Out of Band Pairing Methods for MBANs

Fedde van der Meer
Saul Pennings

Delft University of Technology

TU Delft

Out of Band Pairing Methods for MBANs

by

Fedde van der Meer
Saul Pennings

Bachelor graduation project
Delft University of Technology,

Students	Fedde van der Meer	4749693
	Saul Pennings	4477502
Supervisors:	Prof. Dr. Ir. Said Hamdioui	TU Delft
	Dr. Ir. Rajendra Bishnoi	TU Delft
Project proposer:	Dr. Ir. Christos Strydis	Erasmus MC
Daily supervisors:	Ir. Muhammed Ali Siddiqi	Erasmus MC
	Dr. Ir. Anteneh Gebregiorgis	TU Delft

June 18, 2021

Abstract

Epilepsy is a medical condition which is caused by excessive or synchronous neuronal activity of the brain cells. These activities can lead to attacks where the patient can lose conciseness or experiences random muscle cramps at seemingly any point in time. Using implantable on body sensors these seizure attacks could be detected and even prevented. These sensors would form a Medical Body Area Network (MBAN) which interconnects all of the sensors.This project looks at a proof of concept implementation of such an MBAN and focuses on a secure connection between an implant and a gateway device, which is a mobile phone.

The implant and mobile phone will communicate with each other using Bluetooth Low Energy (BLE). This form of communication does not provide a secure pairing method for devices that lack in- and output capabilities, such as an implant. To set up a secure connection the data will be encrypted with an encryption key, which has to be shared between the implant and mobile phone. In order to do this in a secure way, an Out Of Band (OOB) channel will be used to pair the two devices. This thesis looks at three different OOB channels, Near Field Communication (NFC), ultrasound and galvanic coupling and compares them in therms of security, health safety, data rate, power consumption and feasibility.

Preface

This thesis is written as part of the Bachelor Graduation Project. The project was commissioned by the Neuroscience department of the Erasmus University Medical Center Rotterdam. Our work contributes to their research which is to design a proof of concept implementation of a secure an reliable WBAN system for seizure prevention.

We would like to express our appreciation to our daily supervisors Ir. Muhammad Ali Siddiqi and Dr. Ir. Anteneh Gebregiorgis, as well as our project supervisors Prof. Dr. Ir. Said Hamdioui and Dr. Ir. Rajendra and the project proposer Dr. Ir. Christos Strydis. Thank you all for your time and effort to help us with our project. A special thanks goes to Prof. Dr. Ir. Wouter Serdijn who has given us useful tips and insight halfway through the project. Finally we would like to thank our colleagues: Jeroen Vermeulen, Tarik Benaich, Erik Speksnijder and Isamil Bourhial for an enjoyable and educational experience.

Fedde van der Meer & Saul Pennings
Delft, June 2021

Contents

1 Introduction

Epileptic seizures affect around 50 million people worldwide[1], making it one of the most common neurological diseases. A new method relying on a Medical Body Area Network (MBAN) is being developed which is able to detect epileptic seizures in real-time in mice and can execute vagus-nerve stimulation to prevent such an attack. An MBAN consists of multiple implantable or external, wearable and portable nodes, which can be sensors, actuators or relays and communicate with a gateway for processing of the sensor data. This gateway can be a smartwatch, smartphone, computer or other apparatus which itself can process data or relay data to the cloud for heavy duty data processing. To make such an MBAN usable for humans in a medical context, some criteria such as security, usability, size, safety and power have to be met.

One of the most popular protocols for wireless communication is Bluetooth. Because of the medical context, secure communication without the possibility of Man-in-the-Middle (MITM) and other threats must be implemented. For this goal, out-of-band (OOB) pairing is proposed which solves the problem of MITM attacks that traditional low energy radio-frequency communication have.

This project was the effort of one subgroup, which was part of a larger group with the goal of prototyping a complete MBAN system. This project is Task 1 in the system overview in figure 1.1. Task 2 looked at developing an Android application and interfacing with Task 1, Task 2 and the cloud. Task 3 developed a secure bus architecture for secure firmware updating and communication of MBAN nodes. Eventually the three tasks will be integrated to create a secure and reliable MBAN prototype, but that is outside the scope of this report and this report will focus on Task 1.

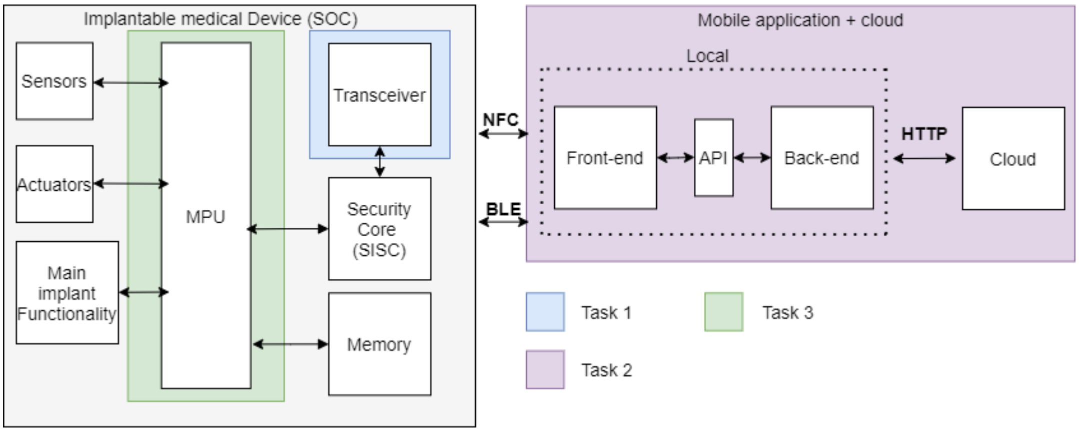


Figure 1.1: System overview

1.1. Objective/approach

This project will apply existing techniques for OOB communication using three different communication techniques namely: Near-Field Communication (NFC), ultrasound and galvanic coupling. These three techniques will be qualitatively compared in terms of security, feasibility, size, safety, and power. One of the goals of this project is to apply these techniques and integrate one of them, NFC, in an MBAN. This is done in an effort to show a proof-of-concept for using these channels in MBANs. The other goal is to experiment with different OOB pairing methods and give recommendations based on these experiments.

1.2. State of the Art

Medical Body Area Networks are actively being researched. It is clear that MBANs will only be viable if low power data protocols are used and studies have been done to show which one is best suited [2] [3]. Out of these protocols Bluetooth Low Energy (BLE) was deemed the most suited candidate, consuming around 10 mW of power.

The biggest concern in these protocols is the security aspect. BLE has been shown to exhibit security flaws during the discovery and pairing phase [4]. To counter these security flaws it is necessary to do the initial pairing sequence using a different channels, which is an OOB channel. Multiple comparisons have been done on OOB methods and current research looks at radio-frequency, including NFC, and intra-body communication (IBC) including ultrasound, galvanic coupling and capacitive coupling [5] [6]. NFC has been used as a communication channel for heart-rate monitoring in [7] and [8], an advantage is that NFC is present in most modern smartphones, a disadvantage for this method is limited security. The acoustic channel of human tissue was analyzed in [9] and in [10] the security of ultrasound in implantable medical devices has been analyzed. The advantage of ultrasound transducers is that they can be made very small. Galvanic coupling has been studied [11], prototyped [3] and a testbed was designed in [12].

1.3. Thesis Outline

The main subject of this thesis will be a comparison between different methods for OOB pairing. It will first describe a programme of requirements that a good OOB pairing method should adhere to. Next literature is evaluated to select the three most promising methods and give a comparison between them. Finally, these three methods are implemented and validated.

2

Programme of Requirements

This program of requirements defines what properties the final product must exhibit. This project is a proof-of-concept implementation of three methods which will then be compared in terms of these requirements.

1. **Mandatory requirements**

   (a) A safe connection must be established between the sensor and the gateway device. That means that other users cannot intercept the communicated data.

   (b) The data must be accurately transferred from the sensor node to the gateway device.

   (c) The product must meet health regulations.

   (d) The product must be able to at least send a 128-bit key in one second

   (e) The data has to be sent through a human tissue like medium.

   (f) The prototype must be built using off-the-shelf components

2. **Properties to be evaluated**

   (a) Security, how difficult it is for a third user to intercept the data.

   (b) Health safety, does the technique meet health regulations.

   (c) Data rate, how many bits can be transferred per second

   (d) Feasibility, what kind of hardware is required to make this technique work and how easy is it to implement.

   (e) Power consumption, how much power does the hardware need when it is communicating and when it is idle.

   (f) Attenuation, how far does the data travel in and outside of the body

3

OOB Pairing

In order to send data via Bluetooth there must first be a connection between the two devices that want to communicate. The set up of this initial link is called pairing and it is used to share a secret key between the devices that can then be used to encrypt the data that is send. The receiver then uses the same key to decrypt the data and thus it becomes very difficult for a third user to read the data without this key.

3.1. Methods of pairing

In case of BLE pairing can be done in four different ways namely: Passkey, Numeric Comparison, Just works and OOB. With Passkey both devices display a number and the user is asked if these numbers match. With Numeric Comparison one of the devices displays a number and the other device has to enter this number using a keyboard of some sort.

Both of these pairing methods are not suited for implants as the implant does not have a display unit nor any input capabilities. With Just Works one device is simply asked if it wants to connect to the other device and thus this pairing method does not block other users from establishing a connection.

The last option is OOB pairing, which connects the two devices with each other using another communication channel and then share the secret key that is necessary for the Bluetooth communication. This means that the security aspect of the communication is now mostly depended on this OOB channel as without the secret key it is very difficult for the attacker to decrypt the data.

3.1.1. Intra-body communication

There are a number of different OOB channels suited for pairing with an implant, for example Radio Frequency (RF) based channels or an intra-body communication (IBC) channel. IBC uses the human body as a transmission medium which can be used to interconnect devices that are placed in or on the body. This allows them to communicate through low power consumption and low data rate channels[6]. Examples of IBC methods are Ultrasound, galvanic coupling and capacitive coupling (CC).
These methods use low power signals and in some cases they can be confined within the human body making it less vulnerable against eaves dropping [13]. This is in line with requirement 1a which states that a safe connection has to be established where attackers cannot intercept the data.

3.1.2. Radio frequency

Radio frequency is one of the most common form of wireless communication and can be found in many fields including the medical field. Information is send via an oscillating electromagnetic wave which varies in frequency. Radio frequency comes in many different forms and the frequency that is typically used ranges from 3 kHz to 300 GHz. In order to prevent different users from interfering with one another, the frequency spectrum is split up into specific bands which are allocated for different applications. In the Netherlands these bands are recorded in the so called ”Nationaal Frequentieplan” (NFP) and they follow the guidelines set by the European Telecommunications Standards Institute (ETSI).

RF-Narrowband
First, narrowband frequencies are discussed. One example of a band specifically for ultra low power implanted medical devices has a range of 402 – 405 MHz [14]. This band has a good conductivity in the human body, a high data rate and a communication range up to 2 m [15].
Then there is also the 2483.5-2500 MHz band which is specifically for Medical Body Area Networks (MBAN). It is used for low power sensors that are controlled by either an on body or implanted hub device [14].

All of these bands are free to use and thus do not require a licence. However, they do have to follow specific guidelines regarding the use of the frequency band set by the ETSI. Next to that any equipment that is put on the market has to comply with the Radio Equipment Directive (RED). This sets the requirement for any radio equipment regarding health and safety, efficient use of the radio spectrum, etc.

RF-Ultra wideband
Another form of RF is so called ultra wideband which works by sending a lot of pulses across a wide frequency band. It provides data communication over a shorter range compared to narrow band, but it can achieve a higher data rate. In Europe, the Electronic Communications Committee allocated the ultra wide band between 3.1 and 9 GHz with an unauthorized band between 4.8 and 6 GHz[16].

NFC
A specific implementation of RF is Near Field Communication (NFC), which uses inductive coupling between two antennas at a base frequency of 13.56 MHz. It is designed to share relatively small amounts off data over a short distance between two devices. There is what is called active NFC that can both send and receive data, this is currently implemented in most phones, and passive NFC. Passive NFC can only send data but has the benefit that it can do so without consuming any power.

Ultrasound
Ultrasound has been used extensively in underwater exploration as the ultrasonic waves propagate better than radio waves through media that is mostly composed out of water. Considering that the human body consists for 65% out of water makes ultrasound communication a promising alternative to RF communication [17].
Ultrasound uses transducers that convert electrical signals into pressurised sound waves. These sound waves can then be picked up by another transducers which converts it back to a voltage. The reason why it is called ultrasound is because the frequency that is used is at least higher than 20 kHz, which is above the audible spectrum of humans. One downside of ultrasound communication is that it requires a line of sight between the transducers which is not always possible.

Galvanic Coupling
Galvanic coupling works by connecting two electrode pairs to human tissue, one transmitter and one receiver pair. Putting a voltage signal across the transmitter pair induces a primary current. Besides this primary current a secondary current and voltage is induced between the receiver pair. By using a modulated signal, data can be sent over the tissue. Usable frequencies are 10kHz - 100MHz as below 1k0Hz one might interfere with naturally occurring body frequencies and above 100MHz attenuation becomes too high[3].

Capacitive Coupling
Capacitive coupling also uses two electrode pairs, but at each pair there is one electrode free floating in air. When a signal is applied the transmitter side, this then generates an electric potential between the signal and the floating electrode which acts as ground. This generates an electric field that is coupled with the human body and its surroundings. As the receiver also has a free floating electrode there is a return path through the air for the signal to travel through. The link between the electrodes, air and external ground can be modeled as a capacitor which is why it is called capacitive coupling [6]. The frequency range for capacitive coupling ranges from 100 kHz to 120 MHz.

4 Comparison

In order to test which OOB channel is most suited for this application, several channels will be compared in further detail. As this project has to be completed within 10 weeks it was decided to try to implement three different OOB channels, which are NFC, ultrasound and galvanic coupling.

It was decided to test one radio frequency based method as this is the most common way to communicate between devices. The reason for specifically choosing NFC is because this method is easy to implement, as it is already integrated within mobile phones, and could fairly easily be operated using an app. The biggest downside to NFC compared to other RF based methods is that it does have a much lower data rate. However, this is not an issue as one of the requirements 1.d2 is that a 128-bit key has to be sent within a second, which NFC can easily achieve.

Ultrasound was chosen to be tested as it was already being used in medical applications such as medical imagery. Because it does not use any ionizing waves it is very safe to use in the body and the transducers can be even smaller than RF transducers making it a very promising technique. As stated in the requirement 1.f the technique should be built from off the shelf components which is the case for ultrasonic communication over the air as it does not require many or complex components. According to [5] communication through ultrasound can be made very secure when compared with the other methods which is in line with requirement 1.a, a secure connection between implant and gateway.

Galvanic coupling and capacitive coupling are very similar techniques with the biggest difference being the free floating electrodes for capacitive coupling instead of the on/in body electrodes. When using an implant it is very impractical to have a free floating electrode to couple the electric field of the body. Next to that capacitive coupling is more vulnerable to attackers as the electric field is outside of the body which can more easily be picked up. One upside to capacitive coupling is that it can achieve a higher data rate, but this is not an important parameter as only a 128-bit key has to be sent. Because galvanic coupling is more in line with the requirements, in particular 1.a, safety, 2.d, feasibility, this method was chosen to investigate further.

4.1. Security

The purpose of using OOB channels is to achieve a secure BLE connection through OOB encryption key sharing. It is therefore important to evaluate the possible security flaws of each channel. It is assumed that only a trusted gateway can get close enough, meaning closer than 10cm, to the patient and that an attacker would have to be at a significant distance. Security threats include eavesdropping, skimming, man-in-the-middle (MITM) attacks and battery-drain denial of service (DoS) attacks.

4.1.1. Forms of attack

Eavesdropping occurs if during pairing the OOB channel can be listened to by the attacker. This can allow an attack to retrieve the transmission key.

A MITM attack occurs when an attacker intercepts a key request from the receiver and relays this to the transmitter, the transmitter responds with the transmission key. Next the attacker sends its own key to the receiver. The receiver now thinks this is the correct key and starts communication encrypted with the attackers key. The attacker can only decrypt this information and can encrypt it with the transmission key and relay it to the transmitter or send its own information to the transmitter who does not suspect a 'man in the middle' because communication seems normal.

In a denial-of-service (DOS) attack the attackers objective is to make the service unavailable to the receiver. This can be done by flooding the channel with noise or requests, making it impossible for the transmitter to read any key request or answer all requests respectively. By flooding the channel with noise it also becomes impossible for the receiver to read the key sent by the transmitter.

Battery-drain DOS attempts to empty the battery by making many requests, which have to be responded to by the transmitter. As the transmitter only has limited amount of energy, especially in implants, and reading the request and sending the key costs energy, this drains the battery and stops the service of the transmitter.

NFC

NFC uses electromagnetic waves to communicate wirelessly, because of this it is clear that eavesdropping is a large threat. NFC is typically used at a distance of less than 10cm, this does not however mean that it is impossible to detect the signal from further distances. The distance an attacker might be able to detect a signal depends on a lot of factors such as the attackers receiver quality, the transmitting power and whether the transmitter is in active or passive mode. For instance, in [18] eavesdropping was achieved with minimal electronics up to 90cm on a reader and tag (the tag is a passive transmitter). An active transmitter can be eavesdropped upon up to 10m [19].

As discussed in [19] NFC is inherently protected against MITM attacks. The attacker has to disturb the transmitted signal by generating a RF field, which is possible, but the receiver also detects the disturbance. When this happens the receiver can stop the key agreement protocol.

In [19] data corruption is discussed, which is essentially the same as a DOS attack. By checking the RF field while transmitting data the disturbance can easily be detected, but not much can be done to stop the attack.

As shown in [20] there is a technique called Zero-Power Defence (ZPD) that harvests energy from the attacker. Implementing this makes a battery DOS attack useless as it will not be able to drain the battery of the implant.

Ultrasound

With ultrasound the sound waves have to be confined within the human body as much as possible to prevent attackers from picking up the signal. The type of medium in which the sound waves travel greatly affects the attenuation of the signal. These characteristics can be defined by the acoustic impedance (Z) and the absorption coefficient (α) [10]. When the wave travels from one medium to the next the ratio of the transmitted signal amplitude and the incident signal amplitude is

$$2Z_2/(Z_1 + Z_2) \tag{4.1}$$

As the acoustic impedance of sound is only 0.0004 $kg/m^2 * 10^6$ while that of fat is 1.345 $kg/m^2 * 10^6$ and 1.801 $kg/m^2 * 10^6$ for skin. That means that $Z_1 >> Z_2$ so the signal will suffer from an attenuation of

$$1/Z_1 \tag{4.2}$$

Next tot that the waves suffer from absorption at a rate of α dB/m which increases with frequency. This shows that the higher the frequency of the transmitted wave the lower the propagation outside of the body is. The simulations in [10] show that when using a transducer with a frequency of 2 MHz the maximum distance to demodulate the signal is 5cm. This concludes that if a sufficiently high frequency is used (in the MHz range) it is almost impossible for an attacker to receive the signal. Which means that attacks such as MITM and eavesdropping are not possible. A DOS attack could be possible if the attacker can be in the line of sight of the transducer. But this is fairly difficult as the receiver would be placed directly on the skin.

A ZPD can also be implemented for ultrasound, protecting against battery DOS attacks [20].

Galvanic coupling
Galvanic coupling has a low attenuation and the signals are fully confined inside the human body [5]. This allows for a very safe and secure channel where it is almost impossible for attackers to directly receive the transmitted signals. However as there is a current running through the body this means that there is also an electric field present which does leak outside of the body.

In a study on galvanic coupling[21] a setup is used where instead of electrodes two pairs of wires were directly stuck into a fake hand. The signal strength at the receiver was measured and plotted against the distance to the transmitter. What they found was that up to around 13cm the strength was detectable, after that the signal was equal to the surrounding noise level. But at every distance the bit error rate was 0.5 which indicates that it is impossible to decode the signal considering a random string of ones and zeros would also have a 0.5 bit error rate. This concludes that the information of the signal can indeed be confided within the body making it very secure against eaves dropping and MITM attacks. DOS and battery DOS attacks are not feasible as it is not possible to send a meaningful signal to the implant without making physical contact. It would be technically be possible to induce a voltage by putting the patient in a strong altering electric field. But doing so would just be harmful causing health issue, so this can not be done unnoticeably.

4.2. Data rate

A BLE transmission key is 128 bits and according to requirement 1.d the OOB channel must be capable of sending this in at most one second.

NFC
NFC offers a data rate of 106kbit/s up to 424kbit/s. This allows transmission of the key in less than 2ms.

Ultrasound
Data rate is limited by bandwidth and data levels. With L data levels and B bandwidth the maximum data rate D is given by $D = 2B\log_2(L)$. With binary data this becomes $D = 2B$. Of course the ability to send data also depends on the signal to noise ratio, but as long as this is higher than unity a binary signal should be detectable. Beside the data rate, using US also introduces some latency into the system because sound travels slowly relative to EM waves and electricity. Data would travel at around 1600m/s in human tissue, introducing a latency of $62.5\mu s$ at 10cm. Group velocity of EM waves in human skin is around 4.383e7 m/s at a frequency of 403.5MHz giving a latency of around 2.3ns[22].

Experiments have been done through synthetic phantoms to show that a data rate of 28.12 Mbps can be achieved[23]. Which means that the 128 bits key can be send in roughly 4.6μs. However a higher data rate does come at the cost of a higher power consumption. Another study has shown that while using low power transmission of about 8 the data rate 70kbit/s[24]. This means that sending the key takes about 1.8ms.

Galvanic Coupling
The same theoretical boundary for data rate holds for galvanic coupling. Experimental research in [25] has shown that galvanic coupling can reach a data rate up to 1.23 Mbps with only a frequency rate of 200 kHz and a power consumption of 2 mW.

4.3. Health safety

When using any energy source in or on the human body it is important to be aware of the potential harmful effects that they can cause. The most straightforward effect when energy is applied to or in the body is tissue heating, which may lead to heat damage to the skin or to internal tissue. To prevent this, the body's temperature should not rise more than $1°C$ as this is still considered safe. If the temperature rises even more then at some point biological effects may occur. However, there has been no recording of lethal effects for temperatures lower than $41°C$ [17].

NFC

Prolonged exposure to electromagnetic waves can be harmful, that is why there are several standards that set limits to prevent damage to human organs and tissue. One of such standards is the IEEE C95.1 standard [26] which expresses the limits in terms of dosimetric reference limits (DRL) and exposure reference levels (ERL). DRLs are expressed in for example in-body electric field strength and Specific Absorption Rate (SAR [Watt/kg]), which is the rate at which energy is absorbed per unit mass by the human body. Using this the Maximum Permissible Exposure (MPE)[mW/cm^2] can be derived which is a quantity that describes the maximum rms, peak electric and magnetic field strength or power density that a human can be exposed to without causing adverse health effects. These limits are to ensure that the DRLs are not exceeded.

These limits are different depending on the frequency of the wave. For the frequency range of 0 Hz to 5 MHz the limits are defined to mostly protect against painful electrostimulation. In the frequency range from 100 kHz to 300 GHz the main limit is to prevent adverse tissue heating. Then there is a transition range from 100 kHz to 5 MHz which limits are to protect against both of these phenomena.

Note however, that these standards might not be protective enough for the use of medical implants. There are standards that can be bought that are specifically for active implantable devices that contain electromagnetic compatibility requirements (EN 45502-1 [B396]; IEC 60601-1-2 [B652]; International Organization for Standardization (ISO) 14708-1 [B689]). As the cost of these standards are quite high, it was decided to look at the general guidelines as given by IEEE C95.1 standard.

As NFC operates at a frequency of 13.56 MHz, the limits for 100 kHz to 300 GHz electromagnetic waves have to be further investigated. This frequency range is again split up in smaller ranges and for 1 to 10 MHz the MPE is calculated as $9000/f_M^2$, where f_M is the frequency in MHz. This means that the MPE is 4.89 mW/cm^2.

Ultrasound

The speed of sound in tissue is much slower compared to the speed of electromagnetic waves which means that it causes less tissue heating. To compare ultrasonic waves with electromagnetic waves they are expressed in terms of intensity, so the energy absorbed by the tissue transferred from the mechanical waves [5]. The Food and Drug Administration Staff has set 720 mW/cm^2 as MPE for ultrasound systems with a center frequency from 1 to 20 MHz. When comparing this to other IBC types it is clear that a lot more power is permitted which is a great upside to using ultrasonic communication as IBC.

One other risk that can be caused by ultrasound waves is so called cavitation which is the behavior of gas bubbles in an acoustic field. Due to the pressurised sound waves gas bubbles can form, grow and collapse which can result in local hot spots. These hot spots can reach high values which can cause biological effects or damage objects in close proximity. It can be shown that this phenomenon is frequency dependent and that higher frequencies lead to shorter pressured oscillations which restricts the formation of bubbles and limits the cavitation effects [17].

Galvanic coupling

As galvanic coupling send a signal through the human body there is a danger of giving painful electrical shocks to the patient or interfering with the body's functions. The international Commission on Non-Ionizing Radiation Protection (ICNIRP) has guidelines for limiting the exposure to induced currents [27]. These limitations are also split up into different frequency regions which are similar 'to those in the IEEE 95.1 standard. The threshold for maximum contact currents up to 100 kHz rises with 0.2 times the frequency and above 100 kHz is fixed at 20 mA. The reason why it is kept at a maximum of 20 mA is because 50 mA is used for nerve stimulation. The MPE (which by ICNIRP is defined as Equivalent plane wave power density) for time varying electric fields for a frequency between 10 and 400 Mhz is fixed at 2 mW/cm^2.

It is also important to consider ionization effects when using galvanic coupling. When only positive or only negative current is used in the PWM signal, electrolysis might occur at the electrodes which can cause substances harmful to the skin to form. This can be avoided by using non-return-to-zero (NRZ) code as this assures equal positive and negative electric current.

4.4. Power consumption

At the transmitter side, i.e. the implant, battery size is limited by the size of the implant. Therefore low power consumption is critical at the side of the implant. At the side of the gateway power consumption is less important, because of this, mainly the implant power consumption will be looked at. An overview of the power consumption per OOB method is given in table 4.1

NFC

The PN532, a commonly used NFC controller, uses around 0.5W during operation [28]. This means when sending 106kbit/s it consumes about $4.7\mu J$ per bit. For a 128 bit transmission key this means about $600\mu J$ per transmission key.

Ultrasound

Ultrasound transducers can be operated at extremely low power, the power necessary at the transducer going down to 8 μW [29]. In this case though, much more power would be used by the MCU, so power consumption can be limited by reducing power needed for processing. Santagati et al. showed a data rate of 70kbit/s at a power consumption of 20mW for the transducer with receiver, which equates to 0.286μJ per bit or 36.6μJ per transmission key.

Galvanic coupling

[3] has achieved a data rate of 64kbit/s at 726mW, giving 1.134 μJ per bit or 145 μJ per transmission key.

	Data Rate [kbit/s]	Power Consumption [mW]	Energy/bit [nJ/bit]
NFC	106	500	4700
US	70	20	286
GC	64	726	1134

Table 4.1: Power consumption

4.5. Feasibility

Feasibility of the OOB channel defines how easy it is to integrate with the mobile phone and how easy it is to operate the OOB channel. The people that will use the product are regular patients from different ages and doctors and nurses as they have to be able to read the data of the implant as well. It is assumed that the transducer is held or placed directly on the body of the patient during pairing.

NFC

In the last couple of years NFC has been increasingly used in for example wireless money transaction, power transfer and tag reading. For this reason most phones are already capable of using NFC, in fact almost every smartphone that was built since 2018 has a NFC reader integrated [30]. This means that no additional equipment is necessary to pair the phone which also makes it easy for nurses and doctors to pair with the implant.

Just simply by holding their phone or other gateway device next to the implant they would be paired which means that it is very easy to use. Study has shown that the rotation of a phone relative to a tag does have an impact on the amount of power that is induced into the tag[31]. This showed that at 180 degrees it was unable to read the tag, while another study showed the same result for a 90 degree rotation. This is because the NFC antenna in each phone can be different so the angle at which the phone has to be held for the best transmission is different as well.

Ultrasound

In order to read the US signals with a phone a separate receiver circuit with ultrasound transducer is needed. A line of sight between two transducers is needed in order to successfully send data. This means that the receiver has to be placed at a very specific spot which is on the body opposite to the implant. The receiver circuit then has to be connected to the phone through wires. For this micro usb

port can be used which would allow for example a UART connection.
An alternative would be to use the microphone and speaker that is build into the phone. There is an open source-project called ”SoniTalk” which is trying to implement a standard for ultrasonic communication. They developed a demo app that is able to send and receive ultrasound messages. The base frequency of these messages can range from 50 to 20000 Hz. As explained in 4.1.1 the frequency needed for secure pairing is in the MHz range. Such a high frequency cannot be achieved using the built in speaker of a normal phone, which means that this option is not secure enough.
So in order to achieve secure pairing a separate transducer with receiver circuit is needed; which means that if the user forgets or loses it, it is not possible to pair their phone anymore.

Galvanic Coupling
For galvanic coupling it is very similar to ultrasound in how to connect it to the phone. It also requires a receiver circuit which sends the data through wires to the micro usb port. The difference is that transducer is now replaced with electrodes. These electrodes can come in the form of sticky pads which can only be used once, but are easily applied and removed. They are also fairly inexpensive as a single pad is around 50 cents.
Alternatively the electrodes could be in the form of a conducting surface that is held against the body. As the pairing only takes about a second it is faster and easier compared to sticky electrodes. It would also allow nurses and doctors to quickly pair with a patient instead of having to apply the electrodes first. It does suffers from the same problem as US which is that it requires a separate receiver circuit. Losing it will leaves the patient being unable to pair with the phone.

4.5.1. Overview

To give an overview of how well each OOB method currently meets the requirements a qualitative comparison is given in table 4.2. More filled in circles meaning a better performance relative to the other methods.

	Security	Data Rate	Health Safety	Power Use	Feasibility
NFC	●○○	●○○	●●○	●○○	●●●
US	●●●	●●●	●●●	●●●	●●○
GC	●●○	●●○	●●●	●●○	●●○

Table 4.2: Comparison table

5 Implementation and Validation

An implementation was done to some degree for all three OOB channels. For demonstration purposes, NFC was most suited as it is already present in most modern smartphones. NFC was implemented using a PN532 connected to an MCU and a smartphone. US was implemented with two 40kHz transducers, the transmitter connected directly to an MCU and the receiver connected to an MCU via a receiver circuit. GC was implemented using the same infrastructure as US, switching the transducers for electrodes. Next, all three OOB channels were evaluated, as far as possible, in terms of aspects specified in the programme of requirements. To control the different OOB modules a microcontroller was needed which also conforms to the set requirements.

5.1. Microcontroller

To control the different OOB methods a micocontroller was selected. The main criteria of the microcontroller were: low power consumption, high enough clock speed and a bluetooth module for testing and preferably libraries for NFC and SPI (a communication interface for communication with the NFC module) should be available. The high clock rate was a criterion as it was unknown at what frequencies the methods would be working at the time of selection. The microcontrollers at hand were the ESP32-WROOM-32, Arduino Uno and Arduino Nano. Each of these was examined and the ESP32-WROOM-32 was found to be most suitable (see table 5.1 for the microcontroller criteria). On top of meeting the criteria, it also has a sleep mode which only uses 16.5μW of power and can be turned on/off by exciting a wake-up pin. Ultimately, the Arduino Nano was also used as this allowed easy prototyping in the Arduino IDE.

5.2. NFC

An NFC library for the Arduino IDE [32] was used to turn the PN532, connected to an MCU (an Arduino Nano) (see figure 5.1), into an RF transceiver. This allowed for data to be transferred between the MCU and NFC module via SPI. The code used to send and receive data can be found in appendix A.

NFC has three main modes of operation: reader/writer, peer-to-peer and tag emulation. Reader/writer is a passive mode as the transmitter, an NFC tag, does not have a power supply of its own. This mode is limited as the transmitter cannot change the data it is transmitting. This implementation should be able to change its data for security reasons, so this is not an option. Peer-to-peer supports two-way communication between devices, this is however not supported for many devices and uses more

	Power Use	Clock Rate	Bluetooth	SPI library	NFC library	Bonus
ESP32-WROOM-32	82.5 mW	80 MHz	Yes	Yes	Yes	Sleep mode
Arduino Uno	290 mW	16 MHz	No	Yes	Yes	Easy prototyping
Arduino Nano	133 mW	16 MHz	No	Yes	Yes	Easy prototyping

Table 5.1: Microcontroller criteria

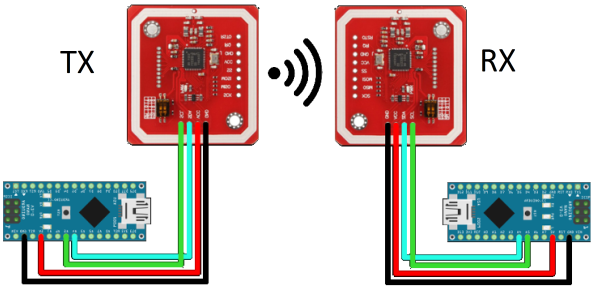


Figure 5.1: PN532 connected to an Arduino Nano

power than the other two modes of operation. Tag emulation allows an NFC module to behave like a tag, while still being able to change its data. This is advantageous as the data has to be changed when the transmission key is changed. Tag emulation lets the reader use the same protocol as for reader/writer mode. Important to note is that tag emulation is only supported with SPI and not with I2C or UART. The PN532 pin connections to the Arduino Nano are shown in 5.1.

It was possible to read data up to 5cm between devices, taking roughly 3 seconds to read the data. This is good enough to protect against attackers using a similar NFC device, but it should be noted that attackers with more advanced receivers might be able to receive from much further distances as has been discussed in section 4.1.1.

5.3. Ultrasound

Hardware

To drive the US transmitter, a 3.3V PWM signal was sent at 40kHz. Data was sent using RZ-ASK from an MCU (an ESP32) through air and received at a similar transducer, connected to a circuit shown in figure 5.2.

The receiving transducer produces a sinusoidal oscillating wave in response to the incoming signal. This wave is first amplified using the LM386N-1, which is an audio operational amplifier. The capacitor and resistor in front of the amplifier form a high pass filter with a cut-off frequency of 1.59 kHz to remove unwanted low frequency signals. The gain of this amplifier is internally set to 20 which is sufficient for this circuit. If necessary the gain could be increased to a maximum of 200 using an external resistor and capacitor.

The LM339N is a comparator to transform the amplified sinusoidal wave into a PWM signal. The reference signal is set by using a potentiometer that connects to the inverting input. The signal is then send into a digital input pin on the ESP32 which reads the signal as either being high or low.

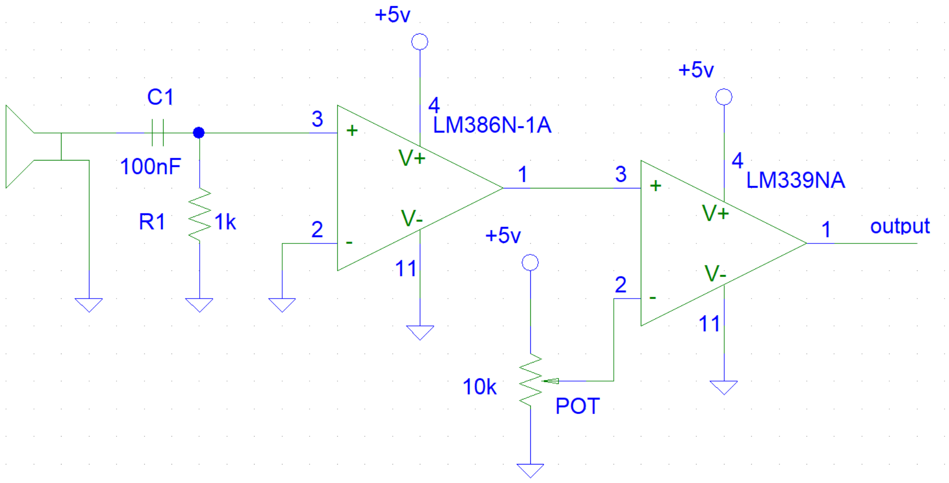


Figure 5.2: Schematic for the receiver circuit

Software

The code that was used can be found in appendix B. The transmitted data are character strings where each character is represented by 8 bits.

On-off keying has been used as this is one of the easier modulation schemes to implement. Before a character is send a high pulse is transmitted so the receiver can synchronize with the transmitter. Then each bit is send by either sending a short pulse for a 0 and a longer pulse for a 1. after the character is send it goes to the next character repeating the process until all data is transmitted.

At the receiver side the code waits until it reads a high signal at the input pin at which it starts counting the amount of high pulses for a set duration. When the amount of pulses is larger than the high threshold it corresponds to the synchronizing pulse at which the code starts to decode the message. If the amount of pulses is lower than the threshold it will wait again until another pulse is received. The decoding of the message is done by counting the amount of pulses for a set time where if it is between the low to medium threshold it is a zero and between medium to high threshold it is a one.

These thresholds are depended on the potentiometer that can vary the reference signal. In order to automatically set the threshold values the code listens for a duration of 9 pulses as this is the length of a message including the synchronizing pulse. The maximum and minimum amount of pulses are then uses to determine the threshold values. If the potentiometer is adjusted or the distance between the transducers is changed significantly the ESP32 can simply be rebooted to automatically update the threshold values.

5.3.1. Test result

Test over air have been successful in transmitting and receiving simple messages up to a distance of about 20cm. The tests could not be performed through the body as this requires transducers capable of sending waves through water like substances. So called ”ultrasonic cleaning transducers” would have been able to send waves through the human body, but due to the limited time and price of the transducers it was decided to no do these tests.

5.4. Galvanic Coupling

Galvanic coupling was implemented by sending a OOK encoded PWM signal from an MCU to a pair of electrodes connected to the human skin via coaxial cable. This signal is received with another pair of electrodes connected to the skin. Because the top layer of human skin is a poor conductor, this setup should replicate in vivo conditions of an implant as the current has the path of least resistance through the fat and muscle below the skin. The receiver electrodes are connected to the receiver circuit with one electrode connected to ground and the other connected to the input of a comparator. The circuit is similar to the ultrasound circuit with some differences. The highpass filter at the input was changed to have a cutoff frequency of 15. kHz as the operating frequency is between 100 and 1000 kHz. Because of the higher frequency a higher gain bandwidth product and higher slew rate for the amplifier and comparator were needed as well. These qualities were found in the AD8056NZ and MAX907EPA+ for the amplifier and comparator respectively. The circuit can be seen in figure 5.3.

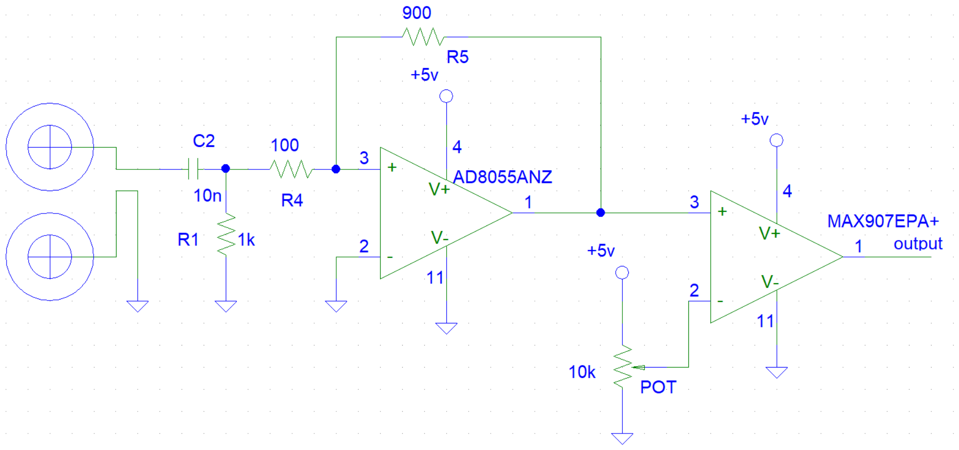


Figure 5.3: GC receiver circuit

5.4.1. Test setup

To test GC, it was important to isolate the wires and ground loops as there is they can make the signal appear through means other than galvanic coupling. This became clear through preliminary tests, in which the signal strength did not change upon changing the distance between electrode pairs.

To verify whether galvanic coupling is actually occurring or if it might be coupled through some other medium, tests were done without the receiver circuit. As the medium of human tissue can be modeled as a network of RC-circuits [21], larger distance should correspond to larger resistance and capacitance. To test this electrodes were put on a leg as can be seen in 5.5. The transmitter electrode pair was connected to the MCU. The laptop charger was disconnected from the mains to prevent possible ground loops.

5.4.2. Test results

To succesfully transfer data with the circuit shown in figure 5.3, it was required the high voltage was not overlapping with the low voltage. As can be seen in the waveforms of figure 5.5, this is the case in figure 5.5a, but in figures 5.5b to 5.5d the noise made the high and low voltage overlap sometimes. This could result in jittery data at the output of the comparator. Interestingly, there is a peek at the rising and falling edge of the signal, signifying a differentiating behaviour of the channel. After this, figures 5.5a and 5.5b look like discharging capacitors.

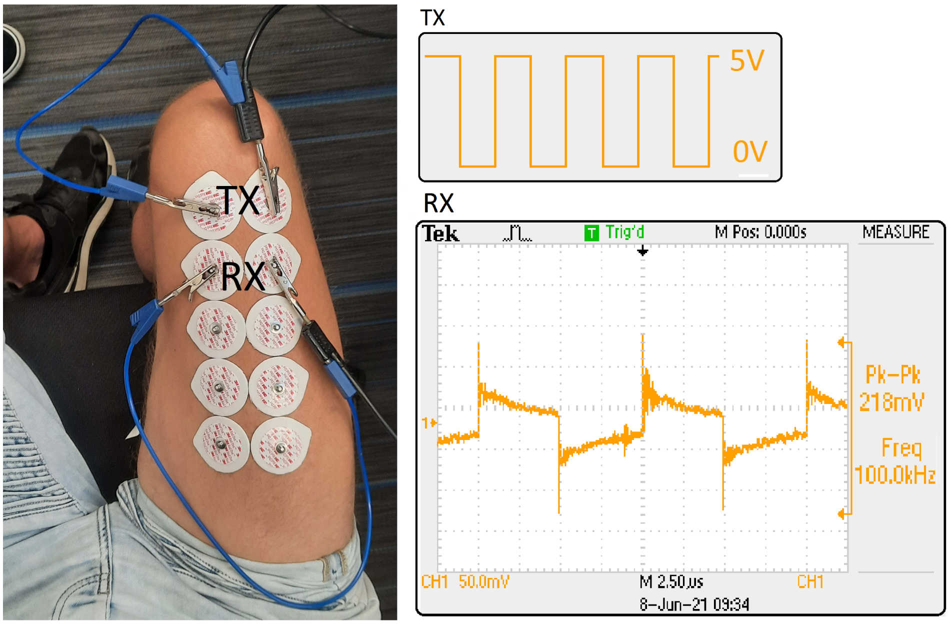
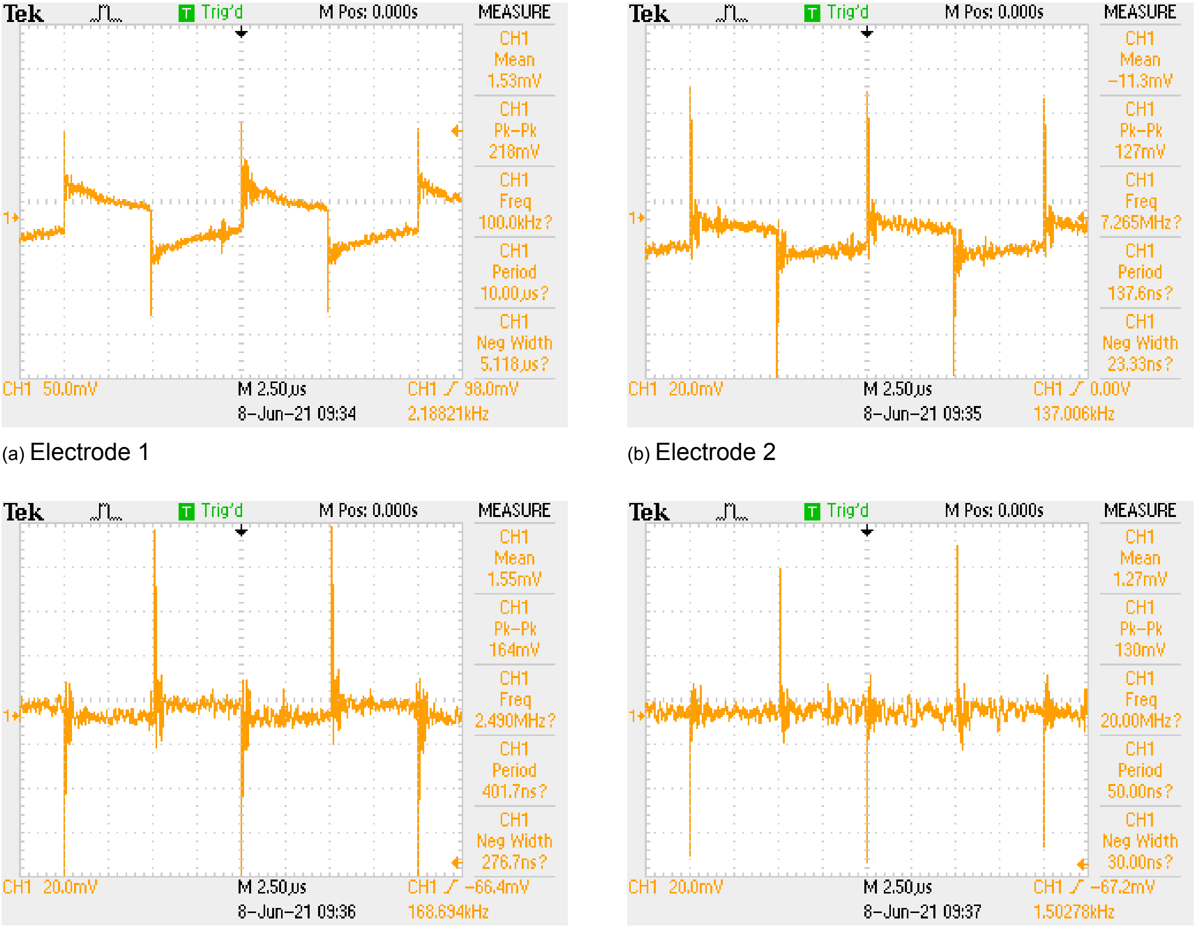


Figure 5.4: Test setup

To test the security and ability to eavesdrop on the galvanic coupling setup, tests were done with the transmitter electrodes connected to the MCU and the receiver electrodes disconnected. An oscilloscope was used to try and pickup the PWM signal from air at varying distance and frequency. The setup is shown in 5.6. The test results are show in table 5.2. According to the comparison in 4.1 the signal should not be detectable at a distance of about 40cm. However due to the fact that on body electrodes were used there is also some coupling with the electric field surrounding the body. The effect that occurs is very similar to how galvanic coupling works where the signal travels through air. The final product would consist of an implant which means that the transmitter is confined in the body, but in order to pair with the phone a pair of electrodes of some sort is needed. This would mean that during the pairing it might be possible to pick up the signal that is being sent. As seen in table5.2 the high and low signals are difficult to distinguish at a distance of around 30cm. In an other study[21] it was found that for galvanic coupling the bit error rate at 2cm was 0.03 and at 5cm was already 0.1 which slowly increased with the distance. This shows that even if the signal is picked up there is still a significant bit error rate which makes deciphering the key difficult.

Distance [cm]	Vpp [mV]	Comment
60	2.64	No visible signal at this distance, voltage coming from noise
50	2.48	Very slightly visible high and low voltage signal, noise still dominates
40	2.56	Rising and falling edges become visible
30	4.00	Clear rising and falling edges, but low and high voltage still overlap due to noise
20	4.24	Hardly any overlap between low and high voltage
10	5.36	No overlap between low and high voltage
5	6.56	No comment
1	9.28	No comment
0.1	9.36	Distance was difficult to keep precise but was estimated to be around 0.1cm
0	164	Contact with the skin makes for a very distinguishable signal

Table 5.2: Comments on waveform for 100kHz and varying distances



(a) Electrode 1

(b) Electrode 2

(c) Electrode 3

(d) Electrode 4

Figure 5.5: Four receiver pair positions at 100kHz

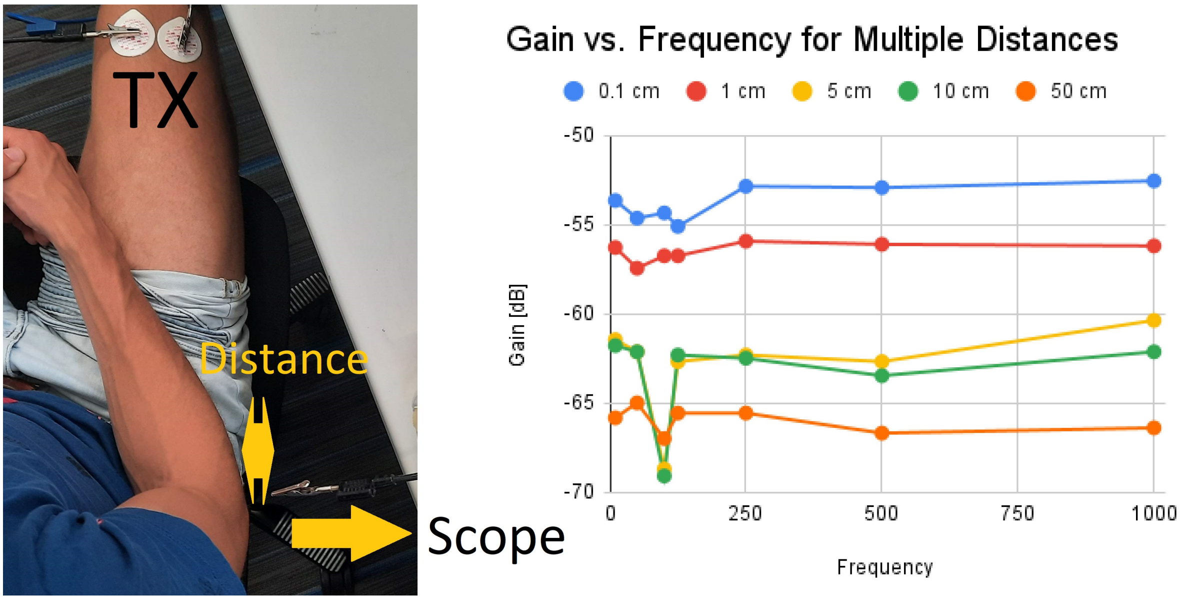


Figure 5.6: Test over air

6 Discussion and Conclusion

Here, NFC, ultrasound and galvanic coupling will be compared with each other based on the literature study and the test results.

6.1. Discussion

6.1.1. Security

The security is the most important aspect of the OOB channel as this is the whole reason for using an OOB channel in the first place. According to the literature study ultrasound is the most secure when used in the MHz frequency range or higher. In that case the signal only travels less than one centimeter outside of the body which means that an attacker has to practically hold the receiver onto the body of the patient.

Galvanic coupling is the second best option as the signal could only picked up if when the receiving electrodes are applied to the body. During this time it is possible to detect the signal that is being transmitted, but the bit error rate already becomes quite high at a distance of around 5cm. This makes an attack such as eavesdropping possible, but very difficult.

Even though NFC is protected against MITM attacks, it can be eavesdropped upon up to a distance of 10m. This makes NFC the least safe in therm of security.

6.1.2. Data rate

The data rate of the channel is not a limiting factor as only a key of 128 bits has to be transmitted. However, one should keep in mind that to improve the security of the BLE communication a longer key could be transmitted to make it harder to decipher.

Ultrasound is able to achieve a data rate of 28.12Mbps which makes it the fasted OOB channel out of the three. For OOB pairing this data rate is unnecessary, but it shows that ultrasound can also be implemented in WBANs that require communication at a high data rate.

Galvanic coupling has the second highest data rate which is 1.23 Mbps and NFC has the lowest data rate being only 424 kbit/s.

6.1.3. Health safety

Health safety is always an important aspect to consider especially when it comes to devices that are placed inside of the body for medical purposes.

The MPE of ultrasound is set at 720 mW/cm^2 which means that the intensity can be 147 times larger when compared to NFC as this has a MPE of 4.89 mW/cm^2. And when compared to GC which has a MPE of 2 mW/cm^2 it can even be 360 times larger. The reason why the intensity can be so much larger is because ultrasound does not send electrical waves but mechanical pressure waves through the body, which do not have ionizing properties. This makes it less likely for tissue heating to occur.

Most RF based channels have stricter limits than galvanic coupling, but because NFC operates at a fairly low frequency the MPE is quite a bit higher. This means that NFC is safer to use when compared to galvanic coupling which operates at a range of 10 to 100 MHz.

6.1.4. Power consumption

Power consumption is an important factor because of the size restriction of implants. NFC modules use a relatively high amount of power, even without considering the MCU. Galvanic coupling has power use similar to NFC, but as this is still an experimental method this surely can be improved upon.

6.1.5. Feasibility

The feasibility of the OOB channel defines how easy it is to integrate with the mobile phone and how easy it is to be operated.
NFC has a clear edge when it comes to this and is also one of the main reasons why it was chosen to further investigate. The fact that NFC readers are very common in mobile phones nowadays means that no additional hardware is needed. This means that patients, but also doctors and nurses, can easily pair with the implant in a matter of seconds.
Compared to NFC ultrasound and galvanic coupling both perform much worse in feasibility as it requires an additional receiver circuit. Galvanic coupling is slightly easier to use when compared to ultrasound. The ultrasound transducer has to be placed in the line of sight of the other transducer while the contact electrodes for galvanic coupling can be placed in a much wider range around the implant.

6.2. Conclusion

In terms of security, health safety and power use; ultrasound has shown to be significantly better than the other methods. It also has a data rate that is comparable to the other methods, but there is one significant downside which is the feasibility. To be secure and small, ultrasound transducers with a frequency of 1MHz or more must be used which are not currently available for commercial use but are being used in industrial and academic environments. Galvanic coupling offers adequate performance in all metrics considered, and does not need special transducers to operate but this is the most significant advantage over ultrasound. NFC has the privilege of already being implemented in modern smartphones, this however appears to be the only advantage it offer over the other methods.

6.3. Future work

As NFC is already a standard protocol, not much can be changed about this. The most progress should be made in power consumption and security, because on these aspects it lacks severely and they cannot be compromised. Future work implementing an MBAN should consider ultrasound, as it is a promising OOB pairing method.

Bibliography

[1] World Health Organization. *Epilepsy fact sheet*. website. June 2021. [Online]. URL: https://www.who.int/news-room/fact-sheets/detail/epilepsy.

[2] Emmanouil Georgakakis et al. “An Analysis of Bluetooth, Zigbee and Bluetooth Low Energy and Their Use in WBANs”. In: *Wireless Mobile Communication and Healthcare*. Ed. by Konstantina S. Lin James C.and Nikita. Berlin, Heidelberg: Springer Berlin Heidelberg, 2011, 168–175”.

[3] Marc S. Wegmüller. “Intra-body communication for biomedical sensor networks”. en. PhD thesis. Zürich: ETH Zurich, 2007. DOI: 10.3929/ethz-a-005479240.

[4] Manoj Kumar. “Security Issues and Privacy Concerns in the Implementation of Wireless Body Area Network”. In: *2014 International Conference on Information Technology*. 2014, pp. 58–62. DOI: 10.1109/ICIT.2014.73.

[5] William J. Tomlinson et al. “Comprehensive Survey of Galvanic Coupling and Alternative Intra-Body Communication Technologies”. In: *IEEE Communications Surveys Tutorials* 21.2 (2019), pp. 1145–1164. DOI: 10.1109/COMST.2018.2879643.

[6] David Naranjo et al. “Past Results, Present Trends, and Future Challenges in Intrabody Communication”. In: *Wireless Communications and Mobile Computing* 2018 (Mar. 2018), pp. 1–39. DOI: 10.1155/2018/9026847.

[7] A. Jara et al. “Heart Monitoring System based on NFC for Continuous Analysis and Pre-processing of Wireless Vital Signs”. In: 2018.

[8] Archana Yarlagadda. “Designing a Wireless Heart Rate Monitor with Remote Data Logging”. In: 2010.

[9] Thomas Bos et al. “Enabling Ultrasound In-Body Communication: FIR Channel Models and QAM Experiments”. In: *IEEE Transactions on Biomedical Circuits and Systems* 13.1 (2019), pp. 135–144. DOI: 10.1109/TBCAS.2018.2880878.

[10] Muhammad Ali Siddiqi et al. “Securing Implantable Medical Devices Using Ultrasound Waves”. In: *IEEE Access* PP (May 2021), pp. 1–1. DOI: 10.1109/ACCESS.2021.3083576.

[11] W. K. Chen et al. “Design of Galvanic Coupling Intra-Body Communication Transceiver Using Direct Sequence Spread Spectrum Technology”. In: *IEEE Access* 8 (2020), pp. 84123–84133. DOI: 10.1109/ACCESS.2020.2991206.

[12] Anna Vizziello et al. “PHY Design and Implementation of a Galvanic Coupling Testbed for Intra-Body Communication Links”. In: *IEEE Access* 8 (Dec. 2020). DOI: 10.1109/ACCESS.2020.3029862.

[13] Assefa K. Teshome, Behailu Kibret, and D. Lai. “Galvanically Coupled Intrabody Communications for Medical Implants: A Unified Analytic Model”. In: *IEEE Transactions on Antennas and Propagation* 64 (2016), pp. 2989–3002.

[14] ETSI. *https://www.etsi.org/technologies/medical-devices*. URL: https://www.etsi.org/technologies/medical-devices. accessed:16-6-2021.

[15] Mohd. Noor Islam and M. Yuce. “Review of Medical Implant Communication System (MICS) band and network”. In: *ICT Express* 2 (2016), pp. 188–194.

[16] Arnaud Vena, Etienne Perret, and Smail Tedjini. “1 - Introduction to RFID Technologies”. In: *Chipless RFID based on RF Encoding Particle*. Ed. by Arnaud Vena, Etienne Perret, and Smail Tedjini. Elsevier, 2016, pp. 1–26. ISBN: 978-1-78548-107-9. DOI: https://doi.org/10.1016/B978-1-78548-107-9.50001-X. URL: https://www.sciencedirect.com/science/article/pii/B978178548107950001X.

[17] Laura Galluccio et al. “Challenges and implications of using ultrasonic communications in intra-body area networks”. In: Jan. 2012, pp. 182–189. DOI: 10.1109/WONS.2012.6152227.

[18] Thomas P. Diakos et al. “Eavesdropping near-field contactless payments: a quantitative analysis”. In: *The Journal of Engineering* 2013.10 (), pp. 48–54.

[19] Ernst Haselsteiner and Klemens Breitfuß. “Security in Near Field Communication (NFC)”. In: (2013).

[20] Christos Strydis Muhammad Ali Siddiqi1 Wouter A. Serdijn. “Zero-Power Defense Done Right: Shielding IMDs from Battery-Depletion Attacks”. In: *Journal of Signal Processing Systems* 93 (2021), pp. 421–437. DOI: https://doi-org.tudelft.idm.oclc.org/10.1007/s11265-020-01530-5.

[21] William Tomlinson et al. “Secure On-skin Biometric Signal Transmission using Galvanic Coupling”. In: May 2019. DOI: 10.1109/INFOCOM.2019.8737540.

[22] Ilka Dove. “Analysis of Radio Propagation Inside the Human Body for in-Body Localization Purposes”. In: *Telecommunication Engineering Group, Faculty of Electrical Engineering, Mathematics and Computer Science, University of Twente* 2014 ().

[23] Emrecan Demirors et al. “High data rate ultrasonic communications for wireless intra-body networks”. In: *2016 IEEE International Symposium on Local and Metropolitan Area Networks (LANMAN)*. 2016, pp. 1–6. DOI: 10.1109/LANMAN.2016.7548843.

[24] G. Enrico Santagati and Tommaso Melodia. “Experimental Evaluation of Impulsive Ultrasonic Intra-Body Communications for Implantable Biomedical Devices”. In: *IEEE Transactions on Mobile Computing* 16.2 (2017), pp. 367–380. DOI: 10.1109/TMC.2016.2561277.

[25] MirHojjat Seyedi et al. “An energy-efficient pulse position modulation transmitter for galvanic intrabody communications”. In: *2014 4th International Conference on Wireless Mobile Communication and Healthcare - Transforming Healthcare Through Innovations in Mobile and Wireless Technologies (MOBIHEALTH)*. 2014, pp. 192–195. DOI: 10.1109/MOBIHEALTH.2014.7015943.

[26] IEEE Std C95.1-2019. *IEEE Standard for Safety Levels with Respect to Human Exposure to Electric, Magnetic, and Electromagnetic Fields, 0 Hz to 300 GHz*.

[27] International Commission on Non-Ionizing Radiation Protection (ICNIRP). *Guidelines for limiting exposure to timevarying electric, magnetic, and electromagnetic fields (up to 300GHz)*. 1997.

[28] *Near Field Communication (NFC) controller*. PN532. Rev. 3.6. NXP. Oct. 2017.

[29] G. Enrico Santagati and Tommaso Melodia. “Sonar Inside Your Body: Prototyping Ultrasonic Intra-body Sensor Networks”. In: *IEEE Conference on Computer Communications* (2014).

[30] NFC Direct. *NFC Phone List*. URL: https://www.nfcdirect.co.uk/nfc-information/nfc-phone-list.htm. accessed:9-6-2021.

[31] M. Mareli et al. “Experimental evaluation of NFC reliability between an RFID tag and a smartphone”. In: Sept. 2013. DOI: 10.1109/AFRCON.2013.6757740.

[32] Username ’Pillar1989’. *PN532 library for Arduino*. GitHub. June 2021. [Online]. URL: https://github.com/Seeed-Studio/PN532#start-of-content.

A

NFC code

A.1. Tag Reader

```

#if 0
#include <SPI.h>
#include <PN532_SPI.h>
#include <PN532.h>
#include <NfcAdapter.h>

PN532_SPI pn532spi(SPI, 10);
NfcAdapter nfc = NfcAdapter(pn532spi);
#else

#include <Wire.h>
#include <PN532_I2C.h>
#include <PN532.h>
#include <NfcAdapter.h>

PN532_I2C pn532_i2c(Wire);
NfcAdapter nfc = NfcAdapter(pn532_i2c);
#endif

void setup(void) {
    Serial.begin(9600);
    Serial.println(”NDEF Reader”);
    nfc.begin();
}

void loop(void) {
    Serial.println(”\nScan a NFC tag\n”);
    if (nfc.tagPresent())
    {
        NfcTag tag = nfc.read();
        tag.print();
    }
    delay(5000);
}
```

A.2. Tag Emulation

```


#include ”emulatetag.h”
#include ”NdefMessage.h”

#if 1
  #include <SPI.h>
  #include <PN532_SPI.h>
  #include ”PN532.h”

  PN532_SPI pn532spi(SPI, 10);
  EmulateTag nfc(pn532spi);
#elif 0
  #include <PN532_HSU.h>
  #include <PN532.h>

  PN532_HSU pn532hsu(Serial1);
  EmulateTag nfc(pn532hsu);
#endif





uint8_t ndefBuf[120];
NdefMessage message;
int messageSize;

uint8_t uid[3] = { 0x12, 0x34, 0x56 };

void setup()
{
  Serial.begin(115200);
  Serial.println(”------- Emulate Tag --------”);

  message = NdefMessage();
  message.addUriRecord(”Hello World!”);
  messageSize = message.getEncodedSize();
  if (messageSize > sizeof(ndefBuf)) {
      Serial.println(”ndefBuf is too small”);
      while (1) { }
  }

  Serial.print(”Ndef encoded message size: ”);
  Serial.println(messageSize);

  message.encode(ndefBuf);

  // comment out this command for no ndef message
  nfc.setNdefFile(ndefBuf, messageSize);

  // uid must be 3 bytes!
  nfc.setUid(uid);

  nfc.init();
}

void loop(){
    // uncomment for overriding ndef in case a write to this tag occured
    nfc.setNdefFile(ndefBuf, messageSize);

    // start emulation (blocks)
    nfc.emulate();

    // or start emulation with timeout
    if(!nfc.emulate(1000)){ // timeout 1 second
      Serial.println(”timed out”);
    }

    // deny writing to the tag
     nfc.setTagWriteable(false);

    if(nfc.writeOccured()){
       Serial.println(”\nWrite occured !”);
       uint8_t* tag_buf;
       uint16_t length;

       nfc.getContent(&tag_buf, &length);
       NdefMessage msg = NdefMessage(tag_buf, length);
       msg.print();
    }

    delay(1000);
}
```

B

Ultrasound and Galvanic Coupling code

B.1. Transmitting code

```
//com4
const int ledPin = 12;

// setting PWM properties
const int freq = 40000;
const int ledChannel = 0;
const int resolution = 8;
const int dutyCycle = 125;

void setup()
{
    Serial.begin(115200);
     // configure LED PWM functionalitites
  ledcSetup(ledChannel, freq, resolution);

  // attach the channel to the GPIO to be controlled
  ledcAttachPin(ledPin, ledChannel);

}

void loop()
{
   send(”Data that has to be send”);
   delay(1000);
}

void send(String msg)
{
   byte ch;
   unsigned int pos = 0;
   unsigned int sz = msg.length();
   while(pos<sz)
   {
      ch = msg.charAt(pos);
      Serial.print((char)ch);
      ledcWrite(ledChannel, dutyCycle);
      delayMicroseconds(700);
      ledcWrite(ledChannel, 0);
      for(int i=0;i<8;i++)
      {
         boolean b;
         b = bitRead(ch,7-i);
         if(b)
         {
            ledcWrite(ledChannel, dutyCycle);
            delayMicroseconds(400);
         }
         else
         {
            ledcWrite(ledChannel, dutyCycle);
            delayMicroseconds(200);
         }
        ledcWrite(ledChannel, 0);
         delayMicroseconds(600);
      }
      pos++;
   }
}
```

B.2. Receiving code

```
//com port is com 15

int pos = 0;
unsigned char CH = 0;
unsigned int bits1 = 0;
boolean capture = false;
boolean reference = true;
const int PinIn = 26;
int readings[] = {0,0,0,0,0,0,0,0,0};
int Treshold_High = 9999;
int Treshold_Med = 9999;
int Treshold_Low = 9999;
int array_test[2000];


void setup()
{
   Serial.begin(115200);
   pinMode(PinIn,INPUT_PULLUP);
}

void loop()
{
   if(digitalRead(PinIn))
   {
      bits1 = 0;
      unsigned long deltaT = micros();
      while(micros()-deltaT <= 1000) if(digitalRead(PinIn)) bits1 ++;
//      Serial.println(bits1);
      if(reference)
      {
        readings[pos] = bits1;

        if ((pos > 0)&&(readings[pos] > readings[0])) //this checks if the current amount of bits is the highest in the string and if so it puts it in the first position and resets the counter
        {
          readings[0] = readings[pos];
          pos = 0;
//            Serial.println(readings[0]);
        }

        pos++;
        if (pos > 8)
        {
        int min_value = 9999;
        int max_value = 0;
        // Finds the maximum and the minimum amount of pulses in the array
          for (int i = 1; i<9; i++)
          {
            if(readings[i] < min_value)
            {
              min_value = readings[i];
            }
            if(readings[i] > max_value)
            {
              max_value = readings[i];
            }
          }
          // Assigns the threshold values based on the max and min values
          Treshold_High = max_value * 1.4;
          Treshold_Med = min_value + 0.5*(max_value - min_value);
          Treshold_Low = min_value *0.2;
          Serial.println(max_value);
          Serial.println(min_value);
          Serial.print(”High threshold is ”);
          Serial.println(Treshold_High);
          Serial.print(”Medium threshold is ”);
          Serial.println(Treshold_Med);
          Serial.print(”Low threshold is ”);
          Serial.println(Treshold_Low);
          pos = 0;
          reference = false;

        }
      }
        else
        {

      // Actual code to receive the data

      if(capture)
      {

         boolean b = 0;
         if(bits1 > Treshold_Med && bits1 < Treshold_High) b = 1;
         if(bits1 > Treshold_Low && bits1 < Treshold_Med) b = 0;
         if(b) bitSet(CH,7-pos); else bitClear(CH,7-pos);
         //Serial.print(b);
         pos++;
         if(pos == 8)
         {
            Serial.print((char)CH);
            pos = 0;
            capture = false;
         }
      }
//      Serial.print("\n amount of bits is ");
//      Serial.print(bits1);
      if((bits1 >Treshold_High))
      {
        pos = 0;
        capture = true;
      }
   }
   }
}
```