use. Security in WHART is often divided into two categories, Data Protection and Network Protection.

Data Protection, also called confidentiality, maintains the privacy and integrity of the messages that are sent over the network. To ensure that only the wanted recipient can read the messages, WHART provides an AES-128-bit encryption of all data transmitted. Individual session keys and a common network encryption key are used. The network key is shared by all the devices in a network.

To keep the transmitted data private during the joining process, there is a separate 128-bit join encryption key. This is also an authentication to the SM, which confirms that the device belongs to the network. To enhance security, this key is treated separately from the other keys. Depending on the user security policies, the join key can be a common key in the network, or it can be unique to each device.

An integrity check is calculated and added to each packet, to ensure that the message has not been changed during the transmission while also protecting the routing information. The integrity check together with the information used to create

the integrity check, plus sender/receiver unique session key that encrypts/decrypts the message, ensures that the source of the message has not been changed.

Network Protection makes sure the network is functional, even during an attack, also called availability. This is achieved by techniques to provide Authentication, Authorization and Attack Detection.

To ensure security in a wireless network all devices in the network must remain secure. To achieve this, the gateway and the field devices joining the network are configured to control which devices can access the network. Using an authentication process, the WHART gateway negotiates with all devices that joins the network to confirm that they are legitimate. This negotiation traffic, like all other traffic, is encrypted end-to-end.

In each WHART network there is one **Security Manager**. However, the SM can service more than one network at the same time, it may even run other applications simultaneously. Its responsibility is to generate, store and manage the different encryption keys. The Network Manager needs the Join, Network and Session keys for authentication and message encryption, these are provided by the SM. It also provides the Join keys to the Field Devices.

2.2.5 Available Hardware

There are very few manufacturers that make WHART hardware, and they are harder to find than Bluetooth and ZigBee. They are also more expensive, the WHART modules are up to ten times more expensive than Bluetooth and ZigBee devices. The hardware is certified by required authorities, which speeds up time to market. An example WHART device is LTP5902IPC-WHMA1A2. This device has a current consumption of 9.7 mA at TX with +8 dBm Tx power and 4.5 mA at RX. No sleep mode is available in WHART /28/.

2.3 ZigBee

ZigBee is designed to be a low-cost, low-power, two-way, wireless communication standard. It is intended for control systems, for example, home automation systems. The standard is maintained by the ZigBee Alliance, which consists of several companies. It supports star, tree and mesh topologies, these topologies can be seen in Figure 9. The mesh networks are self-forming and self-healing, if a route to a node fails, another route is found to reach that node.

ZigBee is built on the MAC and PHY layers defined by the IEEE 802.15.4 standard. It provides mechanisms for network discovery, forming and joining networks, channel changing and interference detection on channels, but not all mechanisms are implemented in ZigBee. IEEE 802.15.4 does not specify anything regarding multi-hop communications, address assignment, or application-level interoperability. Hence, ZigBee has added a network layer capable of mesh networking, a security layer to handle complex security situations and an application layer for interoperable application profiles. /15, 16/

2.3.1 Devices

ZigBee networks include the following three devices: /16/

- Coordinator:
    - Forms a network.
    - Chooses the network ID, also known as PAN ID.
    - Acts as the Trust Center.
    - Acts as router for mesh routing.
    - Only one coordinator per network
- Router:
    - Participates in routing and discovers and maintains routes.
    - If enabled, the router can help to allow devices to join the network.
    - Stores packets sent to their sleeping children.
- End Device:
    - Polls its parent for packets that the parent has stored.
    - Finding a new parent if its parent becomes unreachable.
    - Saves energy by sleeping when not used by the application.

2.3.2 Interference

As previously mentioned, ZigBee also uses the free ISM radio band, which is shown in Figure 5. Apart from the 2.4 GHz band that is used around the world, it also uses the frequency bands 868 MHz in Europe and 915 MHz in the USA and Australia. Unlike the other two technologies, ZigBee does not use frequency hopping to avoid collision, only one channel is used per network, even though the 2.4 GHz band has 16 channels, each 2 MHz wide and 915 MHz has 10 channels, also 2MHz wide. Frequency band 868 MHz has only one channel. /17/

The IEEE 802.15.4 standard specifies a CSMA/CA MAC protocol to help avoid collision. The communication between the end device and the coordinator happens either through a non-beacon-enabled mode, which is based on un-slotted CSMA/CA, or through a superframe structure, which can be seen in Figure 8. The superframe starts with a beacon, which is used to synchronize the clocks of the devices in the network. After the beacon comes the access periods, CAP and CFP. /18/

During the CAP, nodes access the channel using CSMA/CA. Using this method, a node that is ready to send data makes sure that there is no incoming traffic by turning on its receiver to see if a signal is received. If a signal is received, the node waits for a random amount of time before trying again, otherwise it will start sending. The nodes communicating in the CAP needs to make sure the transmission is completed before the CFP period starts. /18/

CFP uses GTS to provide time-critical applications with a specified amount of time in each superframe to communicate. This can be real-time or life-critical applications. Up to seven time slots are allocated by the coordinator in each superframe. /18/

During the active period, which consists of beacon period, CAP and CFP, the nodes need to stay awake. But after that, they can go to sleep, this period is called the inactive period. /18/

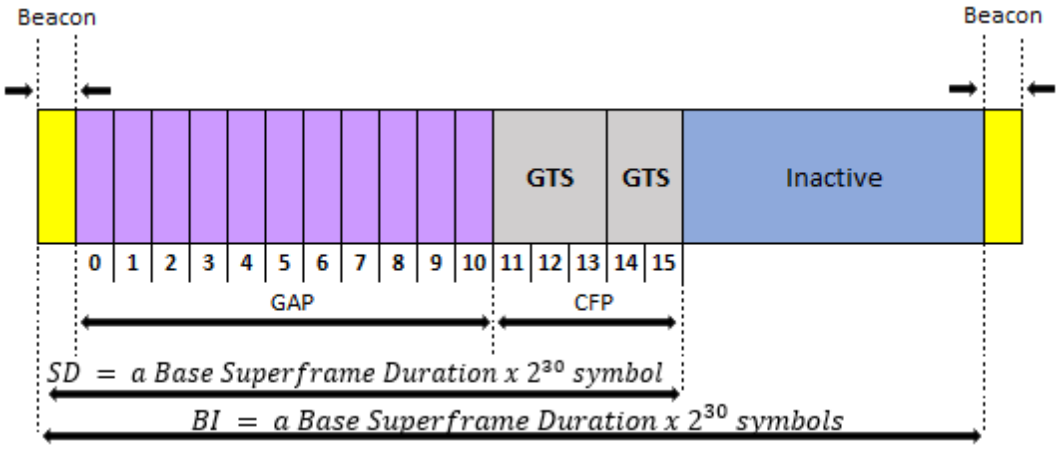

Figure 8. The ZigBee superframe structure /18 (modified)/.

2.3.3 Range

The range of ZigBee depends on the topology used. If the star topology is used, the range is going to be limited to the line-of-sight range, while tree and mesh topology offers extended range, since intermediate devices enable multi-hopping. The line-of-sight range varies depending on the source. According to ZigBee Alliance the line-of-sight range can be 300+ meters and the range achieved indoors is 75–100 meters /17/. Figure 9 shows the different topologies in ZigBee and the placement of the different devices in a network.

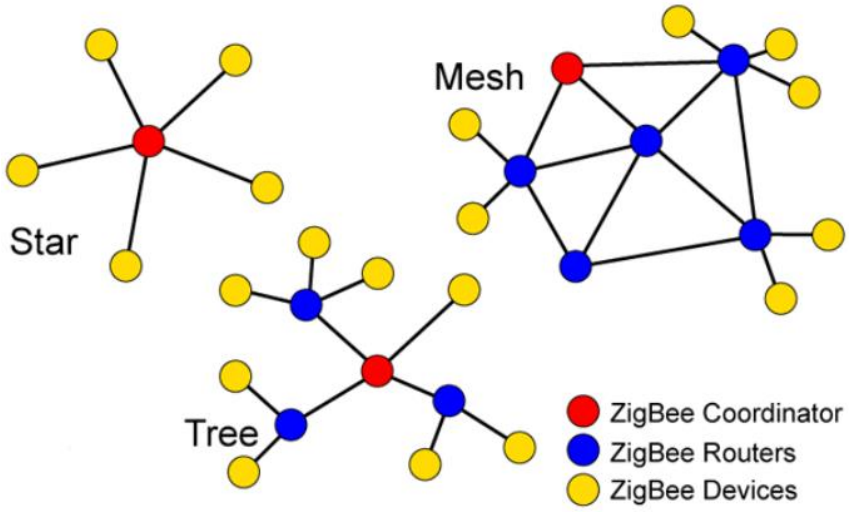

Figure 9. ZigBee Star, Tree and Mesh topology /19/.

2.3.4 Security

In ZigBee, security is not mandatory, this can make the network vulnerable. For example, encryption can be turned off, which enables anyone to read the messages sent in the network. The encryption keys used are 128-bit AES. When a device joins the network, it gets the network key and can encrypt and decrypt its messages. The encryption key can be safely renewed if the old key is compromised. Additionally, nodes can use a link key, which encrypt unicast communication between devices, or an application-layer key to encrypt the communications further. The application-layer keys and the link keys hide the communication from other nodes in the network. /16, 20/

ZigBee also offers the permit joining flag. This is relevant to the coordinator and the routers, which can have children connected to them. The joining flag enables or disables nodes from joining the network, or it can be enabled for a number of seconds and then disabled. This helps keeping unwanted nodes out of the network. Usually after a network is set up, the installer wants to control when new nodes join the network. /16/

When a node wants to join the network, it goes through an authentication process. This allows the trust center to see if the device is authorized to join the network. The trust center is in charge of device authentication. When a node is authenticated, it receives the network encryption key, and it can communicate with other nodes in the network. If the authentication is not successful, the parent tells the node to leave. /16/

Another feature of ZigBee is the frame authentication. This makes sure that potential rogue nodes cannot alter or transmit false messages in the network. In a security enabled network, the MIC field in the network layer makes sure that the data has not been altered during transmission. Such a field is also available on the application layer. This field is also generated with the 128-bit security key. The MAC layer data is checked with the Frame Checksum. /16/

2.3.5 Bit rate

The bit rate tells how fast bits can be transmitted; this is at the physical layer. Because ZigBee operates on different frequency bands, it also offers different bit rates. The worldwide 2.4 GHz frequency band offers a bit rate of 250 kbps, the 915 MHz frequency band offers 40 kbps, while 20 kbps can be achieved at 868 MHz.

2.3.6 Power Consumption

The different devices consume different amount of power. The end devices consume the least amount of power since it sleeps most of the time. The end device is also the only device that can be powered with batteries. The coordinator and routers are always on and require more power and are therefore connected straight to a power outlet. For example, a lightbulb in a home automation system, that could be either a router or a coordinator, is powered by the electricity in the house, while the end device, the remote controller that controls the light bulb, is a handheld device powered by a battery. An example ZigBee device is XBEE 3. This is an end device with a current consumption of 40 mA at TX with +8 dBm TX power, 17 mA at RX and 2 µA at sleep mode /29/.

2.3.7 Available Hardware

There are many manufacturers that make hardware that implements ZigBee and most of them are very inexpensive. Most of them are certified by required authorities, which speeds up time to market.

2.4 Research Summary and Conclusion

Table 1. Research summary.

Characteristic	BLE and BR/EDR	WHART	ZigBee
Bit rate	- 0.125, 0.5, 1 or 2 Mbps	- 250 kbps	- 20, 40 or 250 kbps
Range	- 400 meters	- 225 meters	- 300+ meters
Security	- 128/256-bit encryption keys	- 128-bit encryption keys	- 128/256-bit encryption keys

	- CRC and MIC - Four authentication methods between master and slave.	- CRC and MIC - Encrypted authentication process with the gateway.	- FCS and MIC - Authentication process with the trust center.
Interference	- AFH on 40 or 79 channels - TDMA - 2.4 GHz	- FHSS on 16 channels - TDMA - 2.4 GHz	- CSMA/CA. GTS optional - 2.4GHz, 868 and 915MHz
Power Consumption	- Low transmit current - Sleep mode available	- Lowest transmit current - No sleep mode	- Low transmit current - Sleep mode available

Based on the research, which is summarized in Table 1, it is clear that BLE is the most suitable technology to use in this project. The decision was made based on the following factors:

- The power consumption in BLE is less than in ZigBee. It is more than in WHART, but WHART does not have sleep mode.
- BLE lets the developer implement the data rate needed depending on the modulation used.
- The price of BLE and ZigBee chips/modules are significantly cheaper than WHART.
- BLE efficiently overcomes interference.
- BLE is widely used and integrated into many devices already, so no external dongle is needed on the phone side.

The reason why Wi-Fi was not considered is that the data rate and power consumption is too high. Since the plan is to have the calibration module connected to a phone and not to an industrial network, there is not enough advantages to use Wi-Fi.

2.5 Hardware Research

An important factor in the project was the time to market. This almost unavoidably narrowed down the search to only BLE modules, excluding BLE chips from consideration. However, chips were also researched for reference. A module is a complete circuitry of various components to make a chip function, whereas a chip alone allows developers to make the surrounding circuitry themselves.

Table 2 shows the characteristics of BlueNRG-M2SA, the module that was considered to be the most suitable. Beyond the characteristics shown in the table, the client company already has experience of other products from this manufacturer, which is a big advantage. Figure 10 shows the BlueNRG-M2SA module.

Table 2. BlueNRG-M2SA characteristics /22, 23/.

BLE protocol	Single mode 5.2
Memory	256 kb flash and 24 kb RAM
Current consumption	14.78 mA at TX using +8 dBm, 7.55 mA at RX and 0.9 µA at sleep
Transceiver	Max transmit power: +8 dBm RX sensitivity: -88 dBm
Estimated EOL	2029
Price	< 6€ /module, if buying 100+

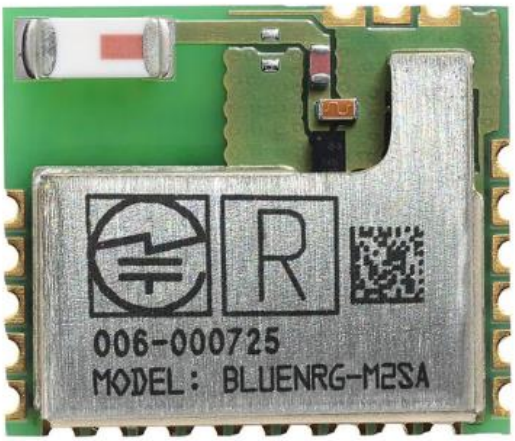

Figure 10. BlueNRG-M2SA /22/.

3 HARDWARE AND TECHNOOLGY EVALUATION

An evaluation phase was necessary to know if BLE and the chosen module is a good option for the intended purpose. The tests were carried out indoors and outdoors. The indoor tests were done both in a 25-meter-long corridor and in a ventilation room, the ventilation room was supposed to represent an industrial environment with a lot of metal and machinery close by. The outdoor test was carried out in a parking lot that was 100+ meters long. Two different cases were tested, one where the signal was not blocked by any object and another where the signal was blocked by an object.

3.1 Brief Explanation of the BLE Stack

BLE consists of a suite of protocols, each of them does different tasks and together they enable BLE communication. Figure 11 shows the BLE stack, which is the software implementation of the BLE protocol suite. The protocols GAP through L2CAP make up the host part of the stack, whereas HCI, LL and PHY is the controller part, the application layer is on top of the host part.

The GAP defines how BLE devices are advertised and how devices can communicate with each other. There are four GAP roles: broadcaster, observer, peripheral and central. The broadcaster advertises data packets without connecting to another device and the observer listens to those packets. The peripheral device sends advertisements so central devices can establish a connection to it. Once a connection is established between a central and a peripheral device, they can exchange data packets. /26/

Like GAP, GATT also defines certain roles: client and server. The client requests to read or write attributes that the server has. The server on the other hand stores attributes and exposes those attributes to requesting clients. It is also possible for the server to expose an attribute without a request from a client. The attributes are stored on the server using the ATT protocol. /26/

The SM´s task is to manage pairing, authentication and encryption between devices. L2CAP segments, encapsulates and reassembles packets, it also takes care of Quality of Service. The HCI provides a way for the host and the controller to interact with each other via a serial interface. The LL interacts with the PHY and it takes care of the CRC generation and verification, it discards packets with wrong CRC. The PHY layer takes care of the analog communication between two devices. It transforms electrical signals to analog format and vice versa.

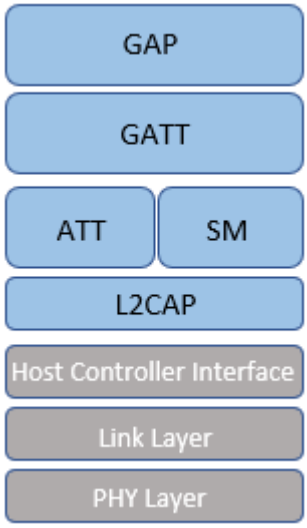

Figure 11. BLE stack /25/.

3.2 Testing code

By default, all packets in BLE are acknowledged at LL and all unacknowledged packets are retransmitted until it is successfully received. Since all faulty packets are dropped at the LL and not forwarded to the upper layers, the application layer will not see any packet loss, only longer delay between packets /25/. In very rare cases, the CRC can fail and cause faulty packets to be forwarded to the application layer. However, this can be handled in the application layer itself and is not a concern in these tests. Because no packets are dropped, it is interesting to test how far away the receiver can be from the transmitter and still receive packets fast enough, and at what distance the connection is broken. The code used in the testing was based on an example code that is provided by ST Microelectronics as an evaluation code for this hardware. The example code was modified to not include unnecessary parts and some features were added.

The slave, also called the transmitter, was programmed to expose a service that continuously send packets with a size of 248 bytes, without any delay between packets. The last two bytes of the packet were used as a packet counter, which started from 0 and went up to 499 before resetting, so one counter cycle consisted of 500 packets. The ATT´s notification feature was used to send data to the master. The notifications do not use acknowledgements at the application layer, so in that sense the communication was unidirectional.

The master, also called receiver, used the packet counter to get the time it took to transmit 500 packets and that value was used to calculate the goodput, which is the throughput at application layer. If the master had to wait 10 seconds or longer to receive a packet, the connection is considered broken, and the master disconnects from the slave. When the 500th packet was received, the calculated values were printed to the serial port together with the signal strength, the RSSI. The code snippet in Figure 12 shows what the master does when it receives a notification from the slave. The variable *NUM_PACKETS* is defined as 500 and the variable *packets* is a packet counter on the master side that is synchronized with the packet counter in the received data. The variable *count* was only used to display how many outputs have been printed. The flow chart of the master code is shown in Appendix 1.

```
if(hci_read_rssi(Connection_Handle, &rssi) != BLE_STATUS_SUCCESS)   printf("RSSI FAIL!!");
RSSI += rssi;

if(packets == 0){
    time = Clock_Time();    //System time when first packet is received
}
packets++;  //Increase packet counter

if(packets == NUM_PACKETS){     //If it is the 500th packet

  time2 = Clock_Time(); //System time when last packet is received
  tClockTime diff = time2-time;     //Time difference from between first and last packets
  //Print to the serial port
  printf("\r\n%d    Time: %d ms    Goodput: %d kbps   RSSI: %ld\r\n",
             count++, (int)diff, NUM_PACKETS*PACKET_SIZE*8/diff, RSSI/NUM_PACKETS);
  time = Clock_Time();
  packets = 0;
  RSSI = 0;
}
```

Figure 12. Code snippet from the master device.

A simple C# console application was made, with the purpose of automating and thus speeding up the data gathering. The application listened to the serial port that the master was connected to, displayed the information, and when the test was done it saved the information to a file. A testing output is shown in Figure 13.

```
7    Time: 3965 ms    Goodput: 250 kbps   RSSI: -63

8    Time: 3754 ms    Goodput: 264 kbps   RSSI: -62

9    Time: 3790 ms    Goodput: 261 kbps   RSSI: -62
```

Figure 13. Sample output from C# application.

3.3 Testing and Result

During testing the slave was powered by batteries to make it mobile. The master had to output data to the computer, hence it was powered by the USB cable connecting it to the laptop. The master was placed at six different distances from the slave, 1, 5 10, 15, 20 and 25 meters. When the object was used to block the signal path, it was placed at a half meter distance from the slave during the one-meter test, during the rest of the tests it was placed at a three-meter distance.

The test was run to get 13 cycles per test, the first three cycles were used for the communication to stabilize and the ten last were used to get an average value of goodput and RSSI. Even though the time it takes to transmit 500 packets was shown in the output in Figure 13, a decision was made not to include it in the graphs, since that value is used to calculate the goodput, so the behavior of the goodput also reflected the behavior of the duration. The result from the outside and corridor tests can be seen in Figures 15 through 18 and the object setup in the corridor is shown in Figure 14 where the object is placed three meters from the slave.

Figure 14. Object setup in the corridor.

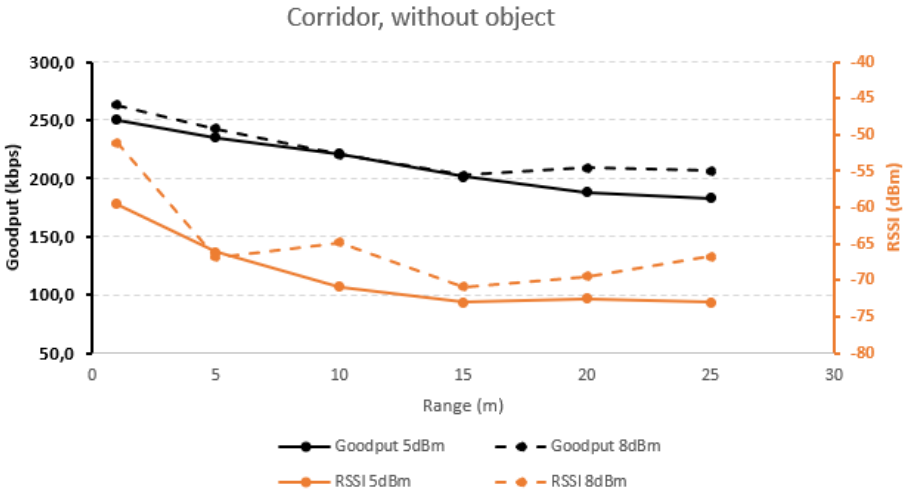

Figure 15. Corridor, without object test result.

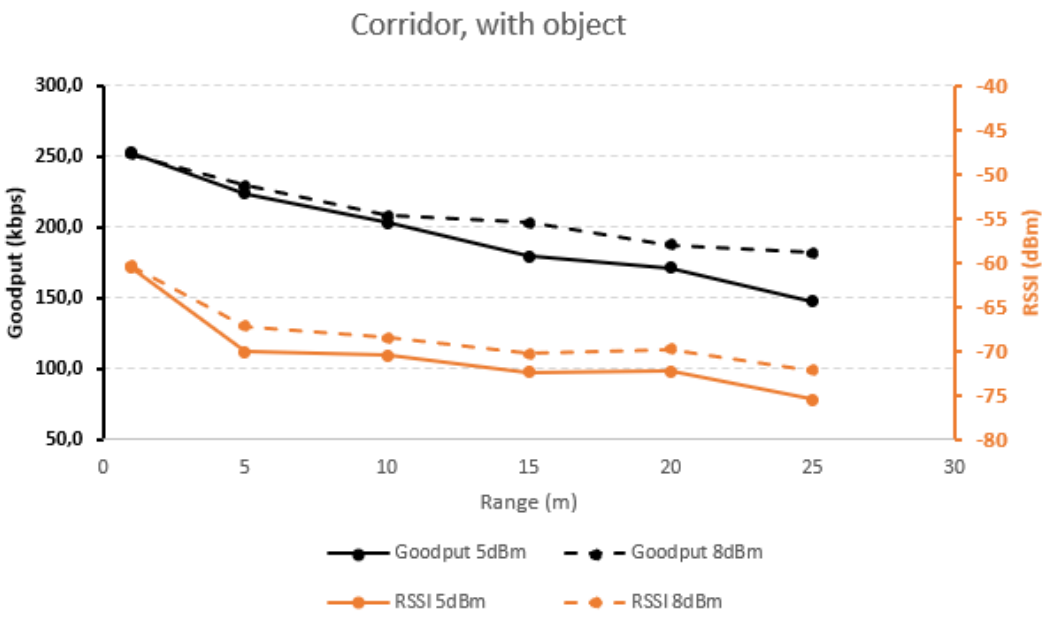

Figure 16. Corridor, with object test result.

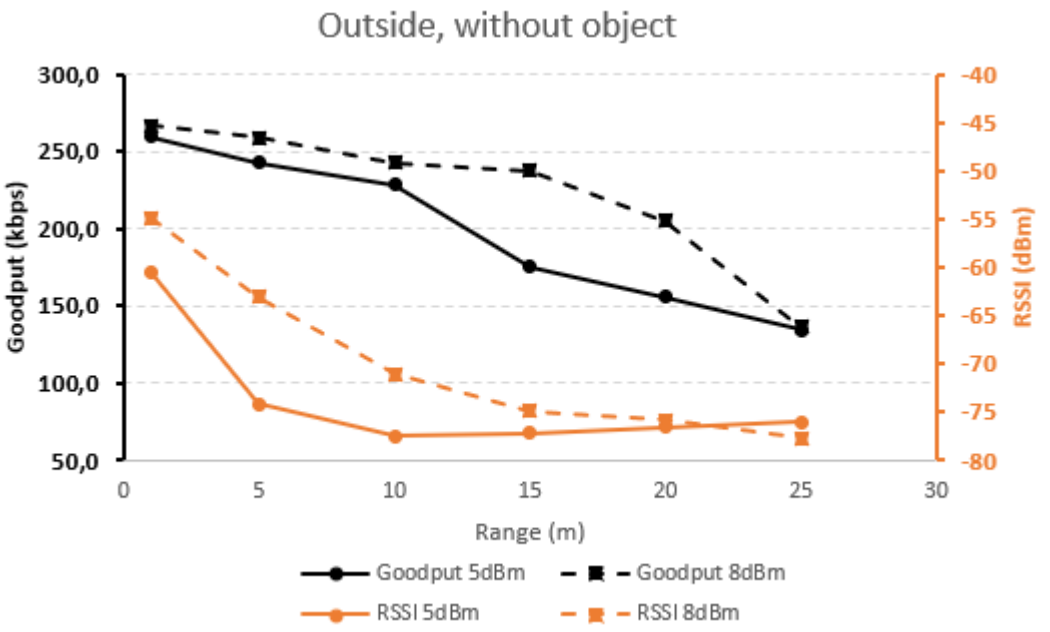

Figure 17. Outside, without object test result.

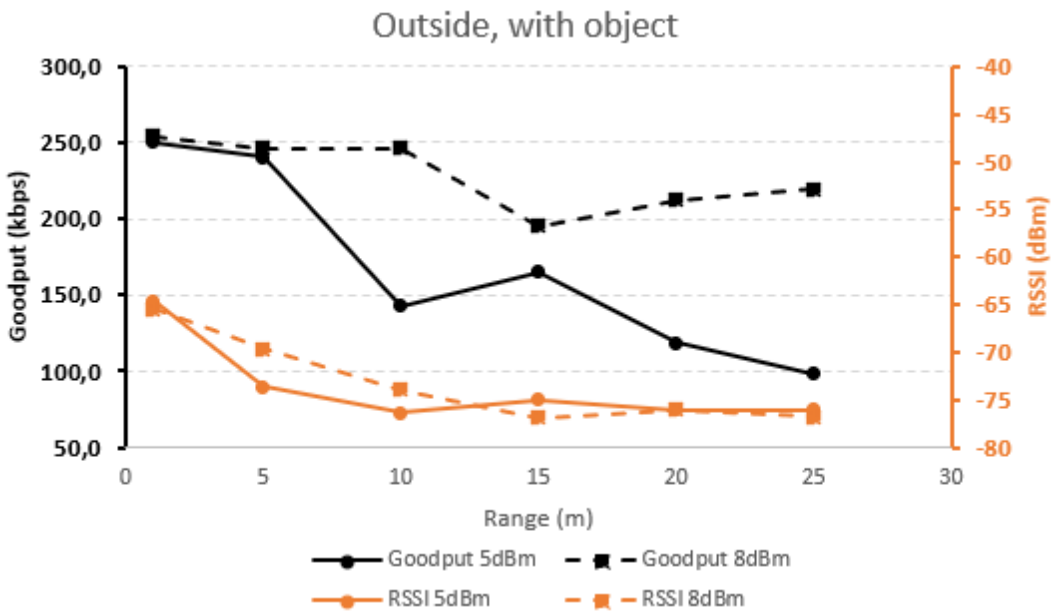

Figure 18. Outside, with object test result.

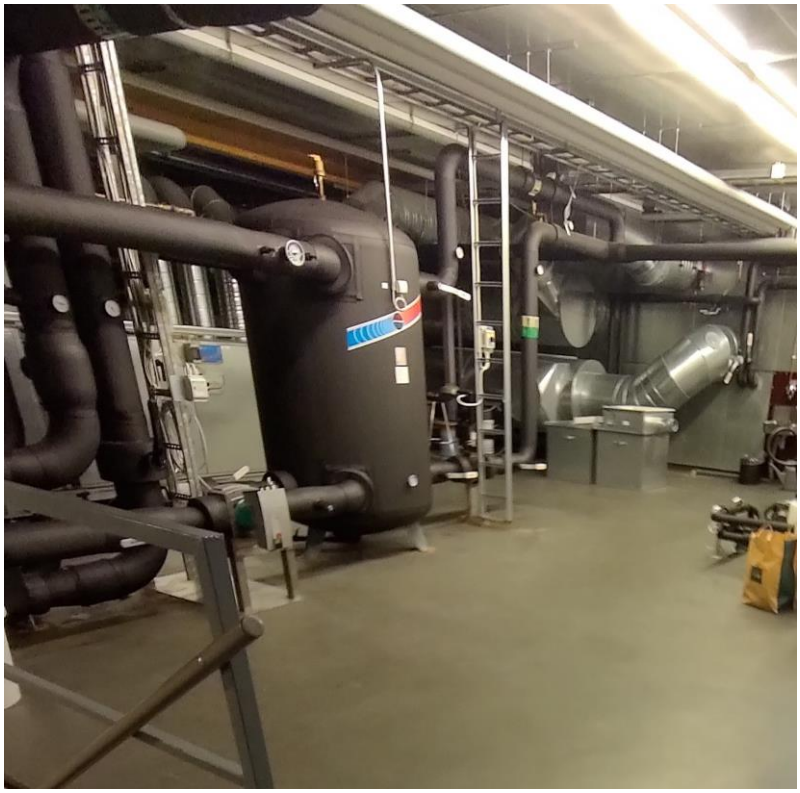

Figure 19. Ventilation room.

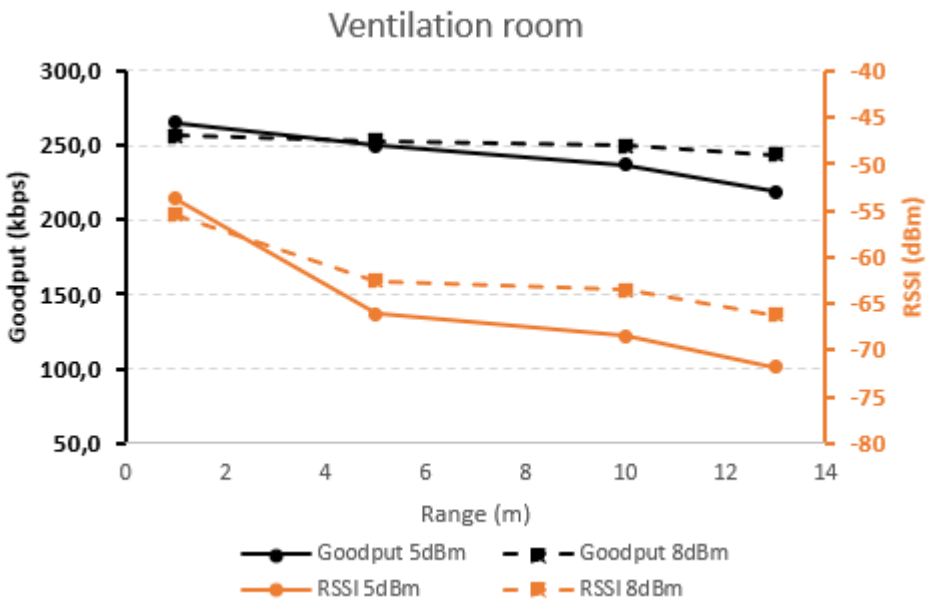

Figure 20. Ventilation room test result.

Since the ventilation room is so small, the maximum range during testing was 13 meters. During the 13-meter test, two machines blocked the signal path, no object was used in the rest of the ventilation room tests. Figure 19 shows the ventilation room where the tests were done, and the result is shown in Figure 20.

3.4 Result analysis

The expected behavior was for the goodput and RSSI to steadily decrease when the range increased. In the corridor test, the goodput was expected to decrease more than in the outside test since the signal should reflect of the walls and cause interference. Since one of the walls is the wall to a bomb shelter, it is designed to be a faraday cage, thus, the reflection should be extra good of that wall. The maximum goodput achieved using this code was 283 kbps; this was achieved at very close distance. This value was used as reference for the goodput.

After the first testing was done, there were multiple unexpected peaks in the graph. Those points were tested again and after the second test, the curve became smoother, but some unexpected behaviors still occurred. For example, in figure 18 at the 10-meter test with Tx power of 5 dBm, the goodput is much lower than expected. Considering that the RSSI value is only 3 dBm lower than in the 5-meter

test, the difference in the goodput should not be that big. The cause of this is believed to be some environmental impact since this point was tested again and the result did not improve. Considering the goodput is still 50% of the reference value, the result is acceptable.

Another anomality is found in Figure 18 during the test with Tx power 8 dBm. As previously mentioned, the value is expected to decrease, but in this case, it increases after 15 meters, while the RSSI value is approximately the same. One possible explanation for this is that there could have been an object close by that reflected the signal well, causing the received signal to be better than at 15 meters.

The result from the corridor tests was not as expected either. In the tests with 8 dBm, the goodput decreased more than the outdoor test at short range as expected, but with longer ranges the goodput outdoors decreased more. In the test with 5 dBm Tx power, the expected behavior is not seen, the goodput decreases faster outside than inside. No explanation was found for this behavior.

The result from the ventilation room tests were better than expected. Even though there were two machines between the transmitter and receiver during the 13-meter test, the goodput was still high. Also, the fact that the lowest goodput was 77% of the reference value, is very positive.

Another test was done to test at which distance the communication was broken. This could only be tested outside, since no indoor space was far enough to cause a disconnection. The result of this test can be seen in Table 3. With the maximum distance of 85 and minimum of 42,5 meters, the result was very good.

Table 3. Distance of disconnection.

5dBm Tx power No Object	5dBm Tx power With Object	8dBm Tx power No Object	8dBm Tx power With Object
45 meters	42,5 meters	85 meters	62,5 meters

The estimated use case for the BLE communication is under ten meters. Hence, the module should have a good goodput at least up to ten meters. A good goodput

was considered to be 50% of the reference value; this would mean a double in time needed to transmit data.

Based on the testing data showed in Figures 15 through 18 and Figure 20, the chosen module is good enough for this use case. The lowest goodput in tests with a range up to ten meters was 50%, which was in the outside test with object and Tx power of 5 dBm. The lowest goodput of all tests was also with the same parameters, outside with object and Tx power of 5 dBm, but at range of 25 meters. During this test, the average goodput was only 34% of the reference value. However, this is still considered good enough, since BLE is not designed to be used at a 25 meter with a Tx power of 5 dBm. 5 dBm Tx power is meant to be used with a distance up to about ten meters. Furthermore, the fact that the shortest distance before disconnection was 42,5 meters is very good and the maximum distance of 85 meters is extremely good.

3.5 Problems

The maximum goodput achieved with this code was only 283 kbps, even though the specification states that it is possible to increase it. This could be increased by changing the time interval when sending the messages. Changing from PHY 1M to 2M would also increase the goodput even more. However, due to time constraints, this was not prioritised.

Even though the goodput during testing did not reach 400 kbps, which was specified as the maximum for the client company´s needs, the test is still considered reliable when evaluating the module. The reason for this is that the result was compared to the maximum goodput of the code and the device is believed to have the same behavior even though the reference goodput is higher. So, if the goodput is 75% of the reference value at one test point, the module is still expected to provide 75% goodput at the same test point with reference goodput of 400 kbps.

Before the final tests that are seen in the report, another set of tests were conducted where the BER of the received data was calculated. After the tests were done, the test result was questioned for providing information that is not accessible by the application layer. As explained in Chapter 3.2, all faulty packets are

dropped at LL, this means, the application layer should not be able to see any faulty packets, let alone faulty bits, thus the BER cannot be calculated at application layer. After a third party looked at the code used in the tests, it became clear that the BLE stack was not used in these tests. These tests were carried out with the module in a primitive mode, meaning it only tested the capability of the hardware to transmit and receive data. When this issue was clear, the BLE was examined further to find out what would be reasonable to look for in the next tests. The answer was, goodput and RSSI.

4 SUMMARY

In the theory research, three short range wireless technologies were examined: Bluetooth, ZigBee and WirelessHART. Based on the following factors, BLE was chosen to proceed with to the evaluation phase:

- The energy consumption is lower than with ZigBee and WHART.
- Multiple modulation techniques available to adjust the throughput.
- The price is low.
- BLE efficiently overcomes interference.
- BLE is widely used already by smartphone manufacturers.

In the evaluation phase, the chosen hardware was tested. The tests were carried out outdoors and indoors; the indoor test was done both in a long corridor and in a ventilation room. The test in the ventilation room yielded the best result and since this place was supposed to represent an industrial environment, it is the most important test place. The result from the outdoor and indoor tests were not as expected, but the worst behavior occurred at greater distance than 10 meters, which is estimated to be the maximum range for the future device.

The final conclusion of the project was that the chosen technology and hardware is ready to be implemented in the future product.

REFERENCES

/1/ Nguyen, T.C. 2020. Who Invented Bluetooth? Accessed 2.2.2021. https://www.thoughtco.com/who-invented-bluetooth-4038864/

/2/ Edström, A. 2008. Grattis Bluetooth, 10 år. Accessed 2.2.2021. https://etn.se/index.php/nyheter/45972-grattis-bluetooth-10-ar/

/3/ Bluetooth SIG homepage. About Bluetooth SIG. Accessed 5.1.2021. https://www.bluetooth.com/about-us/

/4/ Bluetooth SIG homepage. Bluetooth topologies. Accessed 12.01.2021. https://www.bluetooth.com/learn-about-bluetooth/bluetooth-technology/topology-options/

/5/ Chaudhry, M. J., Zahid, M., Saleemi, F. & Chaudhry F. J. 2010. Routing technique for inter slave bonding in Bluetooth scatternets formation. Accessed 2.2.2021. www.researchgate.net/figure/A-typical-Bluetooth-Piconet_fig1_228990705/

/6/ Unseen. Take the first step with Bluetooth. Accessed 2.2.2021. https://www.unseen.fi/en/bluetooth/

/7/ Bluetooth SIG homepage. Bluetooth reliability. Accessed 5.1.2021. www.bluetooth.com/learn-about-bluetooth/bluetooth-technology/reliability

/8/ Bluetooth SIG homepage. Factors that affect the Bluetooth range. Accessed 5.1.2021. www.bluetooth.com/learn-about-bluetooth/bluetooth-technology/range

/9/ Sponås, J. G. 2018. A blogpost that explains Bluetooth range. Accessed 18.1.2021. https://blog.nordicsemi.com/getconnected/things-you-should-know-about-bluetooth-range/

/10/ Bluetooth Core Specification, revision 5.2. Core Specification Working Group 2019. pp. 269-275.

/11/ FieldComm Group. An explanation of WHART. Accessed 5.1.2021. https://fieldcommgroup.org/technologies/hart

/12/ FieldComm Group. An explanation of WHART. Accessed 5.1.2021. https://fieldcommgroup.org/technologies/hart/hart-technology

/13/ HART Communication 2010. Co-Existence of WirelessHART with other Wireless Technologies, revision 1.0. Accessed 10.03.2021. https://www.emerson.com/documents/automation/white-paper-co-existence-of-wirelesshart-other-wireless-technologies-by-hcf-en-42582.pdf

/14/ Cahill, J. 2014 Broadcast Range of WirelessHART Transmitters. A blogpost about WHART range. Accessed 5.1.2021. https://www.emersonautomationexperts.com/2014/industrial-internet-things/broadcast-range-of-wirelesshart-transmitters/

/15/ ZigBee Alliance homepage. An explanation of ZigBee. Accessed 7.1.2021. https://zigbeealliance.org/solution/zigbee/

/16/ Gislason, D. 2008. ZIGBEE WIRELESS NETWORKING. pp. 201-202, 279, 282-283, 287-290, 319,324

/17/ RF Wireless World. A list of ZigBee channels and their frequency. Accessed 8.1.2021. https://www.rfwireless-world.com/Terminology/zigbee-channels.html

/18/ Henna, S., Sajeel, M., Bashir, F., Asfand-e-yar, M. & Tauqir, M. 2017. A Fair Contention Access Scheme for Low-Priority Traffic in Wireless Body Area Networks. pp. 5-6

/19/ Mihajlov, B. & Bogdanoski, M. 2011. Overview and Analysis of the Performances of ZigBee Based Wireless Sensor Networks. International Journal of Computer Applications. p. 30

/20/ ZigBee Specification, revision r21. ZigBee Alliance Board of Directors 2015. Accessed 19.03.2021. https://zigbeealliance.org/wp-content/uploads/2019/12/docs-05-3474-21-0csg-zigbee-specification.pdf. p. 377

/21/ Mouser Electronics. Product page. Accessed 19.03.2021. https://www.mouser.fi/ProductDetail/STMicroelectronics/BLUENRG-M2SA?qs=sGAEpiMZZMu3sxpa5v1qrpe%2F9%2FddSq0j35evv%2FXcPoE%3D

/22/ Mouser Electronics. Product datasheet. Accessed: 19.03.2021. https://www.mouser.fi/datasheet/2/389/dm00629682-1799381.pdf

/23/ Mouser Electronics. Product datasheet. Accessed 26.03.2021. https://www.mouser.fi/ProductDetail/STMicroelectronics/STEVAL-IDB008V1M?qs=%2Fha2pyFadujaqVm%2FgOlTr0z5%252BF4Gpn764TXSOx-VFGhXsVDBE0aw9XQ%3D%3D

/24/ Kellerman, C. 2018. Harmonics Part 1 – Introduction to Harmonics & BLE. PunchThrough. Accessed 6.4.2021. https://punchthrough.com/harmonics-part-1-introduction-to-harmonics-ble-2/

/25/ Programming manual provided by ST Microelectronics. 2019. BlueNRG-1, BlueNRG-2 BLE stack v2.x programming guidelines. p.3, 59.

/26/ Punch Through. 2013. How GAP and GATT Work. Accessed 40.04.2021. https://punchthrough.com/how-gap-and-gatt-work/

/27/ Antenna Test Lab. What Is Antenna Gain ? Accessed 05.05.2021. https://antennatestlab.com/antenna-education-tutorials/what-is-antenna-gain-dbi-scale

/28/ Datasheet of LTP5902IPC-WHMA1A2. Accessed 19.5.2021. https://analog.com/media/en/technical-documentation/data-sheets/59012whmfa.pdf

/29/ Datasheet of XBEE 3. Accessed 19.05.2021. https://eu.mouser.com/datasheet/2/111/Digi_International_01072021_ds_xbee_3_zigbee_3-1951919.pdf

/30/ Nikoukar, A., Raza, S., Poole, A. & Günes, M. 2018. Low-Power Wireless for the Internet of Things: Standards and Applications. Accessed 20.05.2021. https://www.researchgate.net/figure/BR-EDR-BLE-IEEE-802154-and-IEEE-80211-sharing-24-GHz-frequency-band_fig14_328843842

APPENDIX 1

Flow chart of the master device when it receives data.