Future of paying? Exploring the possibilities of contactless payment with Ultra-Wideband technology

University of Turku
Department of Computing
Master of Science Thesis
Computer Science
May 2024
Joona Kairo

UNIVERSITY OF TURKU
Department of Computing

Joona Kairo: Future of paying? Exploring the possibilities of contactless payment with Ultra-Wideband technology

Master of Science Thesis, 95 p., 4 app. p.
Computer Science
May 2024

Contactless payment has streamlined in-store shopping, allowing for swift purchases without the need to input PIN codes. This convenience has been achieved with Near Field Communication (NFC), a radio protocol that works exclusively within short distances. While the limited range provides security, the technology itself is not inherently safe, as it remains susceptible to many potential threats such as eavesdropping and relay attacks.

This thesis examines a possible solution to contactless payment applications with the employment of alternative wireless radio technology known as Ultra-Wideband (UWB). In contrast to NFC, UWB boasts verifiable security features due to its extremely short pulse length, enabling accurate distance measurement between two devices. These capabilities have made UWB a preferred choice for indoor positioning systems. With added security and the ability to know a person's position in centimeter-level accuracy, UWB holds the potential to enhance payment and introduce novel methods to pay.

To find out the viability of this new payment system, interviews were conducted with experts in UWB technology. These interviews sought to address the applicability of UWB technology for payment purposes, the mechanics of such a system, and the challenges that may impede its successful implementation.

According to the interviews, a potential UWB payment solution would involve smartphones, tailored mobile applications to individual stores, and UWB infrastructure. UWB technology would be used to locate and authenticate customers, with the actual payment happening through a mobile application utilizing online payment. The payments would take place separately from regular payment terminals, as the integration of UWB into existing payment terminals would require a long standardization procedure. The system's main challenges involve regulatory constraints, lack of standards and UWB's exclusive availability on premium smartphones.

Keywords: UWB, contactless payment, mobile, security, NFC, positioning

TURUN YLIOPISTO
Tietotekniikan laitos

JOONA KAIRO: Future of paying? Exploring the possibilities of contactless payment with Ultra-Wideband technology

Pro gradu -tutkielma, 95 s., 4 liites.
Tietojenkäsittelytiede
Toukokuu 2024

Lähimaksaminen on virtaviivaistanut myymälöissä asioimista mahdollistamalla nopean ostamisen ilman PIN-koodin syöttämistä. Tämä käytännöllisyys on saavutettu Near Field Communication (NFC) -radiotekniikalla, joka toimii yksinomaan lyhyellä etäisyydellä. Vaikka sen rajallinen kantama takaa suojaa, NFC-teknologia itsessään ei ole täysin turvallinen, koska se on altis monille uhille, kuten salakuuntelulle ja välityshyökkäyksille.

Tässä tutkimuksessa tarkastellaan mahdollista lähimaksusovellusratkaisua käyttämällä vaihtoehtoista langatonta radiotekniikkaa nimeltä Ultra-Wideband (UWB). Toisin kuin NFC, UWB:ssa on todennettavissa olevat suojausominaisuudet erittäin lyhyen pulssin pituuden ansiosta, mikä mahdollistaa tarkan etäisyysmittauksen kahden laitteen välillä. Nämä ominaisuudet ovat tehneet UWB:sta ensisijaisen valinnan sisäpaikannusjärjestelmiin. UWB:ssa piilee mahdollisuus parantaa maksamista ja tuoda käyttöön uusia maksutapoja sen paremman turvallisuuden ja senttimetrintarkan sijaintipaikannuksen ansiosta.

Uuden maksujärjestelmän toimivuuden selvittämiseksi UWB-tekniikan asiantuntijoita haastateltiin. Näillä haastatteluilla pyrittiin selvittämään UWB-tekniikan soveltuvuutta maksutarkoituksiin, järjestelmän mekaniikka, ja mahdolliset järjestelmän onnistunutta käyttöönottoa haittaavat haasteet.

Haastattelujen mukaan mahdolliseen UWB-maksuratkaisuun sisältyisi älypuhelimet, yksittäisiin liikkeisiin räätälöidyt mobiilisovellukset ja UWB-infrastruktuuri. UWB-teknologiaa käytettäisiin asiakkaiden paikantamiseen ja todentamiseen, kun taas varsinainen maksaminen tapahtuisi verkkomaksua hyödyntävän mobiilisovelluksen kautta. Maksut tapahtuisivat erillään tavallisista maksupäätteistä, sillä UWB:n yhdistäminen olemassa oleviin maksupäätteisiin vaatisi pitkän standardointimenettelyn. Järjestelmän suurimpia haasteita ovat sääntelyrajoitukset, standardien puute ja UWB:n saatavuuden olevan rajoittunut kalliisiin älypuhelimiin.

Asiasanat: UWB, lähimaksu, mobiili, turvallisuus, NFC, paikannus

Contents

1 Introduction **1**

2 Ultra-Wideband technology **4**

2.1 History and technical aspects 5

2.2 Applications 10

2.3 Regulations 14

2.4 Standards 16

2.5 Comparison to similar technologies 22

3 Contactless payment **26**

3.1 Research on UWB payment 27

3.2 Contactless payment technologies 28

3.3 Mobile payment 30

3.4 Security 35

4 Research method **43**

4.1 Hypotheses and interview questions 43

4.2 Interviewees selection 45

4.3 Interview structure 46

5 Results **48**

5.1 The UWB market 48

5.1.1 Advantages of UWB 48
5.1.2 Current market segments 49
5.1.3 Improving the availability of UWB 50
5.1.4 Potential consumer markets 52
5.1.5 Replacing narrowband technologies with UWB 55
5.2 Paying with UWB 58
5.2.1 The main problems 58
5.2.2 Building a UWB payment system 61
5.2.3 Addressing presumptions 65
5.2.4 How UWB changes payment 69

6 Discussion **72**

6.1 Future implications of UWB 72
6.2 UWB payment 74
6.2.1 System description 75
6.2.2 Benefits 77
6.2.3 Challenges 78
6.2.4 Payment methods 79
6.2.5 Securing UWB payment 86
6.3 Limitations 89
6.4 Future research 90

7 Conclusion **92**

References **96**

Appendices

A Interview Questions **A-1**

B Haastattelukysymykset **B-1**

List of Figures

2.1 Comparison of narrowband and UWB signal 6

2.2 How time of flight is calculated 7

2.3 The principle of detecting the first path 8

2.4 The frequency spectrum of UWB 15

2.5 The pulse repetition rates in LRP and HRP modes 18

6.1 How UWB payment could work in retail markets 76

List of Tables

2.1 UWB channels defined in HRP standard 20

3.1 Number of search results for UWB payment in Google Scholar 28

4.1 Summary of the interviewees 46

6.1 Comparison of UWB payment techniques 85

List of Acronyms

AOA Angle of Arrival.

ATM Automatic Teller Machine.

BLE Bluetooth Low Energy.

CCC Car Connectivity Consortium.

CIR Channel Impulse Response.

DAA Detect and Avoid.

DLL Data Link Layer.

DS-TWR Double-Sided Two Way Ranging.

ED/LC Early Detect/Late Commit.

ETSI European Telecommunications Standards Institute.

FCC Federal Communications Commission.

Gbps Gigabits per second.

GPS Global Positioning System.

HRP High-Rate Pulse.

LLC Logical Link Control.

LOS Line of Sight.

LRP Low-Rate Pulse.

MAC Medium Access Control.

Mbps Megabits per second.

MFi Made-For-iPhone.

MHz Megahertz.

mmWave Millimeter Wave.

mPOS Mobile Point-of-Sale.

NFC Near Field Communication.

NLOS Non-Line of Sight.

OSI Open Systems Interconnection.

PCI DSS Payment Card Industry Data Security Standard.

PHY Physical.

PIN Personal Identification Number.

POS Point-of-Sale.

PSD Power Spectral Density.

QR Quick Response.

RFID Radio Frequence Identification.

RSSI Received Signal Strength Indicator.

RTLS Real Time Location System.

SE Secure Element.

SSL/TLS Secure Sockets Layer/Transport Layer Security.

STS Scrambled Timestamp Sequence.

TDOA Time Difference of Arrival.

TOA Time of Arrival.

TOF Time of Flight.

TWG Technical Working Group.

TWR Two Way Ranging.

UWB Ultra-Wideband.

1 Introduction

The introduction of contactless payment to consumers has trivialized the complexity of a checkout procedure: obsolete practices such as needing to count cash or remembering PIN codes are redundant as a simple gesture is enough to complete the purchase. As the name suggests, contactless payment means no physical contact is needed with a card and a machine that processes payments. This has become possible with the addition of Near-Field Communication (NFC), a radio technology that allows short distance communication between two devices. NFC has made the purchase process easier than ever, as it only requires swiping a card next to a payment terminal.

While contactless payment has made buying simple and straightforward, the underlying radio communicating protocol poses several security issues. As a result, this thesis studies finding an alternative to NFC by using a more secure wireless technology known as Ultra-Wideband (UWB). The lack of security measures in other wireless technologies has already been noticed in the car industry, where the popularity of UWB has been steadily growing by ensuring secure keyless entry in vehicles.

UWB stands out for its unique ability to produce centimeter-level location accuracy, which has generated demand for indoor positioning systems. UWB is optimal for warehouses, factories and hospitals, which need high precision for tracking objects and personnel. However, outside business-level, UWB has not seen much success due to lack of viable consumer applications and its unavailability on most commercial devices.

The evolution of mobile phones has changed our lives in a way that we now use smartphones for everything. Payment is no exception, although the acceptance of mobile payment is obstructed due to the utility of bank cards. UWB has been projected to being the next big technological push in mobile markets, evidently explaining the sudden rise of integrated UWB chips in the newest smartphone models. It is therefore logical to expect a future UWB payment system to involve mobile payment.

The option to pay using UWB could be the needed traction for both UWB and mobile payment to establish ubiquity in the general public. Incorporation of location data can expand payment by including information on what happens before or after the purchase. Awareness of the buyer's exact location means that payment can be made anywhere in the vicinity, freeing the restriction of needing to be next to the payment terminal. Could the success of UWB-based mobile payment nullify the need for bank cards?

While previous research has focused on the accuracy and security of UWB, this is one of the first studies to touch upon the context of payment. As so, this thesis focuses on finding answers through conducting interviews with various experts in the most central fields. The interview results are thematically analyzed to find an explanation for many crucial questions such as whether UWB-based payment system is plausible, how the system will work technically, and what benefits it would generate.

Preceding the interviews, a background research was carried out on UWB technology and mobile payment to foster knowledge of the subject matter. Chapter 2 gives a technical explanation of how UWB works, while also revealing its current use cases and comparisons to other technologies. In Chapter 3, current payment technologies and mobile payment are analyzed, which contrasts their security differences. The methodology for conducting the interviews and the profiles of the participants are outlined in Chapter 4, while Chapter 5 presents the findings obtained from the interviews. Finally, Chapter 6 provides a comprehensive analysis on UWB payment.

This thesis is made in collaboration with Noccela, a Finnish UWB company that specializes on building custom positioning solutions to global industrial, retail, sport and healthcare markets. Noccela is continuously seeking new market areas for UWB, which is why they proposed me this topic. They believe UWB could enhance the purchase process with the addition of location data and security features.

2 Ultra-Wideband technology

Ultra-Wideband is a short-range wireless communication technology that uses wide bandwidth for fast and precise location tracking. A distinctive characteristic of UWB is its large bandwidth of 500 megahertz (MHz), a significant deviation from other wireless technologies such as Wi-Fi, which operates within a bandwidth range of 20 MHz to 80 MHz. This permits UWB to send and receive data at a high-speed rate. However, the main attraction of UWB lies in its accuracy: it is possible to pinpoint an object's location within a few centimeters, compared to other similar location-based technologies like GPS, which can only achieve accuracy within meters. [1]

Despite the potential of UWB to resolve common challenges in existing wireless technologies, its widespread adoption is hindered by several obstacles, like limited availability of consumer devices and regulatory constraints. Until these issues are addressed, it remains difficult for UWB to attain the same level of adoption as with other established technologies such as Bluetooth, Wi-Fi, GPS and NFC.

This chapter takes a closer look at the technicalities of UWB and its evolution over a century. It discusses the practical use cases, regulatory issues, standardization efforts and the predicted direction of UWB. A comparison between different wireless technologies is given in Section 2.5, highlighting the advantages of UWB over similar technologies.

2.1 History and technical aspects

UWB is not new technology itself but due to restrictions its commercial usage only became possible during this century. The origins of UWB trace back to the 20th century when the first radios were invented. In 1901, Guglielmo Marconi successfully sent Morse code sequences across the Atlantic Ocean using spark gap radio transmitters. Roughly half a century later, modern pulse-based transmission technology was first employed in military applications with the implementation of impulse radar systems. The realization of using this technology for communication systems emerged with the advent of impulse excitation and measurement techniques. This new UWB technology was restricted to military usage from 1960s to 1990s and was used for radar and communication applications. Originally, it was called base band until UWB name was termed in 1989. It was not until 2002 that UWB was approved for commercial use. [2]

The UWB system consists of tags and anchors. Tags are UWB devices that position needs to be tracked. A tag constantly sends radio signals that anchors then receive. Anchors are devices that are placed in fixed positions with a known location. Some devices can also act either as a tag or as an anchor. For instance, when two mobile devices are communicating, they can switch roles where one is a tag and one is an anchor. [3] Additionally, tag and anchor are also referred as initiator and responder, where the initiator (usually tag) starts the communication, and the responder (usually anchor) receives the message and responds back. The device that receives the message can also be referred to as receiver. Lastly, stationary anchors are also known as beacons.

The large bandwidth offers many advantages, such as high-speed data transmission and accurate pulse identification. UWB can transmit up to one billion pulses per second where each pulse can be identified [1]. The wide bandwidth enables the length of the signals to be only 2 nanoseconds, which allows the accurate deter-

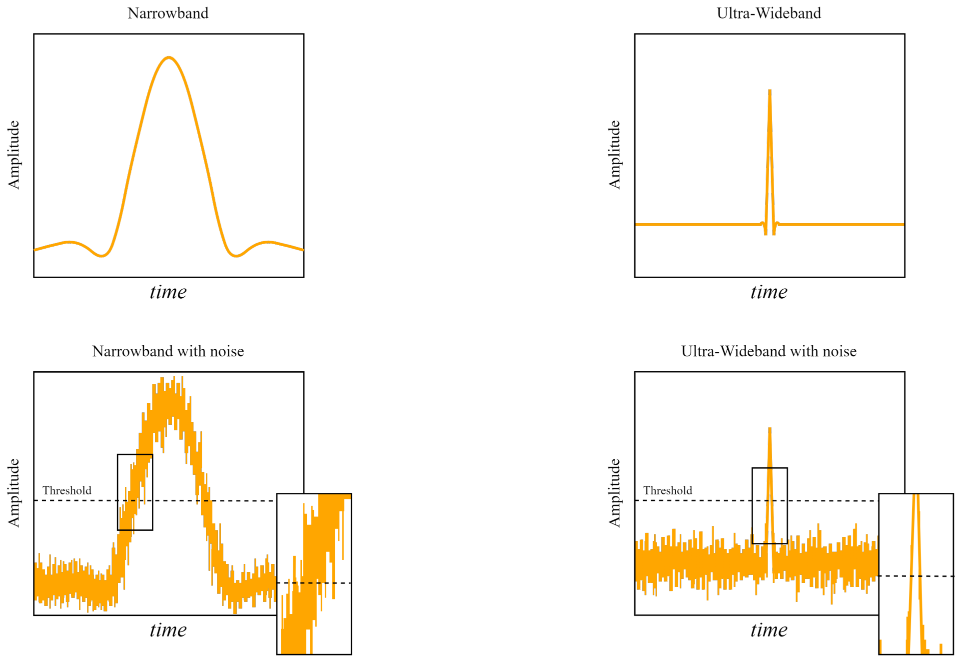

Figure 2.1: Comparison of narrowband and UWB signal. [7]

mination of distance and arrival time of each pulse [1, 4]. In addition, UWB has great channel capacity, which is better known as data rate. Data rate means the maximum amount of data that can be transmitted per second. Because UWB has several gigahertz of bandwidth availability, in theory it is possible to reach a data rate of gigabits per second (Gbps). [5] However, the data rate of modern UWB devices is much smaller due to different regulations and standards [6]. Still, the large bandwidth alongside UWB's low latency means it is possible to use UWB for real-time applications, making it an ideal solution for a system consisting of fast-moving objects [4].

Another advantage of UWB includes its robustness in challenging conditions. UWB has great resistance to intentional and unintentional jamming because UWB covers a wide range of frequencies. If one frequency is jammed, UWB can still work on the other frequencies. It works well in difficult environments: it can penetrate through walls and other objects, resist common wireless communication problems like multipath effect, and achieve high data rates even in noisy environments. [2, 5]

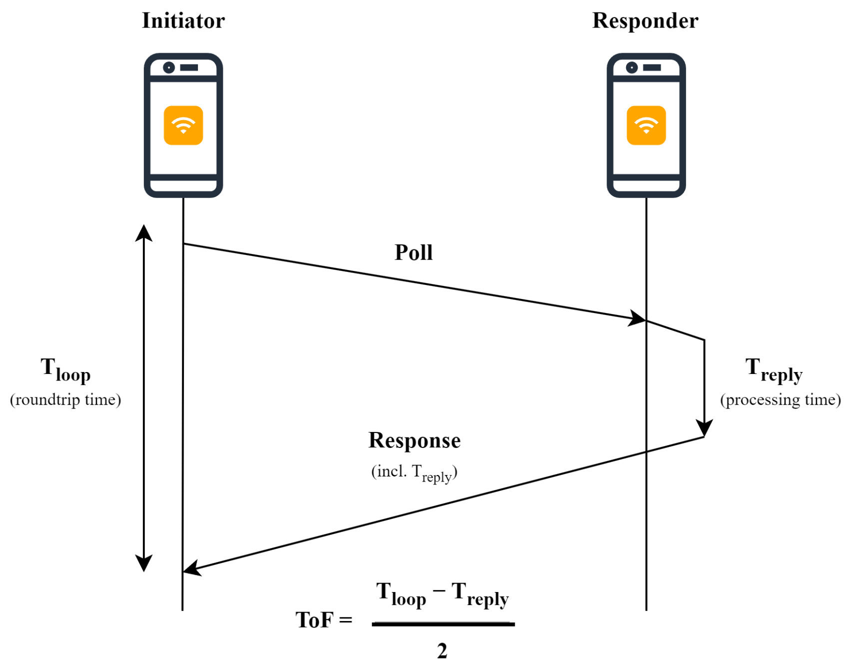

Figure 2.2: How time of flight is calculated. [8]

Because the pulses are extremely short, UWB enables precise measurement of the distance and position of a device. UWB sends short bursts of radio signals that have sharp rises and drops, making the signals' starts and stops easier to identify. As seen in Figure 2.1, narrowband technologies such as Bluetooth and Wi-Fi have longer signals, which makes it more difficult to estimate when the signal arrives. Moreover, narrowband signals are sensitive to interference, as even tiny amounts of noise causes altering to the signal. This complicates determining when a signal crosses a predefined threshold, leading to inaccuracies in distance measurement. In contrast, UWB signals maintain their distinctiveness even in the presence of noise. These characteristics of a UWB signal allow for the calculation of signal travel time between two UWB devices. This is used to calculate the distance between the two devices, which is a process known as ranging. [7] The time for the signal to travel between the two devices is known as time of flight (TOF). As illustrated in Figure 2.2, calculating TOF requires measuring a round-trip time, which is the time it takes for a signal to reach a responding device and back to the initiator device. Once this

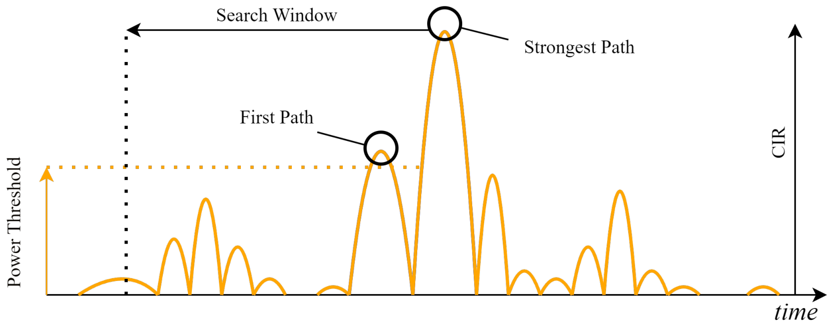

Figure 2.3: The principle of detecting the first path. [14]

value is known, it is subtracted by the known processing time of the responding device and divided by two, which results in TOF propagation time in one direction. When this value is multiplied with the speed of light, the result is the distance of the two devices. [9]

The accuracy of TOF depends on the accuracy of the signal's time of arrival (TOA) calculation. Time of arrival is calculated by performing cross-correlation between the received and expected signal. [10] It uses channel impulse response (CIR), where the compared signal builds CIR estimate. If the signal sequence correlates, it results in a strong peak. Pulses that do not match will result in weaker peaks or no peaks at all. TOA estimation is accepted if the correlation value is above a predefined threshold. [11] This is done to identify the correlation peak which relates to the first and most direct path of a signal between the two devices. Identifying the first path is important to accurately estimate the distance between the devices. [12] However, identifying the first path is not so simple. Ideally, the strongest correlation peak should refer to the first path but there can be situations where this is not the case. Multiple reflections and scenarios where the devices are not in line-of-sight can lead to several peaks where the strongest correlation peak is not the earliest path. This can be solved by conducting a back search after receiving the strongest peak to find a first peak that matches the expected signal. [10, 13] An example of this kind of scenario is given in Figure 2.3.

Two-Way Ranging (TWR) is one of the many localization techniques to determine the position of a tag. It uses the TOF calculation to get the distance between two devices. By incorporating multiple anchors, like three or four, various distance estimations are obtained that can then be used to determine the position of a tag. The continuous communication between the tag and the anchors causes the tag to consume more battery power. [3]

Another localization technique is called Time Difference of Arrival (TDOA). In this method, the tags send "blink messages" to nearby anchors. The anchors receive the tag's signal timestamp, which is then forwarded to a central location engine. The engine processes the timestamps and calculates the tag's position based on the differences in arrival times at each anchor. TDOA requires that the anchors are synchronized, but the benefit is that the tags use very little power. [3]

Different localization techniques are used depending on the use case of the UWB system. TWR is used in secure applications like hands-free access systems, while TDOA is more suitable for precise indoor tracking systems known as real-time location systems (RTLS) where the tag does not need to know its own location [3, 6].

The accuracy of UWB brings another intriguing benefit in the means of improved security. On other technologies, the distance measurement is determined by signal strength. This makes ranging inaccurate and vulnerable to distance manipulation, as it assumes that a strong signal means that a device is nearby. However, since UWB can determine distance using TOF, it makes ranging accurate but also secure. [8] These are discussed in more detail in Section 2.5 and Section 3.4.

When talking about ranging accuracy, it is important to note that the terms accuracy and precision are non-synonymous. Accuracy means how close to the target the estimated position is, while precision is used to describe the reliability and consistency of the estimation. For instance, a system with high precision but low accuracy can recognize that a person walked in a circular motion but incorrectly shows the person walking in a wrong room. [15] However, in this thesis the difference of the words is not important, and they are used interchangeably to mean accuracy. As the meaning of the words can be confusing, the word precision is mostly avoided in this thesis. Still, it needs to be noted that while UWB is accurate, it is also capable of high precision ranging [16].

The essence of UWB is it being able to solve inaccuracies in indoor positioning and security vulnerabilities present in other wireless technologies. While positioning systems using technologies such as Wi-Fi and Bluetooth Low Energy exists for indoor environments, they are not accurate due to their reliance on signal strength for ranging. UWB's centimeter-level accuracy promotes new innovations that were not possible before, which are discussed in the next section.

2.2 Applications

UWB has gained attention as more companies have begun adapting it to their own products. For consumers, UWB is still relatively new technology due to its exclusivity on high-end products. However, UWB has been adopted on enterprise-level for accurate and secure solutions. This section examines what current and future use cases UWB has. It also explores what plans technology companies have for UWB.

FiRa Consortium [8, 17] presents three core services where UWB technology could be useful at a user level: hands-free access control, location-based services, and device-to-device services.

1. Hands-free access control: UWB makes it possible to securely enter locked areas without any user input. In most modern access technologies, a user is required to perform an action, like type a keycode or tap a badge, to open a locked door. With UWB, however, the user would simply need to walk towards

the door and it opens. Similarly, leaving the area would lock the door. The user identification happens instantly, and the user is let through only if they have the rights.

2. Location-based services: A satellite-based GPS is the most used technology for location tracking, but UWB can bring a similar style service to indoor environments where the GPS signal does not work well. UWB can be used to navigate in large indoor areas, such as shopping malls or airports, and make it easier to find your car in a large parking garage.

3. Device-to-device services: As it is possible for two UWB devices to share their positioning data with each other, UWB brings several use cases for consumer applications. UWB-enabled smartphones can locate lost items, such as keys, wallets and backpacks if they have a UWB tag attached to them. Another interesting use case for UWB is an automated and personalized smart home system. Controlling smart devices could happen seamlessly: when a smartphone is directed at a device, a relevant control panel for that device would automatically open on the smartphone. Smart home systems can also detect the presence of a user. When a person enters a room, the UWB devices automatically notice the presence of the person, which could be used to turn on lights and play the person's favorite music.

For a long time, one of the primary use cases of UWB has been its use as a real-time location system (RTLS) in businesses, such as for asset and personnel tracking. In healthcare, a UWB-based RTLS solution can track availability of beds or track the location of patients and staff for safety purposes. During COVID-19 pandemic, UWB was also used for social distancing and contact tracing. UWB's robustness in harsh environments has made it a favored choice in factories and warehouses where various obstacles, such as machinery, can impact positioning accuracy. The capability for real-time location tracking enables UWB to be used for collision detection to improve worker safety. [8]

In recent years, UWB has seen a rise in smartphones but currently it is only available in high-end devices. Many technology companies, such as Apple, Samsung and Google, are finding ways to develop UWB at a customer level.

Apple is one of the biggest pioneers in UWB. They have designed their own UWB chip called U1 that is currently being used in many of Apple's products. For example, Apple is utilizing UWB in iPhone 11, 12 and 13, Apple Watch Series 6 and 7, and in AirTags, with the iPhone 11 being the first ever smartphone to include UWB technology. AirTags are small tags used for locating lost items and they can be placed on any objects, such as on keys. With an iPhone, it is possible to track the location of the AirTag. With the use of augmented reality, the iPhone will display a large arrow that points to the direction where the AirTag is located at. Apple has also made many patents related to UWB. These include shaping UWB pulses for more accurate distance measurements, using a UWB device to enter a car, and a system for authorizing a person that is trying to access a vehicle. [18]

Samsung has started to include UWB in their high-end devices, for example, in Note 20 Ultra and Galaxy Z Fold. Currently their smartphones utilize UWB for Nearby Share feature to find other compatible devices for data transfer and in SmartThings Find for locating a lost device. Samsung has also developed Digital Key, a UWB solution for unlocking car doors without traditional keys. [19]

Google joined the UWB market in 2021 when they introduced Google Pixel 6 Pro, which is their first ever smartphone to include a UWB chip. Similarly to other smartphone companies, Google is currently using it for their Nearby Share feature. They are also working on releasing an API which will allow third-party developers to have better access to the UWB chip and utilize it in their apps. [20]

Xiaomi has shown how UWB could be applied in a home environment. They produced a demo where by installing smart home equipment with UWB and using Xiaomi's Mi 10T smartphone they could control the devices simply by facing them. For example, facing a fan would bring a button to turn it on, and turning towards a music player would change the smartphone to show controls for adjusting the music volume. [19]

UWB has gained interest in using the technology for keyless access due to its high security potential. In 2021, BMW announced their wireless car key system Digital Key Plus. It was initially compatible with Apple devices and later became available on Android devices in 2023. The BMW Digital Key Plus replaces a traditional car key with smartphones that have UWB chips. The vehicle will open its doors and start the car automatically when the car owner approaches it without the person needing to get their phone out of their pocket. [21] Samsung has partnered with Korean car brand Genesis to support keyless access using UWB to Genesis GV60 [22]. In 2022, Samsung announced the world's first UWB-based smart lock system. It allows locking and unlocking of a smart lock with a Samsung smartphone equipped with UWB. Unlike NFC-based systems, a door with a smart lock does not need to be tapped with a smartphone. [23]

Although the focus for companies seems to be mainly to integrate UWB on smartphones and cars, UWB could see more adoption on other electronic devices, such as smart watches and laptops. For instance, UWB is already being used in Apple's Watch Series [18]. UWB-enabled smart watches have the same use cases that UWB-enabled smartphones have [8]. Lenovo uses UWB impulse radar in their ThinkPad X1 Nano –laptop for human presence detection. The value of this is that the laptop will automatically turn on and log-in once a user is close to the device and shut down when the user moves away. [24]

Other usages of UWB include being used for sports for location tracking and in computer hardware devices for high-speed data transfer [18]. The Qatar World

Cup 2022 included UWB tags inside the footballs for faster and more precise referee decisions [25]. NFL uses UWB to track player locations to produce player statistics [1].

Devices equipped with UWB have been predicted to grow to 1 billion in 2025, which is believed to happen as more smartphone manufacturers include UWB chips inside their devices [18].

2.3 Regulations

In February 2002, the US Federal Communications Commission (FCC) permitted unlicensed commercial usage of UWB devices. A radio signal is classified as Ultra-Wideband signal if its absolute bandwidth is at least 500 MHz or the fractional bandwidth is greater than 20% of its center frequency. FCC allocated unlicensed usage of 7.5 GHz between 3.1 GHz and 10.6 GHz frequency bands. [26, 27] FCC also prohibits UWB communication in toys, aircraft and satellites [27].

The UWB regulations were designed to protect other spectrum users from undesirable levels of interference caused by the transmissions, which is why the power spectral density (PSD) of UWB is low compared to other wireless communication systems. PSD is described as the ratio of power transmitted in watts and bandwidth of the signal in hertz. The huge bandwidth of UWB overlaps with the frequency bands of other wireless systems, which is why FCC limited the maximum average PSD to –41.3 dBm/MHz and the maximum peak PSD to 0 dBm/50MHz. The low PSD allows UWB to coexist with other wireless communication systems, like Wi-Fi, Bluetooth and GPS that use much higher PSD. This also makes UWB systems immune to detection and interception by other narrowband wireless communication receivers. [2, 26, 28] The current frequency spectrum of UWB and the overlapping of other wireless technologies is demonstrated in Figure 2.4. The sub-gigahertz band was defined in later standards of UWB [6].

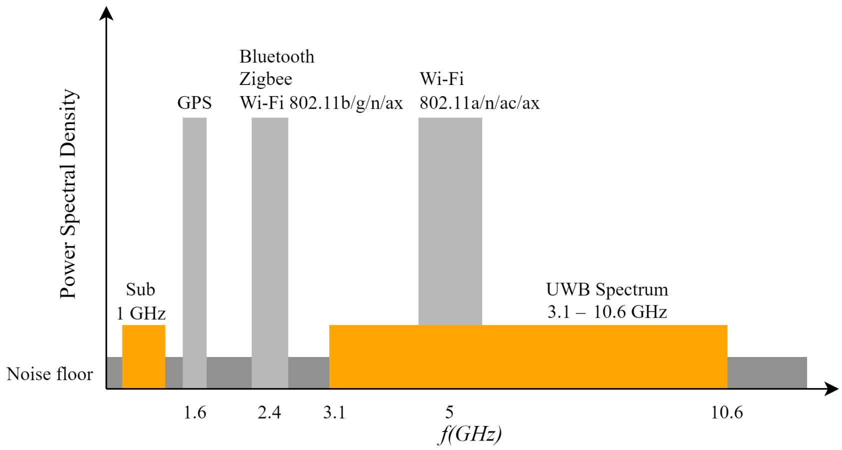

Figure 2.4: The frequency spectrum of UWB. [4]

In Europe, The European Telecommunications Standards Institute (ETSI) formed regulations that followed the same rules as stated by FCC but with some limitations. ETSI defined two bands instead of one single band, a low band of 3.1–4.8 GHz and an upper band of 6–9 GHz. [26, 29] UWB systems working on the lower band should follow detect and avoid (DAA) principle. The principle states that UWB systems should only operate if no other narrowband signals have been detected. [26] Similarly, the band of 8.5–9 GHz can only be used with DAA principle. This means that in Europe the only possible band with no mitigation techniques required is 6–8.5 GHz. [29]

For Asian markets, there does not seem to be a common regulation for UWB, instead countries use their own regulations. Most of the Asian countries allow the usage of UWB outdoors, but fixed outdoor devices are completely or partly prohibited except in China. [30] Japan followed similar regulations that were defined by ETSI, using two sub-bands where DAA principle for lower band usage is necessary [26]. However, the available spectrum width for UWB is smaller in Japan, as it only allows to use a low band of 3.4–4.8 GHz and a high band of 7.25–10.25 GHz. The required bandwidth for a signal to be classified as UWB is also different, as in Japan a UWB signal must have a bandwidth of at least 450 MHz. [29] Other Asian countries use similar regulations as defined by ETSI but with slight modifications. For example, in South Korea the permitted frequency range is 3.735–4.8 GHz and 7.2–10.2 GHz, in Vietnam and Malaysia it is 6–8.5, and New Zealand uses 2.7–4.8 and 6.0–8.5. [30]

For USA, Europe and Japan, the only common frequency band for indoor usage that does not require mitigations techniques is 7.25–8.5 GHz [29].

FiRa Consortium [8] believes that changes in the current FCC regulations would help the growth of UWB. The original regulations imagined UWB would become a high data rate communication technology, while it is used mainly for ranging and positioning. For these purposes, the current regulations are not befitting, as they do not permit the use of fixed outdoor devices. This holds back the rollout of UWB-based locks and RTLS systems. FiRa Consortium suggests changes in regulations, such as explicitly allowing the use of UWB in automobiles, additional spectrum above 10 GHz, permitting the usage of UWB in toys, and granting higher power indoors.

Currently, applications that do not meet the regulatory rules need to obtain waivers from FCC. The approval of waivers can take from half a year to multiple years. Additionally, the waivers are typically limited in scope. Regulatory changes would also benefit FCC, as the waiver process is not sustainable because the number of waiver requests will continue to rise as the number of UWB applications and devices increase. [8]

2.4 Standards

Standardization of Ultra-Wideband is important to achieve interoperability between different UWB manufacturers. Several organizations have been established to standardize UWB for different purposes. Due to these different standards, full compatibility between UWB devices can be difficult to achieve as not all UWB systems support the same standards, restricting the usage of UWB to devices with compatible radio chips. [6]

The IEEE Standards Association is a group that defines standards for various industries. The IEEE 802.15.4 standard has been used as a foundation for UWB standardization. It defines physical (PHY) and medium-access-control (MAC) layers based on the seven-layer Open System Interconnection (OSI) model. In 2007, the first UWB standard was developed in the form of IEEE 802.15.4a. In 2020, a redefined IEEE 802.15.4z standard was released, which improved the security and ranging measurements. [6]

UWB Alliance is an organization launched in 2018 that seeks to enable interoperability and promote UWB to the public. Several of their members have worked on the 804.15.4z standard to ensure that different UWB technologies can work together. The alliance aims to bring UWB to countries where regulations prohibit the use of the technology. They also want to ensure UWB interoperability with current Wi-Fi standards. [31]

In 2019, FiRa Consortium was formed together with several companies like Samsung, NXP and HID Global. The organization defines specifications and certifies the interoperability among UWB chips and devices. Their standardization is built on top of the IEEE 802.15.4z standard. [32]

Apple has implemented their own Apple Nearby Interaction standard for third-party developers to interact with UWB equipped Apple devices. Companies that want to be able to interact with Apple UWB chip need to be part of Made-For-iPhone (MFi) program. [6]

The Car Connectivity Consortium (CCC) is an organization to develop smartphone-to-car connectivity. Their standard, The Digital Key 3.0, defines secure UWB connection for vehicle access. [6]

Omlox is an open standard developed to standardize RTLS. It enables interop-

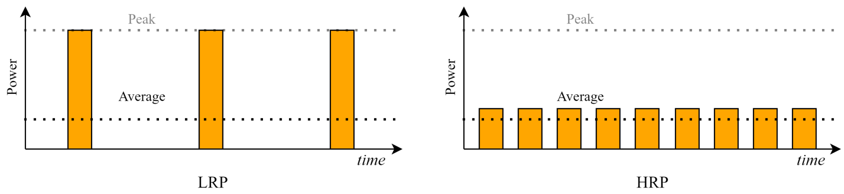

Figure 2.5: The pulse repetition rates in LRP and HRP modes. [28]

erability between different localization technologies and manufacturers. The omlox hub permits the integration between various localization technologies, such as UWB, Wi-Fi, GPS, 5G, RFID and BLE. [33]

The IEEE standard defines two modes for the PHY layer, High-Rate Pulse (HRP) and Low-Rate Pulse (LRP). The HRP mode transmits weak pulses at a higher rate in comparison to LRP that transmits stronger pulses but at lower rate. This is visualized in Figure 2.5. Because the transmission of data is limited by the power spectral density, both modes have equal maximum average transmitted energy. [6, 28]

HRP and LRP have different data rates, pulse repetition rates, ranging support and energy consumption. In the IEEE 802.15.4 standard, ranging is exclusively available with HRP mode. The 802.15.4z enhancement added support for LRP ranging and improved the data rate of LRP. [6] However, LRP data rate is still less than in HRP [6, 34]. Because HRP sends pulses in lower energy, a receiver will need a more complex design to be able to read the weak pulses from the noise. LRP receiver can be based on energy detection because of the stronger pulses. The energy consumption of the two modes is significant, as in short-range LRP consumes 6.4 times less energy and 100 times less energy in longer ranges. However, the accuracy of HRP is better than in LRP, making it more suitable for systems that prioritize accuracy, while LRP is more suitable for ultra-low power devices. [28] Simulation results indicate that LRP has greater accuracy over longer distances, although its long-distance mode also has the lowest data rate [34].

The MAC layer functions as an interface between the PHY and Logical Link

Control (LLC) layers. The MAC layer and the LLC layer are sublayers that together form the Data Link Layer (DLL), the second layer of the OSI model. [35] The MAC layer in the IEEE standard defines protocols that allow for different UWB devices to use the same channel, which ensures the devices are not interfering with each other. The IEEE 802.15.4z enhances the functionality of the MAC layer by adding localization techniques that were previously left up to the chip designer for implementation. The MAC message, which is also known as the MAC frame, did not change in the standard, meaning there are no compatibility issues between the different standards. [6]

When following the IEEE standard, it is not necessary to implement every feature listed in it, which means UWB chips following the same standard can vary in their implementation. UWB chips need to meet certain conditions to be compatible in PHY layer. The pulse shape must be similar, and the used center frequency and frame structure must be the same. [6]

The IEEE 802.15.4/4z HRP defines 16 channels or bands that divide the allocated spectrum of UWB as seen in Table 2.1. Some channels have the same center frequency but a different bandwidth. Each channel has a minimum of 499.2 MHz bandwidth. A UWB chip does not need to support every channel but it needs to support one of the three mandatory channels: channel 0 for sub-gigahertz operation, channel 3 for low-band operation, and channel 9 for high-band operation. For two UWB devices to be able to establish a connection, they need to have the same center frequency and bandwidth, meaning they must both support the same channel. [6]

Prominent UWB radio chip manufacturers such as Apple, Qorvo and NXP produce chips that support either the IEEE 802.15.4 standard or the IEEE 802.15.4z standard. The most widely used chip in the market, Qorvo DW1000, only supports the IEEE 802.15.4 HRP, meaning most of the commercially available UWB products use this standard and mode. [6] FiRa Consortium also chose to use HRP mode

Table 2.1: UWB channels defined in HRP standard. [6]

Channel	Center Frequency (MHz)	Bandwidth (MHz)
0	499.2	499.2
1	3494.4	499.2
2	3993.6	499.2
3	4492.8	499.2
4	3993.6	1331.2
5	6489.6	499.2
6	6988.8	499.2
7	6489.6	1081.6
8	7488	499.2
9	7987.2	499.2
10	8486.4	499.2
11	7987.2	1331.2
12	8985.6	499.2
13	9484.6	499.2
14	9984	499.2
15	9484.8	1354.97

for their certification [32]. Furthermore, smartphones currently only support UWB HRP [36].

To achieve compatibility, the UWB anchor and the tag should use the same localization technique. Some chip manufacturers like Qorvo and NXP do not implement the MAC layer, meaning these chips can be configured to use every localization technique available. Compatibility issues can arise in commercial products that use proprietary localization techniques or implement their own system for determining which technique to use. The IEEE 802.15.4z adds description of the most commonly used localization techniques to the MAC functional description which tells that these techniques should be supported in devices that implement the IEEE 802.15.4 standard. [6]

UWB device discovery must be compatible for the devices to start communicating with each other. The device discovery is a procedure where the UWB devices search for other devices that they can communicate with. Because UWB is more energy consuming than other wireless technologies, the search is usually done using technologies such as Bluetooth or NFC. The device discovery works similarly in FiRa standard and Apple Nearby Interaction, but they are not interoperable due to the different message that is being sent in the device discovery process. Similarly to localization techniques, companies can create their own proprietary device discovery methods, which complicates compatibility. [6]

Coppens et al. [6] suggest that future research could be done to define a standardization for AOA localization technique. To accurately measure a tag's location, there needs to be at least three or four anchors. Angle of arrival (AOA) technique uses multiple antennas to measure the distance. It effectively estimates the distance by only needing one anchor. Currently, there is no standard for AOA estimation, which means each UWB system can implement their own proprietary AOA measurement technique.

IEEE 802.15.4ab task group was formed in 2021 to enhance the PHY and MAC layers of the current IEEE 802.15.4z standard. The planned improvements include additional channels and operating frequencies, lower energy consumption, higher data rate, better support for a large number of tags, improved accuracy, and enhanced native discovery. The standard will be backwards compatible. [37]

FiRa Consortium [38] unveiled their latest standard, FiRa 2.0, in late 2023, offering technical specifications to various applications. These include enabling accurate indoor navigation for smartphones, assisting the localization of individuals or items in crowded areas, and allowing seamless control of connected UWB home devices using smartphones. FiRa Consortium [8] Technical Working Group (TWG) is working on standardizing UWB access control to ensure that locking and opening doors work even when the devices have been manufactured by different companies. The standardization would also make it possible to transfer the access control key to another device.

2.5 Comparison to similar technologies

Numerous wireless technologies are utilized in positioning systems, with Wi-Fi and Bluetooth being common options for indoor positioning due to their widespread availability. Bluetooth, or more specifically Bluetooth Low Energy (BLE), gained attention when Apple announced its iBeacon protocol [7]. In addition, there is GPS, which is the most used technology for outdoor positioning. Currently, UWB's most popular use case is using it for positioning systems due to its high accuracy. Therefore, this section will focus on comparing UWB to these other three technologies in their functionality as positioning systems.

The method for determining distance in UWB, BLE and Wi-Fi differ significantly, as BLE and Wi-Fi use received signal strength indicator (RSSI) while UWB uses more accurate TOF calculations. As explained in Section 2.1, the signal characteristics of UWB and narrowband technologies vary, which is why these technologies have different ranging methods. BLE and Wi-Fi use RSSI for proximity detection, which means the device detects if it is in range of another device. It does not require distance calculations, instead only a steady signal is needed. The signal strength can be used to distinguish the distance of a device, with weaker signals indicating greater distance and stronger signals meaning closer proximity. However, relying solely on signal strength for distance estimation is not reliable, as low signal strength could mean that the device is far away but also that there is an object between the two devices. A technique called fingerprinting can be used to solve this problem, yet it still does not guarantee accurate location determination with RSSI. [7]

On the other hand, UWB makes it easy to accurately measure the distance of a device because of its shorter pulses. As a result, UWB can locate with an accuracy of up to 10 centimeters, compared to Wi-Fi and Bluetooth that can achieve accuracies of around 5 meters. [7] Arsan and Kepez [39] tested the accuracy of Wi-Fi, BLE and UWB in 36 m^2 area, and found an average error of 1.39 m for Wi-Fi, 0.86 m for BLE and 0.24 m for UWB.

Nevertheless, the high accuracy of UWB can primarily be achieved under line-of-sight (LOS) scenarios, where the signal reaches the receiver directly. In non-line-of-sight (NLOS) scenarios the transmitted signal only reaches the receiver through reflected path. [40] In the latter scenarios, the UWB system is significantly less accurate [16, 40].

There are also other differences between the three systems. UWB and Bluetooth consume less battery power than Wi-Fi, however, the main advantage of Wi-Fi is its prevalence in public and private places. Due to the better support of Bluetooth and Wi-Fi in mobile phones, it is easier for a system utilizing these technologies to interact with modern tablets and smartphones. [7] UWB has one major benefit over others, which is its resistance to a common problem with wireless connections known as multipath effect. Multipath effect happens when a radio signal reaches the receiver through more than one path. Immunity to the effect increases the accuracy of UWB. [9] When considering system costs, building a BLE system is more cost-effective than a UWB system. As BLE data rate is only 2 megabits per second (Mbps), UWB is more suitable for systems that send more data. UWB data rate is not as quick as Wi-Fi 6, which can reach speed of 2 Gbps. [1]

The different technologies do not necessarily have to compete against each other but used together to maximize efficiency and user experience. In access control, energy efficient BLE would initialize the communication between devices, while UWB takes care of the precise and secure ranging. Additionally, technology like NFC that does not need a power source can be used as a backup if the device's battery is drained. [8]

Global Positioning System (GPS) differs from the other technologies as it is a satellite-based positioning system. Due to its ease of access, it is one of the most used location-based solutions. The goal of the system is to provide accurate location information from any point on Earth from a satellite. The satellites are formed in such a way that at any point from Earth you will receive signals from 4 to 11 satellites. It works accurately outdoors but the accuracy gets worse if there are obstacles between the signal, making it unsuitable for indoors usage. The main error sources for GPS are ionospheric delay and multipath effect. [41]

A study shows that when comparing the accuracy of UWB and GPS localization in a tennis court, a UWB system provides significantly less localization error compared to a GPS system in both outdoor and indoor environments. UWB is not as accurate in 3D localization as it is in 2D localization, but even there it is still significantly more accurate than GPS. The results found out that the accuracy of the UWB system is great at the center of the field when a tag is within the range of all anchors, but the accuracy starts to drop once the tag moves closer to the boundaries. The accuracy of UWB localization can be increased by increasing the number of anchors or placing them at a greater height. The drawbacks of a UWB system compared to a GPS system are the longer set-up time and cost. [42]

As Wi-Fi, Bluetooth and GPS are already widely used wireless communication technologies, it can take time before UWB could get a foothold on the market. De Luna et al. [43] suggest that building partnerships with other companies can help to achieve success and control for new technology, which was the case for Blu-ray when it competed against HD-DVD for the leading disc storage format. Den Uijl and de Vries [44] conclude that the two main reasons why Blu-ray technology took over its rival HD-DVD was because of the availability of Blu-ray for households in the form of PS3 and exclusive support from Warner Bros. HD-DVD relied on the technology being cheaper and being the first one on the market, but Blu-ray was able to surpass them due to their strategy of allying with other companies and develop a product that meets the allied companies' requirements.

Because of the high-quality and precise localization, introduction of various UWB organizations, and the projected growth of UWB in smartphones, UWB holds great promise for future applications. The next chapter will review the current state of contactless payment: how it works and what additional benefits UWB could bring to payment.

3 Contactless payment

Contactless payment is a payment method available on bank cards and smartphones that enables transactions without the need of physical contact to a machine that accepts payments. These machines are known as point-of-sale (POS) devices. A typical POS device is a payment terminal, where a consumer inserts their bank card and types a personal identification number (PIN) to complete a purchase. Alternatively, if the card and the machine support contactless payment, it is possible to complete the purchase by swiping the card next to the terminal, eliminating the need to type a PIN. Bank cards use NFC technology for contactless payment, whereas smartphones offer a variety of payment options.

The reason UWB is being proposed as a replacement for NFC is due to its security features. NFC lacks inherent security measures and instead it relies on its short distance as a primary security mechanism [45]. UWB on the other hand is secure against many vulnerabilities seen in other wireless technologies, such as relay attacks, making it a promising alternative for contactless payment.

Due to the popularity of smartphones, UWB's potentiality lies in its integration to smartphones. As previously mentioned, Apple, Google and Samsung have started investing in the technology by including UWB chips in their flagship smartphones. If UWB becomes as widely available as NFC, it creates new possibilities such as its use for contactless payment. However, NFC main advantage seems to be its implementation in bank cards, where UWB is not possible to be added due to the need of a power source. In addition, for UWB payment to succeed, paying via a smartphone must be safe and reliable.

This chapter focuses on the procedures of contactless payment systems and their security measures. The first section presents research and recent advancements done in UWB payment. Following this, the most prevalent contactless payment technologies and the mechanisms of mobile payment are introduced. Finally, a security analysis of the various technologies, including UWB, is conducted.

3.1 Research on UWB payment

At the time of writing this, research on UWB as a payment method is almost non-existent. As presented in Table 3.1, Google Scholar only produces 132 results when using the search words "uwb" and "contactless payment". Including “smartphone” as a search word and searching for publications made after 2019 produces only 41 results. 2019 was chosen as the minimum publishment year because that was the year Apple launched the world's first UWB smartphone. From these results, only one research is related to using UWB for payment purposes. Juopperi [46] studies the implementation and accuracy of UWB-based mobile point-of-sale (mPOS) device, where a smartphone or similar handheld device would work as a payment terminal. In LOS scenarios, the accuracy was excellent up to 20 meters, but in NLOS scenarios the accuracy and range degrade. They suggest further research for NLOS situations as those are likely the intended use case for a such payment system. Several sources [9, 17, 18, 31, 32] list payment as one of the potential use cases of UWB, yet they lack details on how the system could work or what advantages its introduction would yield other than the improved security and faster payment.

Even though the research for UWB payment is limited, the technology is already being utilized for paying. NXP highlighted a UWB solution for mobile payment in 2020 that demonstrates how UWB in smartphones could be used for drive-through

Table 3.1: Number of search results for UWB payment in Google Scholar.

Search words	Year range	Number of results
"uwb" AND "payment"	all	3900
"uwb" AND "contactless payment"	all	132
"uwb" AND "contactless payment" AND smartphone	2019-2023	41

payment in vehicles and hands-free payment in stores [47]. In 2022, NXP announced the world's first UWB-based peer-to-peer payment system. It works by pointing a smartphone towards the recipient's smartphone, selecting a payment sum and confirming the payment. There is no need to set the recipient's bank account, name or phone number. UWB streamlines the process by automatically linking the two people together using their smartphones. However, this system is currently restricted to users who are part of ING Bank and own Samsung Galaxy smartphones. It only allows to share money between two people through the ING banking application, not for example purchasing goods using POS device. [48] A prototype of an automatic contactless payment system has been presented by Hannula and Angerpuro [49], who display how a customer could walk past a payment terminal without stopping as UWB authenticates the user, applies loyalty cards and finishes the payment. The process is successful even when the customers have their smartphones inside their pockets.

3.2 Contactless payment technologies

Contactless payment is commonly associated with Near Field Communication (NFC), a wireless communication technology included in the Radio Frequency Identification (RFID) technology. The popularity of NFC is based on its simplicity, as it allows automatic data transfer by touching a reader or another NFC device. To allow this, the range of NFC is about 10 centimeters. NFC is currently being used for contactless identification and payment. For example, NFC enables contactless payment by only needing to place a credit card next to a POS device. [50]

NFC operates at a frequency of 13.56 MHz with transfer rates of 106, 212 and 424 kilobits per second. A device that starts the communication is called an initiator, while the device that responds back is called a target. NFC tags are called passive devices because they use the power supply of other devices, while smartphones and NFC readers are called active devices as they use their own power source. All initiator devices are usually active devices and have their own power supply, while the target devices, like NFC tags, can be either passive or active. [50]

Due to its uncomplicated design, NFC is found in most modern smartphones. In fact, 94% of the smartphones today are equipped with NFC, and the number is estimated to grow to 99% by 2027 [51]. NFC is highly available technology, as it can be added to any type of mobile terminal by adding a dedicated NFC chip inside it [43]. According to CFPB's analysis, most of the POS payments that are made with a smartphone are using NFC technology [52].

NFC equipped smartphones work similarly how typical NFC devices work, meaning it must be held next to a contactless reader. However, in order to use NFC-based mobile payment, a person must own a contactless bank card and an NFC-enabled smartphone. In addition, the user must download a mobile payment application to their phone. [53]

Another option for contactless payment is Quick Response (QR) code scanning, which is not as flexible as NFC. Typically, the payment transaction proceeds by a cashier presenting a QR code that is generated in the POS terminal to a customer who uses a mobile application to scan the code. The process can also happen in vice versa, where the customer presents a QR code generated in the app, which the cashier reads with a scanner. [52, 54] QR code scanning is not as simple as using NFC, as it requires unlocking the phone, opening an app, scanning or generating the

QR code, and confirming the purchase. The scanning also requires a good quality camera and internet connection. [52]

The main benefit of QR code payment is its inexpensive cost. For businesses, QR code payment is cheaper to implement as it requires no additional hardware in contrast to NFC, which requires a POS device. In addition, QR code payment has lower transaction fees as compared to bank card transactions. [54]

3.3 Mobile payment

For UWB payment to thrive, mobile payment must become a prevalent method for making regular payments. It should be dependable, secure and user-friendly. It is more likely for users to adopt a UWB payment system if they are familiar with similar mobile payment applications. This section examines the factors impacting mobile payment usage. It also introduces some of the existing mobile payment services and presents the global adoption of mobile payment.

De Luna et al. [43] report that user's subjective norms have the biggest effect on accepting a mobile device as a payment model. Attitude to a new technology directly affects the intention to use. Mobile payment's ease of use and perceived security have also influence on the intention to use but in lesser impact. The study suggests that companies developing new mobile payment methods should prioritize making a reliable system that satisfies the customers' needs, gather opinions of technology enthusiasts, and market the system to people who could have a high impact on customers' intention to start using said system. In addition, the likelihood of mass adaptation increases if the new payment system surpasses the currently available systems in terms of speed, usefulness and convenience. As security is also one key factor for mobile payment systems, companies should reassure their customers that the new system is as secure or more secure than traditional payment methods like cash or credit cards.

Opinions on mobile payment are positive most of the time. Cocosila and Trabelsi [53] observe that customers see more benefits with NFC smartphones than risks. Promoters of mobile payment should focus on reinforcing the utility value of the payment to consumers to increase mobile payment adoption. However, privacy issues and justification of the service need to be mitigated to increase the success rate of the system. Fiedler [55] says that availability of information about mobile payment and contactless payment is a key factor to increase the customer acceptance of mobile payment.

Mobile payment system popularity may be hindered by smartphone operating system manufacturers, as the payment may need to be completed using the operating system's proprietary payment service. Apple's iOS and Google's Android are the most common operating systems for smartphones. The business models that these two companies make can have an impact on how well UWB mobile payment systems can evolve. For instance, Apple users are unable to use any third-party applications for NFC-based payments; rather, they are required to use Apple's proprietary Apple Pay application. [52]

Apple smartphones come with a prebuilt Apple Wallet app, where users can load their payment cards. Apple Pay can then be used to perform any payments with the loaded cards, such as contactless payments, in-app purchases and online purchases. Users can set one of their cards as a default card that will be used automatically when making a payment. Apple has agreements with over 5100 card issuers. An agreement with Apple is necessary for a particular card issuer's payment card to appear in Apple Pay. Apple charges the issuing bank 0.15% on each credit transaction and 0.005 dollars on each debit transaction made using Apple Pay. Apple also collects the consumer data, such as the payment history. [52] Apple is known for charging companies that use their services, as they require commission for in-app purchases and subscriptions made using apps that were downloaded from App

Store [56].

Google's Android on the other hand has more flexibility, as it can be used by other mobile device manufacturers and different mobile payment services are available to it. Google have their own payment service, Google Pay, which works similarly to Apple Pay. The main difference is that Google does not require a fee for every purchase. Similarly to Apple, Google collects consumer data from their users. Android devices are not restricted to Google Pay, instead, users can use any third-party payment services like those developed by banks. However, there is no guarantee that Google will not change these terms and create restrictions similar to Apple. [52]

Fiedler [55] suggests that the restrictive nature of Apple may even turn into a positive influence on the customers. Apple is a global brand known for their simple-to-use products. Due to this, Apple has a loyal customer base. Knowing that the payment process goes through a system verified by Apple can make mobile payment more appealing to certain people.

Each mobile payment service works without internet access but some of them require being online after a certain number of payments to download necessary token keys, which makes mobile payment more restrictive than regular bank card payment. Apple Pay does not have these kinds of restrictions and it can always be used without internet connection. The same is true for Samsung Pay when using Mastercard because the token keys are generated inside the smartphone. However, when using Visa network, internet access is required after 10 transactions to download new token keys. Google Pay also requires internet access to download new token keys but they do not specify how many transactions can be done before the need to reconnect to the internet. [57]

To ensure the reliability of payment, UWB must work faultlessly inside smartphones, which seems to be the case for at least LOS scenarios. Heinrich et al. [36] conclude that smartphones with UWB chips can measure distance reliably enough on average that it can perform well as a smart lock or as a passive keyless entry system. The devices were able to accurately measure the distance in shorter distances but performed worse in longer distances. They tested three different smartphones, Apple iPhone 12 Pro, Samsung Galaxy S21 Ultra and Google Pixel 6 Pro. The different smartphones shared a common weakness of it being possible for the measurement to fail depending on the position of the antenna. The low power signals could not be properly detected because of the internal components of smartphones blocking them. In real use case this could worsen the user experience, as a smartphone placed in a pocket or a bag would be unable to perform ranging depending on the position and angle of the smartphone. In this kind of case, a successful ranging means the measured distance can increase by several meters because the device relies on reflected signal that travels a longer path. The authors present that longer measurement distances could turn out to be an issue for example in smart homes, where the devices would fail to recognize that the user is present and turn off lights or heating. However, at shorter distances the smartphones were accurate, and the distance measurement worked at every position they tested. Additionally, they found out that the ranging performance significantly varied between different environments, such as in garages, outside in open space and in laboratory environment. Juopperi [46] finds similar results for UWB-based smartphones, where the distance determination is accurate up to 20 meters in LOS situations but performs poorly in comparison to NLOS scenarios.

In Finland, a traditional bank card is still the most used payment method, but the use of mobile payment services has increased. Apple Pay is the most used mobile payment service, however, it is still only used by 5% of 15–79-year-old Finnish people while other similar apps are used by 1%. Contactless payment is a familiar concept to most people, as 93% of the respondents use it at least once a week. [58]

Similar behavior is seen in other European countries, although cash remains the most popular method in various countries. However, the number of transactions made using bank cards has risen, while the number of transactions made using cash has declined. In 2022, cash accounted for 59% of all POS transactions, while card transactions accounted for 34% of all POS transactions. The number for mobile payment was only 3%. [59]

Mobile payment is favored in countries that have launched mobile payment applications. This is noticeable in Denmark, where the influence of Danish MobilePay has grown interest in the use of mobile payment. In 2021, 37% of all payments there were made using smartphones. Interestingly, Apple Pay was used for 42% of all mobile payments, whereas MobilePay made up 22% of all mobile payments. This is primarily because Apple Pay is compatible with NFC technology for making purchases at payment terminals. On the contrary, MobilePay uses separate infrastructure and necessitates an individual store to engage in an agreement for the use of MobilePay. [60] In China, 36% of all POS payments were made using smartphones in 2017. This is due to the popularity of Chinese mobile wallets Alipay and WeChat Pay but also due to the hardship of acquiring bank accounts, meaning cash and mobile payment are the only payment choices for most Chinese consumers. [54]

Bradford et al. [54] argue that even if mobile payment is as easy as paying with a card or cash, consumers may not be willing to switch to another system. One reason why mobile payment has been successful in China is due to the flexibility of AliPay and WeChat Pay, as they offer various other services than just payment. For instance, Japanese consumers have high trust in cash, meaning it may be difficult to turn them into mobile payment users if these applications offer no additional benefits.

3.4 Security

The security challenges associated with contactless transactions have become a growing concern in digital payments. Every payment system service provider and merchant who processes payment cards must comply with Payment Card Industry Data Security Standard (PCI DSS) and other regulations that are enforced to protect private data. Even still, data breaches where credit card information and user identity are stolen occur. [61] This section explores the security considerations surrounding contactless payment by evaluating the previously discussed technologies from a security standpoint and analyzing the security differences between HRP and LRP modes of UWB.

The characteristics of contactless payment introduce various security vulnerabilities associated with bank cards. As contactless payment requires no PIN code or any other form of authentication, bank cards are susceptible of theft. To prevent thieves from using a stolen card, contactless payment purchases are typically limited. Users are mandated to enter a PIN for high-cost transactions and upon reaching a spending limit within a short period of time. Similarly, automatic teller machines (ATM) typically necessitate a PIN for cash withdrawals. Contactless payment poses an increased risk of fraud, such as accidental payments or overcharging when the payment terminal displays an incorrect sum. [62]

Mobile payment is safer than traditional contactless payment due to countless security measures, such as tokenization. When adding bank card information to a mobile payment service like Apple Wallet, a digital account number is created in the form of a token and a token key. The card information is sent to the card issuer's network, which is either Visa or Mastercard. No actual bank card details are stored in a smartphone, as the digital account number is different from bank card's number. During a payment transaction the device gives the token and the token key to the terminal and generates a dynamic cryptogram that is different for each transaction.

The cryptogram is validated in the card issuer's network by using their copy of the token key. When the validation is completed, the card details are de-tokenized and sent to the corresponding bank to finish the payment. However, Google Pay works a bit differently due to it being available on different Android devices. As some devices are not capable of generating the cryptogram, Google Pay uses a unique 24-byte identifier that is assigned to each Google account for the purpose of token verification. [57] Smartphones have many additional security mechanisms, such as fingerprinting, password input and multi-factor authentication. Secure Sockets Layer/Transport Layer Security (SSL/TLS) protocol is used for protecting the data as it transits over the Internet. Smartphones also use Secure Element (SE) for storing sensitive data and for cryptographic processing. [61] Further security measurements include obligation for the phone to being unlocked, and ability to remotely lock a lost or a stolen phone [62].

Because smartphones are used for many other things than just payment, they face multitude of threats compared to traditional POS devices. There are many mobile applications available for smartphones that may contain vulnerabilities or malware. A user must update the operating system and make sure that it has the latest security patches to keep the device safe. Other challenges of mobile payment security include SSL/TLS vulnerabilities, data breaches and fraud detection. [61]

When evaluating the security aspects of NFC, QR codes, and UWB, it is worth noting that despite NFC being approved for contactless payment, the technology itself does not have any built-in security features. As an example, there is no protection against data eavesdropping. This leaves developing a secure solution solely up to the application developers. With proper data encrypting the user data is going to be secure, however, from a user's perspective there is no knowing whether the data is truly secure. Similarly, NFC has no countermeasures against data corruption or modification, jamming, relay attacks and man-in-the-middle attacks. One reason for the lack of any protection is because many such attacks are difficult to perform in practice due to NFC's limited range. Hence, the security of NFC purely lies in the fact that it can only be used in close proximity. When the weaknesses are acknowledged and properly cared for, NFC systems can be used securely. [45] To protect smartphones against NFC-related risks, users are mandated to manually enable NFC functionality on their devices [43].

The primary security concern of QR codes is that humans cannot read and verify the scanned code. A viable attack could be as simple as leaving a harmful QR code to a public place. QR codes can be used to lead to a real looking fake bank website to try to steal user information or run arbitrary commands that install malware or take control of a person's device. An attacker could place a poster with a QR code on a parking lot and claim that the parking fee can be paid using the code. In these situations, it is impossible for a person to know from the code alone whether it is real or not. [63] Dynamically generated QR codes for each transaction are used to tackle this issue, but at the same time they require extra steps for implementation [52, 54]. QR code scanning itself has no security measures as scanning the code just redirects the user into a specific web address. Therefore, authorization and encryption need to be built into the payment system to make QR code scanning secure. [52]

A relay attack is a distance reduction method that works against wireless technologies that rely on RSSI, however, UWB is completely immune to the attack due to its TOF calculation. Relay attacks are executed to gain unauthorized access, and they have become a preferred method for thieves to steal cars that use passive keyless entry systems. Relay attacks require two people. One person stands next to the car door that needs to be unlocked and uses a device that relays signals from the car to the other person. The second thief stands next to an apartment holding a device that transmits the relayed signal inside the house. In the house, the car key then receives the signal and responds back. The response is relayed back to the car which opens the car door. The reason why relay attacks work is because the cars rely on ranging technology that measures the distance based on signal strength, while UWB uses TOF to measure the distance between the two devices. Trying to intercept and send back an illegitimate UWB signal will only delay the signal, which in UWB-based locks makes it clear that the devices are actually far away. [9] Relay attacks have been successfully performed in various wireless ranging systems, such as in those that use Wi-Fi or NFC [10]. Relay attacks have been reported for example in Tesla Model Y that uses an NFC keycard to unlock a car [64]. In the UK, relay attacks accounted for over 90% of all the recorded vehicle thefts in 2019 and 2020 [65].

While UWB is safe from relay attacks, it is not immune to external attacks. The original UWB standard 802.15.4a that was released over a decade ago has vulnerabilities to distance manipulations. An attacker with access to timestamps or other elements of the TOF calculations can alter the proximity calculations. This enables the attacker to decrease the measured distance and trick the system into thinking that they are closer than they are. The IEEE 802.15.4z standard was developed to enhance the security of UWB. It introduces a Scrambled Timestamp Sequence (STS), a cryptographically secured sequence generated using pseudo-random generator, to keep the TOF related data inaccessible by adding random numbers into the packet. [9, 36] Only the UWB initiator and responder have access to the secret key to decrypt the sequence. An adversary cannot guess the STS because it changes every time. [36] 802.15.4z added STS to UWB HRP mode, while LRP improvements include bringing distance bounding and distance commitment features from the IEEE 802.15.4f to make ranging more secure [10].

Although the STS prevents attacks on the logical layer of UWB, it does not provide protection against physical layer attacks. Logical layer attacks involve manipulation of message bits, whereas physical layer attacks focus on altering the signal's arrival time. While STS and distance bounding protocols have shown to be effective against attacks on the logical layer, various attacks have successfully managed to reduce the measured distance when targeting the TOA estimation on the physical layer. These attacks include Early Detect/Late Commit (ED/LC), Cicada, and Ghost Peak. [10, 13]

In these three attacks, the goal of the attacker is to create a fake early peak to influence the TOA calculations despite not knowing the STS [13]. In ED/LC attack, the attacker detects the initial part of a symbol (early detect) and uses it to reproduce the symbol. By detecting a part of a symbol, an attacker can reproduce the symbol by sending the remaining pulses with a small time offset to manipulate the distance measurement. [66] Cicada attack works by transmitting the same polarity pulses at a constant rate to try to cause an early peak [10]. In Ghost Peak, the attacker who is in range of two victims waits for the first UWB packet to arrive, which triggers transmission of a malicious signal. The malicious signal is sent simultaneously as the legitimate signal to the victims to trick the algorithm into computing a wrong distance. [14]

LRP is secure from physical layer attacks, which is explained by the fact that the stronger pulses mean that one bit of information can be represented by a single UWB signal. This mode has larger peak power, meaning it is more likely the receiver will see each individual pulse. Because of this, each pulse can be used to depict one data bit. [12, 13] The pulses are decoded directly to binary, and the receiver checks afterwards whether the binary sequence matches with the expected sequence. An attacker that tries to affect the distance measurement will fail if the pulses do not match with the correct sequence. [11] Consequently, for LRP mode it is enough to have 32, 64 or 128 pulses long secure key, whereas in HRP the length of STS is at least 4096. When a bit is represented by a single pulse, an attacker that tries to affect the distance measurement would have to guess every single one of the pulses correctly. Any malicious or non-malicious interference will result in a failed ranging if the pulses do not match with the expected binary sequence. This means the probability of a successful attack is simple to evaluate, as for 32, 64 and 128-bit long keys the success rate is 2^{-32}, 2^{-64} and 2^{-128} respectively. [12, 13] Using one signal to represent one bit of data grants immunity against ED/LC attacks, however, this representation mode only works in short range LOS scenarios [10].

Because of the higher pulse rate, HRP mode represents bits by multiple UWB pulses, which leaves it vulnerable to physical layer attacks. Longer bits increase the range and robustness to noise and multipath effect, but at the same time they weaken the security. HRP pulses are only a few nanoseconds apart from each other, which means most of the time it is not possible to decode individual pulses. Instead, HRP relies on aggregated pulses. In practice, this means that HRP receiver does not care about individual pulses but the entire pulse sequence. [13] Similarly to LRP, the received signals are turned to binary and compared to the expected signal sequence. However, this mode uses the TOA method displayed in Figure 2.3 that utilizes CIR [11]. An attacker can exploit this method by randomly sending pulses in advance, and if those pulses are similar enough to the expected sequence, it can cause a high peak in CIR estimate. As explained before, a back search will find the earliest peak and accept it as the real time of arrival. Therefore, an attacker can shorten the distance by sending random pulses that can cause a fake early peak. [13] Shortening the back search window will reduce the likeliness of the attack success but also degrades the system performance in NLOS scenarios [10].

HRP mode's security is difficult to truly evaluate because the chip companies utilizing HRP, such as Apple, NXP and Qorvo, use their own proprietary TOA estimation algorithms [13]. The security depends on the configured detection threshold and first path algorithm [11]. Future standards should consider standardization of security algorithms to increase the security of HRP mode.

The security of both modes worsens over extended distances. At distances exceeding 300-400 meters, individual pulses may not always be visible even when utilizing LRP mode due to weakened pulse strength. In these situations, the pulses would need to be aggregated like in HRP, albeit at the cost of reduced security. [13] As LRP can be vulnerable to ED/LC attacks in long distances, UWB systems using LRP must choose between security or performance. Similarly, secure utilization of HRP demands operation within short-range LOS conditions. Increasing the security of HRP may lead to a reduction in ranging performance. However, methods for securely using UWB with long range have been proposed, for example UWB-PR, which uses pulse reordering and cryptographic pulse blinding to prevent physical layer attacks. [10]

Obstructions, the positioning of the UWB devices and other wireless devices can affect the accuracy of the distance measurements negatively, which is why Heinrich et al. [36] suggest that four things should be considered when implementing a secure UWB system:

1. The system should use the IEEE 802.15.4z standard and utilize Double-Sided Two-Way Ranging (DS-TWR) algorithm. In this algorithm, both the sender and receiver devices calculate the distance measurement. If a smartphone sends a signal to open a lock, the receiver should validate the measured distance.

2. At least 10 to 15 ranging cycles should be done before determining the distance. A mean value should be calculated from these calculated distances, which would be used to determine if access should be granted or not.

3. Wrong calculations should be dropped out of the distance determining, for example negative values.

4. Potential attacks should be detected and dealt with appropriately. If the

system detects strong negative values or distances that fluctuate strongly, the measurement should be suspended and the user notified.

In addition to security concerns, UWB devices need to consider privacy risks. The easily accessible UWB tags pose a privacy risk of using them for tracking other people. Google has announced that Android smartphones will start warning its users when detecting an unknown AirTag traveling with the user. Similarly, Apple has addressed the problem by including a warning on their smartphones. [67]

It is important to note that while this section treats the security of the three technologies critically, the security in real applications is more sophisticated and consists of many factors. NFC and QR codes are widely used in payment systems despite the lack of security features. UWB is already being used in secure applications, such as keyless access control systems in modern vehicles. In real applications, the security differences of LRP and HRP modes can turn out to be insignificant, as Apple's and NXP's HRP chips are already used for security purposes in automobile industry [21] and to transfer money between two people [48]. Regarding the known UWB attacks, such as ED/LC and Cicada, FiRa Consortium has addressed that they are difficult to produce in real life situations and are not easily scalable, as they require placing transmitters close to every UWB receiver that is near the location of the attack target [66]. Leu et al. [14] argue that ED/LC attack is impossible in HRP mode due to the high rate of pulses and a single pulse being 2 nanoseconds long. Nevertheless, the planned IEEE 802.15.4ab standard is working on improving the security of UWB by incorporating integrity protection mechanism against distance reduction attacks [68].

4 Research method

As mentioned in Section 3.1, the research for the use of UWB as a payment method is minimal. Many UWB chip makers and experts list contactless payment as one of the use cases for UWB, however, there is no explanation how system of this nature would work, how realistic building such a system is and what limitations and risks it has. This thesis aims to find an explanation to these questions. Noccela thinks UWB could be potentially suitable alternative to NFC as it shares similarities with it as well as protection to many vulnerabilities such as relay attacks. The capability to accurately determine the position of a paying customer inspires novel ideas to enhance the purchase process. In order to obtain answers, a series of expert interviews were conducted with individuals possessing expertise in UWB and payment systems.

4.1 Hypotheses and interview questions

After collecting sufficient source material, hypotheses and questions were developed to be presented to the interviewees. Based on the source material, four hypotheses were formed:

1. UWB technology will become more popular.

2. UWB payment will not replace bank cards.

3. UWB will become the most used mobile payment option.

4. UWB is secure for contactless payment.

The first hypothesis was the easiest one to make since many sources note the rising prevalence of UWB. Most of the largest smartphone manufacturers are offering the technology in their newest products, particularly Apple, which has developed several UWB solutions. Although this hypothesis is not directly related to the subject of this thesis, it is still an important factor to consider. Growth in availability and awareness of UWB will create more interest to develop new applications using the technology, which facilitates the concretization of a payment system.

The second hypothesis is established from vulnerabilities, accessibility, and usability of smartphones. As UWB payment is expected to happen via smartphones, there will be questions regarding privacy and security, which are factors that negatively impact the likelihood of using mobile payment and therefore UWB payment. Not everyone around the world has access to smartphones or internet connection, and even if they do, not all of them know how to use them. Mobile payment is not as straightforward as paying with a bank card, as it involves downloading and using a mobile application. Bank cards are also smaller and require no batteries.

The third hypothesis is that because UWB is more versatile than NFC, it could replace NFC in the mobile payment space. If UWB becomes as available as what NFC is today, there is little to no benefits using NFC over UWB. UWB has the potential to offer the same benefits as NFC while also bringing new features.

The fourth hypothesis is based on the security of NFC and the current use cases of UWB. NFC is not considered secure technology, yet it is still used for contactless payment. UWB is already being used for peer-to-peer mobile transactions and replacing other technologies in keyless entry systems, meaning companies consider the technology secure to use.

The interview questions were structured around the aforementioned hypotheses. The questions were divided into three categories: general questions about UWB, technical questions of UWB, and questions related to building a UWB payment system. See Appendices A and B for a full list of all the questions.

The first section of the interview questions is reserved for general questions about UWB that do not directly concern payments. It consists of comparing UWB to other technologies, reflections on the status of the UWB market, and thoughts of potential use cases. The first two questions also act as warm up questions for the interview, as they freely allow the interviewee to share their general thoughts and insights about UWB.

The second section is reserved for brief discussion about the technical details of UWB. This consists of the differences between HRP and LRP modes with also a question related to their security considerations. This topic was chosen as security is heavily discussed in Chapter 3 and it is a crucial factor on payment systems. Additionally, it would be interesting to find a better conclusion on the HRP and LRP dispute as information related to the topic is minimal outside few studies.

The last part of the interview focuses on UWB payment systems. The questions seek to find answers to technical details, benefits and demand of such a system.

4.2 Interviewees selection

The participants were selected by Noccela, as they have contacts with experts who work on UWB and payment systems. Table 4.1 provides an overview of the interviewees and their expertise. The participants are anonymized and they are referred to as code names. Their workplaces are included with their permission to give a better context of their expertise.

P1 has worked for a long time in various roles at Nets, which is one of the largest payment service providers in Nordic countries that offers various payment solutions for businesses. Currently, P1's role includes introducing new product types to small and medium sized stores while ensuring their commercial functionality. P1 has done

Table 4.1: Summary of the interviewees.

Code name	Company	Expertise
P1	Nets	Payment and UWB Expert
P2	Qorvo	UWB Expert

collaboration with Noccela and are familiar with UWB technology.

P2 oversees marketing in Europe at Qorvo, where they have worked for several years. Qorvo provides semiconductor solutions and is one of the largest UWB chip manufacturers in the world. Previously they were known as Decawave, which Qorvo acquired in 2020. P2 says that they are not as familiar with payment systems and have only been in discussions about payment a few times.

In addition to UWB and payment experts, Noccela suggested interviews with experts from different retail markets in Finland as these companies could be the adopters of a potential UWB payment solution. While it could have brought an additional perspective into the thesis, the reason they were not included was due to the limited time for conducting the research. Furthermore, unlike the other interviewees, they are not UWB experts and therefore do not have suitable knowledge of UWB for the purpose of this thesis. This would have meant creating additional materials for the interviewees to get familiar with the technology, having different sets of interview questions and potentially having a separate section for discussing their interview results. There is also a risk of them not completely understanding the technology, meaning their interviews would not bring much value to the thesis. Lastly, their answers would have likely not answered the research hypotheses.

4.3 Interview structure

Prior to each interview, an introductory email was sent to a participant, outlining the interview topic and asking their interest in participation. After accepting the invitation, a follow-up email containing three pre-interview questions was sent. In addition, the participants were told that this thesis will be publicly available, and their names will be anonymized. The pre-interview questions are:

1. Is it okay that I record the interview? The recording won't be shared or published, instead it's only used for the purpose of writing this thesis so that I don't need to write notes during the interview.

2. Is it okay that I mention your company's name?

3. Is it okay that I mention what you do at the company?

The interviews were carried out in a semi-structured format because most of the questions were open-ended and lacked a definitive answer. All interviews were conducted remotely using Microsoft Teams. At the beginning of each interview, the three pre-interview questions were briefly reiterated before commencing the recording. Both the interviewer and interviewee introduced each other, with the interviewee given an overview of this study's context. Following this, the participants were presented with the interview questions. The participants did not know the questions in advance, however, they were given a summary of the themes of the questions via the introductory email. All the interviewees were asked the same questions, but they were often asked follow-up questions during the interview about the topic at hand. One of the interviewees was asked clarifying questions via email after the interview had ended. The interviews lasted around 60 to 90 minutes.

Following each interview, the video recording was transcribed. After completing all interviews, the process of writing, combining, and categorizing the results began. One of the interviews was given in Finnish and translated to English.

5 Results

This chapter presents the results of the interviews. The grammar of direct quotations has been slightly changed. The results are categorized into two topics: the present and prospective markets for UWB, and the utilization of UWB for payment-related purposes.

5.1 The UWB market

The respondents concur that the current UWB market looks healthy. While acknowledging the absence of commercially viable products in the consumer sector at present, they anticipate a shift towards increased availability and adoption in the future.

5.1.1 Advantages of UWB

As the first question, each participant was asked the most interesting aspect of UWB. Unsurprisingly, both participants shared that accuracy is the key reason to be intrigued by UWB.

The exceptional accuracy of UWB technology introduces innovative business models that were previously unattainable, P1 tells, as UWB enhances the discourse on localization. For example, it is possible to see if a customer picks up a product and puts it back to the shelf, which means it becomes possible to track what products arise the interest of customers but do not produce sales. Bluetooth has already enabled this in a simpler format, as it is possible to see if a customer was in front of a shelf.

P2 includes that the reliability compared to BLE and Wi-Fi is one of the key features of UWB over other technologies. Having your phone in your pocket or in front of you makes almost no difference in UWB, while in BLE the measurement difference is many meters. This means UWB is great technology for access control and payment as the distance from a person to a machine can be known accurately.

P1 suggests there is potential for increased gamification through UWB. For instance, in the context of horse racing, spectators could track real-time distances between horses throughout the race, as opposed to only being able to see the distance from a fixed camera at the finish line. Indoor playgrounds could also benefit from UWB, as it produces fun statistics for children, such as seeing who slid the fastest or who jumped the highest. In general, UWB has many opportunities in sports.

> *"In indoor sports, the team receives information after the game how many meters each player ran. It is also possible to do this with other technologies, such as camera-based, but UWB is a cheaper and simpler solution for example to a junior team."* (P1)

5.1.2 Current market segments

While UWB sounds promising, it is still relatively new technology. When asked why UWB systems are not more common, P1 and P2 both correct that there is a lot of demand for UWB products.

"Qorvo is currently shipping to more than 40 different market segments, such as drones, animals, tracking, AI and safety... it is a long list", P2 says. They continue by stating that there are three applications areas today which have the most demand: car access, the mobile market and industrial market. UWB in mobile phones enhances the user experience, as it can be used to access vehicles and control household devices. For instance, Apple uses nearby interaction to automatically play music when a user gets close to a speaker. Because UWB gives better precision than BLE, many companies in industrial market are moving to UWB for better tracking, which can be used in shops, sports, factories and for collision avoidance to improve safety.

P1 feels that the major market players are those who are simultaneously the owner and user of a UWB product, meaning they control the system and profit from it. This is the case for truck terminals utilizing UWB, where the owner can track the company's performance and therefore benefits by using such a system. A tailored marketing solution for these types of customers is the easiest method to start developing UWB applications, as it does not matter if they are the only user of the solution. The more difficult cases are open environments with multiple factors. In these, there are usually strict standards and one party developing the solution and another one benefiting from it. P1 gives airports as an example of this, where the airport maintains the system while the consumers benefit from it by being able to navigate inside the airport using their smartphones. They add that these systems become more common "in the next wave". The current standards have only made it possible to start developing applications on top of UWB, similarly how Uber was developed on top of GPS.

> *"[UWB] is a new technology that has its own role compared to other technologies such as Bluetooth and RFID that have served up to a certain point."* (P1)

5.1.3 Improving the availability of UWB

Even though there are currently many UWB applications worldwide, there are several reasons why UWB is not nearly as common as its counterparts such as BLE.

While the industrial market has been utilizing UWB for years, consumers currently lack incentives to use UWB technology.

P1 and P2 think the lack of useful consumer applications significantly affects why UWB has not seen success in consumer markets.

> *"The lack of UWB devices is not a cost issue, for example iPhone uses Lidar technology, but a customer does not really use it for anything. Technology comes first and those who figure out how to utilize the technology will follow. UWB chip itself is not a big investment."* (P1)

> *"UWB is more expensive than BLE, but before you put it into your smartphone, even if it is cheap, people need to have a use case."* (P2)

While P2 agrees that the consumer market is currently lacking products, the higher cost of UWB compared to BLE affects the availability of UWB in smartphones and vehicles. P2 lists that Samsung and Google have UWB only on high-end phones and other phone manufacturers have decided not to include it.

> *"Deployment to the smartphones has been slow except Apple who has it everywhere."* (P2)

The reason why UWB is currently only available on high-end devices is due to its higher manufacturing cost. UWB is more expensive than other technologies because of its antenna design, and P2 suspects that some features of UWB may need to be removed in order to include it in cheaper phones.

> *"Angle of arrival is complex especially on the phones because of the number of antennas. It's very complex to put on phones and that also costs a lot of money to produce. On previous iPhones there has been 4-6 antennas to do the angle of arrival. iPhone 13 went to 6 antennas and iPhone 14 back to 2."* (P2)

P2 believes that keyless car access will push UWB into second tier phones, but for that to happen, UWB needs to become more available in vehicles. They explain that the synergistic integration of UWB in both cars and smartphones creates unique possibilities such as seamless car sharing, where you can rent a car without the need to get a physical key but instead use your phone.

> *"UWB is in some expensive cars and slowly replacing the traditional keyless entry by a more secure keyless entry using your phone. BMW, Audi, and Kia already have UWB in some of their cars."* (P2)

Currently, UWB is only available on high-end cars and smartphones, but P2 estimates that in few years UWB will become more available. They believe that the availability of UWB in middle-tier cars would mean that we will see more usage of UWB also, as it simultaneously pushes UWB into middle-tier phones, which then creates more applications. "Or at least this is our expectation", P2 laughs.

5.1.4 Potential consumer markets

Qorvo and Decawave have been trying to find a market for consumers, P2 informs, and one such use case is point and control. It works by pointing your phone into another UWB device, such as to your speaker or air conditioner, and then your phone becomes a controller for said device. P2 describes that this is being standardized but it is not yet deployed or in the FiRa standard.

P2 continues that there are three utilizations for UWB in consumer devices: determining distance, radar and data transfer. They do not go into details about distance determination other than finding objects such as your keys as it is the most obvious use case for UWB.

Interestingly, radar could solve some of the core issues of UWB.

> *"Currently [UWB] can detect you when you have a phone but it is*

> *very limited, if you don't have a UWB phone then [UWB applications] won't work. Radar doesn't need UWB smartphones, it can detect people when they move."* (P2)

Radar differs by not needing tags to work and instead uses anchors to sense the environment. An anchor can sense people moving and perform an action, such as turning on the lights when detecting people moving into a room. It can detect if there are multiple people or a single person closeby. The disadvantage of this is the increased challenge to authenticate people, possibly resulting in the ability to detect nearby people without knowing who they are. Some music companies are currently looking at radar technology as this solution could optimize the music depending on the distance of a person. P2 hints that a product like Dolby Atmos could benefit from this as it needs to know where the user is located at.

P2 portrays the problems with data transfer and why it is not a bigger use case. The low latency of UWB makes the technology compelling for data transfer, which is why some companies are looking at it, however, current regulations limit the efficiency of its usage.

> *"In terms of frequencies there is only one available worldwide which is channel 9 at 8 GHz. If two people are transferring data in a room, small amount is not a problem, but if you're sending music for example, it will not work if you have multiple people."* (P2)

They continue by saying that they have demonstrated playing music but only in lab circumstances. Additionally, UWB could be a potential replacement for Wi-Fi in speakers because of the better latency and better controlling ability.

P2 also points out that both radar and data transferring with UWB have not been standardized, which is one of the main reasons for not having more UWB consumer devices. UWB for data transfer has no real deployment currently mainly due to this.

> *"Today there is no standard for radar, no standard for data transfer. ... [UWB] won't reach worldwide markets without [standards]."* (P2)

Similarly to what P2 told, P1 encapsulates that mobile phones are going to play a large part in getting UWB to consumer markets. There, car access is going to be the most typical use case for UWB. They say UWB is an easy replacement for car companies as it improves the stability and controllability of the key.

> *"Tesla's key works with Bluetooth, you go close to the car and it either opens or not. When UWB arrives in smartphones, it is enough for Tesla to update the software in their application and add a corresponding UWB chip to their car, in which case they can offer more reliable opening mechanism but also a more secure connection that cannot be listened to or hacked."* (P1)

P1 thinks that in addition to UWB smartphones working as car keys, there will be traditional car keys with integrated UWB chips. A classic car key that works by pressing a button to open a car can be swapped to a similar UWB device. "You don't have to wait for [UWB] to come to phones", they add.

> *"Mobile phones will play the main role in bringing UWB to the consumer side."* (P1)

P1 expresses that we will see other UWB consumer devices in addition to UWB-enabled smartphones.

> *"UWB will inevitably come to other consumer devices as well, for example the latest Chromebooks already have a UWB chip inside, but that does not mean that there are consumer applications for it yet."* (P1)

They specify that by having UWB in both smartphone and laptop, the laptop will open once you come close to it. It would not require typing out passwords because you have authenticated yourself already in the phone and UWB recognizes it is you that is in front of the laptop.

P1 states that consumer devices can include UWB way before the consumers even truly understand what UWB is.

> *"For example, Husqvarna robotic lawnmower searches for its own charging station in the yard using GPS, and it also has a Bluetooth transmitter in the station that refines [the station's] location from the mower's point of view."* (P1)

They reason that UWB is better technology in this context, as it improves the situational awareness of the mower and provides a more accurate position of the charging station to the mower. However, P1 reminds it may not make a difference to a consumer which technology is being used because from a user's point of view they all work the same.

> *"UWB may become available to consumers through various devices very soon, depending on the device manufacturer's challenges, e.g. the positioning of a robotic mower."* (P1)

5.1.5 Replacing narrowband technologies with UWB

Given the numerous advantages of UWB compared to narrowband technologies, the interviewees were asked whether UWB could potentially replace some of the existing technologies, which would help with the growth of UWB. Although UWB appears to be a suitable replacement for Bluetooth, it will likely not completely replace it or the other technologies as they have different use cases.

> *"It very much depends on the application field. In some application fields [the technology] can be completely replaced, in some [the technologies] can complement each other."* (P1)

P1 gives as an example an RFID label that works passively and is cheap to manufacture, meaning UWB would likely work together with it rather than replace it. They remind it is the same question as whether 5G will displace some other technologies. P1 continues that it is rare for technologies to get replaced and instead they work alongside each other until at some point it is noted that the other one is better and there is no need to use the inferior one. For instance, for some technologies it is common to release a new standard and slowly replace the older devices which used previous standards. This was the case for serial cable and USB cable, where both were used for some time until eventually devices stopped supporting serial cable because nobody used it anymore.

> *"[Replacing another technology] happens by application field instead of directly deciding not to use a certain technology, especially since it does not generate huge costs to keep different technologies side by side."* (P1)

P2 agrees that the other technologies, like NFC, still have their uses. In their opinion, UWB could be seen as an additional functionality to NFC.

> *"When talking about the current access control and payment, NFC will remain due to the reason that it uses no power source. For access control this is mandatory."* (P2)

When asked if UWB would replace the other technologies in the context of indoor RTLS, P1 thinks UWB is more likely to replace BLE there, while P2 still sees use cases for BLE.

P2 rationalizes that BLE is still a viable option depending on the use case:

> *"In indoor positioning, most of the time you don't need to know with five centimeter accuracy where you are but with 100 percent accuracy in*

which room you are. So, if you know the person is in this meeting room in this big warehouse the job is done. Battery-based BLE does the job." (P2)

However, P2 agrees that even in these situations UWB is occasionally better depending on the environment, as in hotels and hospitals there are many small rooms close to each other. With BLE, it is more difficult to know which room you are in.

Other than reliability and accuracy, there is no clear winner when comparing BLE with UWB. P2 lists that BLE is cheaper in general, and in addition the anchors are cheaper, easier to install and require no cables. P1 in turn names lower overall maintenance cost, lower number of anchors needed, better accuracy and energy efficiency being the benefits in UWB over BLE. P1 mentions that the differences between the two technologies make it easy to move to another technology especially in industry.

> *"In industry, UWB can very quickly replace other indoor position systems because they are easy to compare. ... A factory that has been using Bluetooth is easier to switch to UWB because it is clearer what you want to achieve and see that this system offers it better."* (P1)

> *"When people need accuracy there is no competition. UWB, end of discussion."* (P2)

P1 also reminds that while Bluetooth is used for indoor positioning in industry, it is not being used for positioning in consumer side like UWB is, but instead for other purposes like sound transmission.

> *"Bluetooth and Wi-Fi are very limited in indoor positioning."* (P1)

When asked about Wi-Fi positioning, P2 sees no reason to use it. P2 says that Wi-Fi consumes more than BLE and UWB, requires cables and has low precision. They say that the same points apply to 5G positioning as well.

> *"[Wi-Fi] is mostly used in access point, but there are companies that offers it for location but I honestly don't see it as a big competitor."* (P2)

In response to the question whether the participants believe that in the future consumers will be more familiar with the UWB technology similarly how people currently know what GPS is, P2 thinks it will happen due to the advertisement of UWB, while P1 has a contrasting viewpoint.

> *"Certainly yes. Apple is advertising around UWB with a list of features, so I believe in car access they will tell you that the car can be opened with UWB, so you need a UWB phone."* (P2)

> *"Radio technologies are not as concrete as satellites orbiting the sky, whether you have 5G or UWB it gets buried away in [applications], instead of becoming something that someone asks or demands if this has UWB. The trend is that these things happen unnoticeable in the background without the need to know how they work."* (P1)

5.2 Paying with UWB

The interviewees reveal there is currently a few significant problems hindering the development of a global UWB payment solution, however, when tailored to a smaller scope, building a UWB payment system is realizable. Based on the findings, UWB has potential to provide diverse payment methods while benefiting businesses.

5.2.1 The main problems

Both P1 and P2 agree that the lack of standards is the reason for the lack of UWB payment systems.

P1 explains that making UWB payment a worldwide solution requires updating the whole infrastructure at once. They continue that it is the same reason why it took long before contactless payment became available on payment terminals. Banks slowly released cards with contactless payment, but the technology only truly became available once Visa and Mastercard managed to create regulations that payment terminals must have support and compatibility to contactless payment. This resulted in NFC becoming available worldwide.

Payment terminals will not support UWB anytime soon because it is a global issue. P1 explains:

> *"What NFC standardized was that terminals must be able to recognize NFC, i.e. if you are a payment terminal accepted by Visa, you must support these features. It is difficult for an individual actor to add a feature there and expect it to be supported everywhere globally."* (P1)

This is also the reason why Nets currently do not have a UWB supported payment terminal. Likewise, P2 believes that the wide adoption of UWB payment will not occur until it is standardized.

> *"If you do [UWB payment] for open market, it's a bit too early. You need standardization for the open market, but you can still start doing it in smaller companies."* (P2)

P2 mentions that UWB payment brings different issues depending on the use case.

> *"We have to distinguish between different ways of paying, there's contactless payment that you do in point-of-sale when you're in shops, there's automatic payment when you are leaving the shop, so when you cross the door you pay automatically."* (P2)

They detail the problems of an automatic payment system in public transportation, as the system must know the intention of the user with certainty. In metros, there are several gates close to each other which people pass constantly. P2 explains that this kind of system must be able to work reliably, meaning it knows that a person crosses a specific gate and has the intention to do it. It must also work even on edge cases where the person decides to not cross the gate but switches to another gate.

> *"This is super complex and I have discussed it with several people already and this is extremely complex to solve. It also requires proper security. There are multiple parties involved, the people who make the gates, people who make the security. Today, there is no global discussion [of UWB payment]."* (P2)

Still, P2 believes there is a demand for UWB payment even though it has its difficulties.

> *"It's an application that we have been pushing for a while to a start-up company, so yes, there's still case for UWB payment. Some people were saying this is an NFC long distance, because you do the same stuff, and you know pretty well at which distance is the person. There are companies trying to solve this but slowly, I suppose they don't have the pressure to solve the problem."* (P2)

P1 explains that Bluetooth payment has been considered in the past and it poses similar issues that UWB payment now has. Like P1 mentioned earlier, adding a new technology to payment terminals is a difficult process.

> *"Bluetooth modules were considered for payment terminals at some point and the aim was to make the smartphone pair with the payment terminal using Bluetooth and that the payment information can be transmitted through it. At the time, it was that the terminals that read cards*

> *went through strict certification processes and they may not have the most dynamic operators that add new features, but instead safety and compliance are put first."* (P1)

However, P1 says that technologies do not necessarily need to be integrated into the payment terminals but can work independently. When Bluetooth paying was tested, it had a separate device that was connected to the checkout point. Users then would proceed to pay using a mobile application. Nevertheless, the technology was swiftly seen as insufficient.

> *"It was tested, and it ran into the problem that when there were a lot of people in line who had opened the mobile application ready to pay, the device didn't know how to take the right person and the payment amount might be shown to a different person than who was paying."* (P1)

Surprisingly, the issues of Bluetooth payment did not seem to concern the consumers as much as it did the retail markets that had the system.

> *"The customers liked it and thought this was a good idea, but it didn't work so well in use. It's important for the store that the payment goes smoothly and reliably and you don't have to go to help [the customer]."* (P1)

5.2.2 Building a UWB payment system

How can we begin the development of UWB payment? P1 explains that similarly to how Bluetooth payment worked, UWB payment does not require a compatible payment terminal, but instead can be used as a separate device next to the terminal which communicates with the customers' smartphones:

> *"For example, Kesko (Finnish retail company) could add a UWB sensor to their self-checkouts, and since they control the payment side partly with their own K-Ruoka mobile application, they could add an option to pay with the application and a person would add their own payment card information there."* (P1)

On the use of market-based payment applications, P1 thinks it would speed up the launch of UWB payment:

> *"This would solve the problem that someone has to launch a UWB payment method and another would have to set up a receiver."* (P1)

When asked if all retails markets should utilize their own smartphone applications for payment, P1 says:

> *"That would be the easiest way. Apple could open the UWB sensor as part of Apple Wallet and then you can add cards and payment would go natively at the operating system level. A faster way, however, are these applications, which also get customers to use these applications and activate benefits there before going to the cashier, so in that sense payment method could be added there."* (P1)

P2 also thinks that UWB payment will happen mostly with smartphones:

> *"For me, the trend is to do everything with smartphones. Every year you do more with your smartphone, now you can even open your car with it."* (P2)

They continue that payment could also be possible with another device that would work like a regular tag, but the deployment would be small, so they see no benefit using another device over a smartphone.

P1 lists three criteria that must be met when considering a new payment system:

1. The system should be faster or as fast as current payment methods.

2. The system should be easy and seamless for the user.

3. The system should not cost more than current payment methods or at least not cost significantly more compared to the benefit of said system.

P1 thinks that UWB meets all three requirements:

> *"[UWB payment] does not require reinventing the infrastructure, instead you can install a [UWB receiver] in certain places, which brings seamless security and identification of who is at the cash register. ... Kesko could offer UWB payment, and many of these criteria are already met because they have their smartphone app. It would work so that in practice you just go near the self-checkout point and a [message] will come to your phone asking if you want to pay."* (P1)

P1 presents four different scenarios how UWB could be used to transfer money:

1. Closed loop –payment: The consumer loads money into a service provider's digital wallet (such as a mobile application) in advance in the form of virtual currency, and pays using the virtual currency. Since the money has been transacted in advance, the virtual money will be directly reduced from the consumer's account when they buy something without the need for banks to be involved.

2. Custom solution: A company, such as a retail market, utilizes their own mobile application that has integrated payment solution. The consumers can store their bank card information in the application and pay with real money using said card. When the card is charged, the money is transferred via a traditional online payment transaction.

3. Open solution: Both the company that provides services and their customers utilize external application to transfer money. Similarly to custom solution, the bank card information of a consumer is stored in the application in advance and charged during purchase. Examples of these include Apple Pay and Alipay.

4. Point-to-pay: A consumer points their UWB device towards another UWB device and receives the other device's bank account number, phone number or other information needed for payment. The consumer then proceeds to pay using a mobile application and it is processed as an online purchase. The currently available UWB payment solution made in collaboration by NXP, Samsung and ING Bank works with point-to-pay –principle [48].

It is important to note that in all four scenarios, UWB is only used to authenticate the buyer and not used to transfer money. In the first three scenarios, the seller's UWB device detects the buyer using UWB and sends a payment request to the buyer's device. The buyer then confirms the purchase, and money is reduced from their account. In closed loop –payment, the buyer's virtual currency is reduced, which means no actual bank transaction occurs. In custom and open solutions, the buyer's bank card that they have linked to the application will be charged, and the transaction is processed as an online payment via bank card. Upon successful transaction, the buyer's device sends a confirmation back to the seller with UWB to inform that the buyer has completed the purchase.

> *"In practice, UWB takes care of the identification of the buyer and monetary transactions happen by other means. ... For the consumer, paying with UWB would mean that they receive [a payment request] in the app."* (P1)

5.2.3 Addressing presumptions

Several potential challenges arose in the source materials and in the interviews that affect how a UWB payment system would work. These involve the compatibility of UWB in cheaper phones, the interest to use UWB payment and mobile payment in general, the practicability of implementing an automatic payment system, and the security concerns of UWB. These challenges are classified into three topics: utility-related concerns, the feasibility of automatic payment, and security concerns.

Utility-related concerns

As P2 previously stated, integrating UWB into cheaper phones would likely mean that it includes less antennas, however, P2 convinces that the number of antennas will not be an issue for payment.

> *"You don't need several antennas for payment, only one for measuring the distance. Maybe the point-of-sale needs to know where you are but in that case the point-of-sale has a dual antenna, not your phone. [The phone] just need one antenna like in a tag."* (P2)

On whether people would be interested in paying using UWB, P1 states that the problem has nothing to do with UWB itself.

> *"People don't decide whether to use UWB or NFC, they decide whether to use Apple Pay, etc. People don't necessarily care about the technology itself, but about which technology offers the best user experience. Such technology is chosen for the application and people use it and notice that this is convenient. You don't open an application like K-Ruoka and choose whether you want to pay via Bluetooth, NFC or UWB, but instead you start the application and the developers of the application have come up with a certain technology that must be used in order to make the*

> *payment and the user either likes it or not. When UWB becomes more prominent and people use it and like it, there may eventually become a situation where no other options are even offered."* (P1)

When asking the same question from P2, they wonder, "Isn't it a question of generation? Like bank notes, check, cash and credit card." P2 reminds that cash is not an option in many places in Sweden, and in France there is a limit of 50 euros for contactless payment with credit card. Mobile payment does not have such a limit, which is one reason P2 always pays with a phone, other reasons it being faster and easier as you always know where your phone is. When asked if they think that eventually everyone will pay with a smartphone, P2 says yes.

Feasibility of automatic payment

As seen in a video, Hannula and Angerpuro [49] demonstrate how UWB could be used to automatically pay as you walk past a counter. When asked whether this kind of payment is realistically possible, the interviewees believe so, but do not think it is practical for a customer.

> *"It is possible, but if an account that has been saved is charged, then the systems usually want confirmation from the consumer so that it does not happen that the consumer is charged an amount that he does not want to pay. The phone can offer different ways to verify the payment, such as Face Id, fingerprint recognition or a PIN code with which the payment is verified or, in the simplest, a button to accept."* (P1)

Previously, P2 explained the issues associated with an automatic payment system in a metro station, emphasizing the difficulty in discerning the intention to buy, which proves to be exceedingly challenging in such a system.

> *"If you leave your phone in your pocket, with NFC you need to take it out, which shows that you have the intention to pay. With UWB in your pocket, you cross the cashier, we don't know if you have the intention to pay or not, there is no physical gesture which shows that you want to pay. Or that you have seen it and acknowledged it. It's very complex, and in some countries there is a rule that we have to make sure that you have the intention to do an action."* (P2)

P1 thinks that this system fits better for authentication than for payment.

> *"When paying, you want a receipt, while when authenticating, you can just walk up to the door and it will open without needing any access tags or cards."* (P1)

There are still scenarios where the use of an automatic payment is justified, like in public transportation. P1 imagines people could walk into a bus and walk out without needing to pay in advance or show a ticket. UWB would recognize when a person arrives on the bus and leaves it, and the system charges the person based on the distance traveled. Using such a system should not be difficult in theory, as the payment happens in the background to compatible devices. The consumers do not need to know anything about the technology but only be aware that this kind of payment option is available.

P1 reminds that in the above scenario the bus transportation operators would offer multiple payment options, which brings its own challenges. These service providers already offer a wide variety of choices such as paying with cash, bus card, QR code, invoice, and mobile application. Having multiple systems simultaneously causes maintenance issues and considerations whether each system is necessary.

In any case, this system would require NFC or the user to be close to the UWB transmitter to confirm the user's intention to pay. NFC would need the user to make a gesture to confirm the purchase, but it is also necessary if a phone runs out of battery. P1 says that HSL (public transportation in Helsinki) already has protocols on what to do in scenarios where a customer is unable to display their ticket on a mobile device. However, P2 states that "you do not need NFC for UWB payment to work, but you still have NFC with UWB on top", likely referring to the fact that nearly all smartphones include NFC nowadays.

Security concerns

Several previous studies state that while LRP has provable security, HRP mode of UWB is not secure. Neither P1 nor P2 were familiar enough with the two modes to answer the question regarding their security. Nevertheless, they both were willing to share their opinion on why HRP mode is prevalent today compared to LRP.

> *"Could it be related to the fact that the radio modules have to be certified and must stay within certain limits, which for example the FCC has determined, so that it is easier for HRP to achieve these? Or could it be that HRP has been found to have a sufficiently good performance? It may be that there is a limit to where [LRP UWB] can be installed, for example if it produces too strong signals and interferes with another device."* (P1)

Questioning P2 on why Qorvo uses HRP, they put it bluntly, "Because FiRa chose HRP and use it in their standard".

Both interviewees were unable to state whether UWB is currently secure enough for payment but agreed that it is still more secure technology than the currently used ones.

> *"NFC is good because it is not possible to create a fake payment card, but it is possible to read unencrypted data from it. However, abuse is difficult because you need an account to store the payments and through that*

> *the abuser can be tracked, meaning there is no anonymous abuse. But [NFC] is by no means in line with the best current cybersecurity practices that UWB could be. ... NFC can be remotely read and interfered, not much damage has been done in practice but it ultimately isn't a sustainable solution. There are also problems with its reading distance."* (P1)

5.2.4 How UWB changes payment

UWB could speed up the payment process, as it is possible for the system to know what each customer is doing. P2 thinks swiftness is one of the benefits of such a system.

> *"It's quicker. The goal is to be quicker. You can get pre-authorization when you're close to the cashier, for example you can do the pre-authorization and check you have enough money on the bank account."* (P2)

On a similar note, P1 thinks the system offers much more flexibility for the customer and more control for the store.

> *"For example, many self-checkout points now have a gate where you have to show the receipt that you have paid. But with UWB, the system knows all the time that this person has been queuing at the checkout for a couple of minutes, went to the checkout point number 1, completed the purchase in 12 seconds and walked away from the gate, meaning Kesko's system would have a complete picture the whole time. The consumer can benefit from a couple of small things here, i.e. not having to pay right here or not having to show a receipt here."* (P1)

Depending on the setup, the range of UWB payment can vary significantly. Instead of having a few separate UWB transmitters, stores can have a full UWB network with anchors around the building. When all compatible UWB devices are known and their locations are known, payment becomes possible in any distance visible to the system. As an example, P1 says that if the system knows what areas belong to each checkout point, the system just needs to verify which consumers are within the boundaries of an area and then send a payment confirmation to those. P1 states that it is a matter of parameters, which can be easily adjusted with UWB, for example, depending on how close or far away checkout points are from each other. In certain cases like self-checkouts, it makes sense to keep the distance small and require the user to be next to the machine.

Building a UWB infrastructure in a store enables versatile use of the system. P1 outlines advantages such as automatically deactivating security tags on purchased items and collecting user positioning data as valuable features for a store that implements a UWB payment system.

> *"The benefit of UWB payment is that it is a more secure solution than NFC and Bluetooth, but the added value could be the additional data that can be obtained from outside the payment. ... This additional data can be one of the main reasons why a store would like to roll out UWB payment and be interested in offering it in its mobile application."* (P1)

P1 compares UWB payment to online payment, where a website knows every step that a user takes before completing purchase.

> *"For example, an online store knows exactly what I clicked on before paying, so UWB basically brings the same but to a physical environment."* (P1)

P1 believes UWB could create new methods to pay in the future.

> *"UWB could bring a new kind of payment to some extent in the form of a remote control, meaning you point to the object where you want to*

> *pay. In the future, it could be possible that you point your smartphone at a soda machine and choose a coke [from your smartphone], but this will take time and requires different standards compared to a store's own mobile application."* (P1)

Although the absence of standards slows down the adoption of UWB payment, P1 stresses that the launch of UWB payment system is contingent on the individual stores, as they already support non-standard payment methods such as AliPay that uses QR code payment. In that sense, UWB payment has a promising future, given that UWB is already standardized, supported on mobile devices, and only requires UWB anchors and a network for store integration.

> *"UWB meets the criteria for a successful payment system. ... UWB payment is something that one operator cannot solve by an innovation, so the easiest solution is to start with customer-specific solutions."* (P1)

6 Discussion

In this chapter, the interview results will be discussed to explore the details of UWB payment systems. Initially, a brief overview of UWB's expected future is provided, followed by an in-depth analysis of UWB payment. The analysis will look at the role of UWB in payment, explaining the advantages and challenges of UWB payment solutions in comparison to existing systems, while also proposing different methodologies to implement the system. Furthermore, the security concerns of UWB payment will be addressed. Lastly, this chapter will also acknowledge the study's limitations and suggest potential areas for future research in UWB technology in the context of payment.

6.1 Future implications of UWB

The interviewees unanimously agreed that smartphones have an important role in ensuring UWB's global success. This is not surprising considering the predictions on growth of UWB-enabled smartphones as more big tech companies are interested in the technology. As P2 mentions, we carry phones everywhere, making it only natural to include the technology there instead of having to carry a separate device. However, the interviewees estimated that we could see the technology integrated in other appliances, such as in car keys, laptops and speakers.

While the participants eagerly shared their ideas on potential applications of UWB technology, their concepts primarily centered around position measurement.

It is evident that the primary focus of UWB lies in its accuracy, security and real-time position statistics. This explains why UWB has seen success in the business sector, while facing challenges in finding practical use cases for consumers. Businesses can benefit from precise position data, whereas consumers may not find it as useful, especially considering the limited ownership of UWB devices. Apple AirTag is an example of a successful commercial UWB product, but it is difficult to see a competitive device for it. This is due to the flexibility of AirTags, as the tag can be affixed to any item, which allows localization of non-UWB devices. As estimated by the interviewees, a more plausible scenario involves companies incorporating UWB technology into a range of existing devices, such as laptops and speakers, where the UWB connection is not mandatory for using said device. This way the product's sales are not as heavily dependent on the number of individuals possessing a UWB-compatible smartphone.

The higher cost and lack of consumer applications directly relates to absence of commercial UWB products. The UWB antenna design for smartphones is a costly operation, which explains the presence of UWB being constrained to higher value products. Once there is more demand for UWB smartphones, there will be efforts to put it in cheaper phones. The interviewees agreed the secure car access with UWB is one of the cases which will create more demand for UWB smartphones. It remains to be seen whether the same is true for UWB payment.

Although the participants did not admit UWB replacing other similar technologies, they recognized that it would bring enhancements compared to existing technologies. The spread of UWB will create new products and produce more meaningful and accurate data. In certain application fields, where the benefits of technologies can be easily compared, such as indoor RTLS systems and car access, UWB has the possibility to slowly settle as a replacement. Even still, the seemingly inferior technologies have their uses. For instance, BLE is still a viable technology for RTLS depending on the expected outcome, offering less accuracy for cheaper cost. It is likely the technologies will work together, utilizing the best parts of each technology to result in the best outcome.

P2 hints that in the future we could see more of UWB being used for radar purposes. One of the original uses of UWB included it being used for radar in military applications, however, commercial applications have not yet seen much use of UWB radar. This can be partly attributed to the lack of standards, which limit the utilization of UWB radar applications. Radar would allow the use of UWB without the need for tags but with the downside being that it is more difficult to authenticate and differentiate people from it. An aspect that remained unexplored during the interviews was how UWB differs from the existing radar systems. Cheraghinia et al. [69] review studies related to UWB's use in radar and list several benefits of UWB over other radar technologies such as millimeter wave (mmWave). The large bandwidth of UWB, its relatively low frequency range of 3.1-10.6 GHz compared to mmWave's range of 30-300 GHz, and its pulse-based modulation makes the technology most suitable for distinguishing small objects, while being able to penetrate through objects and provide long range. They conclude that UWB radar has four major applications: presence detection, device-free localization, activity recognition, and vital sign monitoring. For example, UWB radar has seen positive results in hand gesture recognition, being able to differentiate 14 gestures with over 90% accuracy [70].

6.2 UWB payment

The interviewees pointed out that global UWB payment will not happen any time soon due to the lack of standards. Payment terminals must comply with several standards and supporting UWB is a long process that may never happen. However, P1 says that this is not mandatory, and UWB payment can be added to any business similarly to how many non-standardized payment methods are already available in stores.

6.2.1 System description

Similarly to NFC- and QR code-based payment systems, a UWB payment solution would take advantage of smartphones due to the utility of mobile applications. The participants agreed that using smartphones for payment is more practical than developing a dedicated payment device. Additionally, this means that the projected growth of smartphones with UWB technology would expand the accessibility to UWB payment without the need for separate devices.

The easiest way to start developing this new system is by integrating UWB payment into existing mobile applications. For example, many retail markets already have a mobile application, which can be used either for paying or getting various bonuses when visiting the store. These so-called supermarket apps are a popular payment method in Denmark, where you can use an app to pay for a specific supermarket [60]. Instead of waiting for global standards or products, the fastest way to get UWB payment to use is by providing tailored solutions for stores and utilizing their already existing mobile applications.

It is noteworthy that based on the description of UWB payment, UWB is merely used for authenticating and locating instead of being directly involved in the payment process itself. Authentication using UWB occurs through communication between UWB anchors near the payment terminal and the user's UWB-enabled smartphone, while the payment process is an online purchase conducted via a smartphone. After successful authentication, the system sends a payment request to the identified customer to accept the purchase. Essentially, UWB changes the user interaction steps while maintaining the underlying payment mechanisms the same.

Interestingly, a similar concept was tested with Bluetooth, which resulted in the

Figure 6.1: How UWB payment could work in retail markets.
Image generated with Icograms Designer [71].

wrong people receiving the payment prompt as the system was unable to accurately identify the person currently paying. Still, the users who tested the system liked the idea, which brings hope for success of a similar UWB system.

A concept of UWB payment system in supermarkets is visualized in Figure 6.1. At the store's checkout counter, a UWB transmitter is positioned alongside a conventional POS device. Optionally, the store may deploy UWB anchors around the shop, enabling customer authentication upon their arrival at the store, provided they possess compatible smartphones. The UWB transmitter located next to the POS device can be used to identify the customer currently paying by measuring which customer is located closest to the transmitter. Upon successful authentication, the system sends a payment request to the identified customer's phone. The customer can then either complete the payment through the mobile application or normally by using a bank card at the POS device.

6.2.2 Benefits

UWB seems to be well suited for payment, bringing several benefits for consumers and businesses. P1 explains three criteria that must be met when designing a new payment method: it should be fast, easy to use, and cost the same as current methods. All these criteria are met with UWB payment.

1. Faster payment: UWB enables payment from outside of the payment terminal, meaning there is no need to stand next to the payment terminal. Depending on the number of anchors, payment could be possible from anywhere that is in hearing range of the anchors. However, for better accuracy and user experience, it probably is best to keep it close to the payment terminal. Other ways in which UWB could expedite the payment process include pre-authorization, automatic application of bonus cards during payment, and eliminating the need to show receipts at self-checkout gates. Lastly, UWB data rate is faster than NFC, which will increase the speed of communication between devices.

2. Ease of use: In theory, the system should be easy to use, as the user would automatically receive the payment request and only need to accept it. The acceptance could happen by myriad of choices, such as pressing a button, typing a PIN code or with a fingerprint. Because of authentication and payment validation, UWB payment system should not need to have a limit on how large sum you can pay at once, which is currently the case for NFC-based contactless cards.

3. Low cost of implementation: While UWB payment requires some work before being fully operable, it should not be expensive. At minimum, UWB anchors must only be installed on checkout points. As most markets already have mobile applications, a software update is only needed for the application to work together with UWB.

Unlike other payment methods, UWB could benefit businesses from the additional data that it produces. As UWB can accurately determine the position of consumers, businesses can collect various data, such as the average duration of queuing and paying. Building a UWB infrastructure around the store can provide further data, such as a map of routes that consumers take and information of areas and shelves where customers spend the most time.

Lastly, UWB payment is versatile as it can provide consumers with a variety of novel payment methods. These different methods are detailed in Section 6.2.4.

6.2.3 Challenges

The overall challenges present in UWB also impact UWB payment systems, as the absence of standards and the limited availability of UWB-enabled smartphones have a detrimental effect on UWB payment adoption. These factors are the primary reasons for the lack of global interest in developing UWB payment solutions.

Despite the prospects of UWB payment, NFC payment may still be preferrable in certain scenarios. When considering the ease of contactless payment using bank cards and smartphones, bank cards only need to be held near a payment terminal, whereas mobile payment may involve added steps. Therefore, it can be assumed that UWB-based mobile payment would lose in speed to NFC-based contactless cards. This depends on what the user must do to complete a purchase: unlocking the phone, opening an app and inputting a PIN is slow, but pressing an OK button on the homescreen would make the payment quick. Additionally, the proposed system would require an internet connection because the payment itself is processed as an online purchase. This can be problematic especially when traveling abroad, where internet connection can be expensive or unavailable. The requirement for a power source and internet connection makes it unlikely for the system to replace traditional bank cards. For mobile payment, the benefits of UWB could make the technology more desirable to use than NFC. P1 pointed out this also depends on whether companies decide to support multiple or only one specific payment method on mobile applications.

The implementation of UWB payment systems for outdoor settings may pose challenges due to regulatory constraints. Internationally, the deployment of outdoor UWB systems consisting of fixed anchors is either restricted or prohibited. This limits the potential utilization of UWB payment solutions, for instance to amusement parks, gas stations and drive-throughs. To address this limitation, some outdoor applications could benefit from peer-to-peer payments utilizing two smartphones for communicating and transferring money, thereby circumventing the need for fixed UWB devices.

Lastly, the mechanisms of the system may pose difficulties in recognizing the customer's intent to make a payment and identifying who is currently paying. While these issues are not present in the illustrated scenario depicted in Figure 6.1, the former issue is challenging in a hands-free automated payment setup, while the latter issue can arise in situations where multiple individuals are close to the UWB transmitter. These matters are further discussed in the next section.

6.2.4 Payment methods

P1 and P2 held contrasting perspectives regarding how UWB payment would function. P1 thought UWB payment would be request-based, where the user receives a payment request on their smartphone. P2 used the term "NFC long distance" for UWB payment, suggesting the potential use of UWB technology in a manner similar to NFC.

P1 believed that implementing a request-based approach would be the most straightforward method for developing a UWB payment solution. Since the customer must acknowledge the payment by accepting the request, it eliminates the issue of recognizing user intentions. However, similar to challenges encountered in Bluetooth payment systems, there remains an issue in identifying which customer should receive the payment request. One way to solve this problem is by selecting whoever is the closest to the UWB sensor, although this approach would decrease the range of UWB payment. This would be the most logical solution in self-checkouts. P1 also suggested an approach where the customers must stand in specific areas in order to receive payment requests. Alternatively, the system could incorporate an algorithm to accurately pick the intended recipient, or a simpler method could involve the cashier selecting the recipient for the payment request.

As UWB enables accurate distance measurement, it should be possible to configure UWB to only accept payments when the distance between the smartphone and the POS device is within a few centimeters. Using this method for payment would solve recognizing the correct person and the intention of purchase. Despite the system's functional similarity to NFC, it is important to note that these two technologies are still distinct. While NFC is restricted to short distances, UWB's range is adjustable. However, unlike NFC, UWB devices require a power source. Additionally, these two systems have different security aspects. While NFC is susceptible to relay attacks, UWB is immune to such threats. Nevertheless, the characteristics of this kind of UWB payment system could render it vulnerable to distance reducing attacks, as demonstrated in HRP-based UWB systems, although executing such attacks in real-world scenarios is complex.

During the interviews, the concept of using UWB for point-to-pay transactions was discussed. The existing UWB point-to-pay solution currently allows sending money to a friend under specific conditions, such as both parties being in the same bank and owning compatible devices. P1 proposed the idea of applying this method to buying from a soda machine, where users would get controls to make purchases from their smartphones by pointing the phone towards the machine. Similarly to

NFC-like payment, this approach solves the two aforementioned issues. There is obviously a risk of accidentally pointing a smartphone towards a machine, but if the payment does not happen automatically but by acceptance, it would mitigate the risk of incidental purchases.

On the use of UWB for hands-free automatic payment, the interviewees agreed that it is achievable but did not recommend it due to the system's uncertainty. It becomes difficult to acknowledge the customer's intentions if it becomes possible to pay by walking past a cashier. Unintended payment would be harmful for both the company and the consumer, meaning there should be a method to confirm the intention, such as with a hand gesture or a button press. Therefore, this concept suits access control better than payment. However, the interviewees hinted that this system could potentially suit public transportation, where the payment happens after leaving a bus and the payment sum is based on the distance traveled.

However, utilizing UWB radar for gesture recognition could make the hands-free payment more functional. Instead of accepting the payment with a smartphone, the person could pay by producing a gesture with their hand. The benefit of this would be that the customer does not need to show either a bank card or a smartphone but still be able to confirm the purchase. This kind of system includes multiple risks that must be considered. Firstly, the range of the payment would need to be low, because we need to make sure that no other person can accept the payment in our stead. Secondly, and more importantly, we need to make sure we have authenticated the right person, and the payment will be charged from the correct person. If Person 1 is about to pay, but the system authenticates Person 2 from nearby, Person 2 would be charged if Person 1 could just accept the payment by waving their hand. The security of this system could be increased by requiring a user to perform a specific hand gesture, in which case the gesture would act as a password. However, this would also complicate the system and potentially make it less reliable, as there are nearly infinite ways you could perform a gesture. Although UWB radar has the potential to complement payment systems, the challenges mentioned above make it unpractical for direct use in payment acceptance. However, a comparable hands-free concept could be achieved through more dependable methods, like substituting hand gestures with fingerprints or PIN codes.

While the participants did not believe that we could see another device used for payment outside smartphones, it could be possible with the use of closed loop –payment. As P1 explained, in closed loop –payment, users load money into an account, and payments happen directly without the need for bank verifications. This would also allow payments to happen without the need for internet connection. Places like amusement parks that fee for every use of a machine could utilize these payment devices. Visitors would pay beforehand and receive a UWB device that has been funded with the same amount of virtual money they paid. When they enter a machine, the virtual money is directly reduced from them. After they leave the amusement park, they would return the device. The amusement park could offer various things, like data showing all the machines they visited or a map of where they walked. However, amusement parks already utilize passive RFID wristbands that do not need batteries for closed loop –payment, so parks may be hesitant to switch to a similar UWB system that mostly offers the same benefits as the current system.

This thesis proposes 10 variations of UWB payment. In all examples, UWB is used to authenticate the person, but the method of identifying the customer and the method of accepting the payment varies. Table 6.1 shows an overview of the different techniques.

1. *Motion payment.* Customers simply place their smartphone near a UWB sensor to authorize the purchase. Because you can determine distance accurately with UWB, this method can be adjusted to function akin to NFC technology,

meaning the devices must be a few centimeters apart from each other. This method could be vulnerable to distance reduction attacks. However, the security can be increased by requiring users to keep the mobile application open during the payment process. Additionally, the user could be required to enter a PIN code or scan a fingerprint to finalize the purchase.

2. *Manual selection.* In this system, a cashier manually selects a recipient to send the payment request to. The customer then accepts the request using a mobile application. While this method is reliable, it adds additional work to the cashier and prevents the system from working in unmanned shops and self-checkouts. Moreover, it necessitates the implementation of specific software and a user interface that enables the cashier to select customers.

3. *Proximity payment.* A customer stands near a UWB sensor, and the system sends a payment request to the nearest user. This method is reliable when only one person can occupy the space. Additionally, it should be limited to a certain maximum range to prevent sending a payment request to a wrong customer. This is necessary to address scenarios where the closest customer does not possess a UWB-enabled smartphone, making them undetectable by the system.

4. *Localized payment.* A customer is positioned in a designated area, such as at the end of checkout counter conveyor belt or on the left side of a gas pump, and the system sends a payment request to a person in that area. This approach provides greater flexibility compared to previous methods. However, it is less reliable due to the potential of multiple users in the same area.

5. *Point-to-pay.* A customer points their smartphone towards a machine, and the system sends a payment request to the user. While generally reliable, there is a heightened risk of accidentally pointing the smartphone towards a

machine. If the user is required to keep a mobile application open to recognize the pointing, the system becomes significantly more reliable and minimizes accidents. Proper functionality may require short-range connection.

6. *Smart identification.* The system uses an algorithm to identify the individual currently paying and sends a payment request to the identified customer. While difficult to develop, this method promises flexibility for a customer and no input from a cashier. In the best-case scenario, it will be reliable, but if the algorithm does not work properly, there is a risk of sending payment requests to the wrong people.

7. *Walk-by payment.* A customer passes by a cashier or a gate, and the payment is automatically processed. This system could provide optimal user experience when functioning properly. However, this system is difficult to create as it must work perfectly even in edge cases, and it poses a high risk of erroneous payments as there is no guaranteed mechanism to verify the customer's intention to make the payment.

8. *Hand gesture verification.* A customer accepts payment with a hand gesture, identified by UWB radar. The hand gesture works as a password, necessitating the performance of a specific gesture to confirm the transaction. While this method presents a novel approach to purchasing, its implementation is challenging due to the need for artificial intelligence to accurately identify various gestures, rendering it unreliable and insecure. Additionally, the method poses privacy risks, as anyone in the vicinity could see the hand gesture password.

9. *Biometric verification.* A customer completes the payment with biometric data such as a fingerprint or an eye scan on a separate device. This process should not be overly challenging, as it is already widely used in various applications. While biometric authentication is generally considered secure, there

is a potential risk of fingerprint duplication.

10. *PIN code verification.* In this method, users accept the payment by inputting a PIN code on a separate device. It functions similarly to traditional card payments, with the added convenience of allowing users to keep their phone and card in their pocket during the transaction. This method therefore might be the best overall, offering reliability, flexibility compared to traditional payment, security and potentially being not too difficult to implement.

Table 6.1: Comparison of UWB payment techniques.

Category	Name	Requires payment confirmation	Can keep phone in pocket	Reliable	Area specific	Short range	Secure	Difficult
NFC-like payment	Motion payment	–	○	●	●	●	●	○
Request-based payment	Manual selection	●	○	●	○	○	●	○
	Proximity payment	●	○	●	●	●	●	○
	Localized payment	●	○	–	●	○	●	○
	Point-to-pay	●	○	–	○	–	●	○
	Smart identification	●	○	–	○	○	●	●
Hands-free payment	Walk-by payment	○	●	○	●	●	○	●
	Hand gesture verification	●	●	○	●	●	○	●
	Biometric verification	●	●	●	●	●	●	–
	PIN code verification	●	●	●	●	●	●	–

● = true, ○ = false, – = unsure.

It should be noted that in situations where a user can keep their phone in their pocket, it is uncertain whether it is necessary to have a mobile application open for payment processing. This may be required if the payment is completed in the smartphone. However, the payment does not necessarily have to happen through the smartphone as it could also be completed using a UWB POS device. This approach could enable payments without any user intervention on their smartphone. Additionally, it could allow payments without the need for internet connection, as the POS device would handle the online payment instead of the smartphone. The author is unable to determine the difficulty of designing a separate UWB machine that functions like a payment terminal.

It is also important to note that hand gesture, biometric and PIN code verifications are performed in a separate UWB machine, enabling smartphoneless payment, but these methods could also be implemented into mobile applications as a way to accept a received payment request. In the context of hands-free payment, the system must accurately identify the individual currently making the payment, which should not be an issue in close range. Hands-free payment could therefore function similarly to proximity payment –method, where the correct customer is selected based on the shortest distance to the payment device.

6.2.5 Securing UWB payment

Unfortunately, the interviewees were unable to answer some of the technical questions related to the security of UWB. They expressed multiple times that UWB is secure but did not elaborate on why it is. However, as mentioned before, one reason why UWB is more secure than other technologies is due to TOF-based distance calculating. In addition, the participants were not able to answer the questions related to HRP and LRP.

According to the description of a potential payment system utilizing UWB technology, the vulnerabilities raised in Section 3.4 might not be as concerning as initially deemed. The attacks in question found ways to reduce and increase measurement distance. These attacks are obviously detrimental when targeted towards access control systems, such as when entering a car or a building. However, there seems to be very little if any use for an attacker to manipulate distance or position to affect the request-based payment process. This could lead to similar cases seen with the Bluetooth system where the payment prompt is sent to a wrong person. In these scenarios, the user can just ignore the request, making such an attack senseless. However, implementing a distance-based automatic payment system that does not require acceptance of a payment request, such as NFC-like payment, may be susceptible to these kinds of attacks. Executing a successful distance reduction attack has the potential to trigger unwanted payments, which could be used to steal money.

Depending on the configuration of the payment system, both HRP and LRP modes of UWB can be used securely. While sources claim that LRP mode is more secure than HRP mode, this distinction may not be relevant in some systems. Since distance reduction attacks do not cause much harm in request-based payment systems, these systems may benefit from HRP mode due to its more accurate ranging. However, systems that automatically process payments based on the distance of a device could be vulnerable to distance reduction attacks. For these systems, LRP mode could offer better security. Currently, deployment of a payment system utilizing LRP mode is difficult due to the lack of smartphones featuring LRP-compatible chips, and it remains uncertain whether there is any global interest in integrating LRP-based UWB chips into smartphones.

Despite the system being secured from distance manipulation, there are still security challenges that UWB payment systems must consider, such as ensuring data encryption. It is difficult to say what data needs to be transmitted between the smartphone and the anchors. In the simplest form, the data would only include the position of a customer, the user's identification number and the payment sum. If the smartphone is responsible of payment, card details are likely not sent between the devices since the system does not need them, as the information is stored in the phone and processed in a mobile application when the user accepts the payment request. If this was the case, the security concerns would not be related to UWB but to how the sensitive information is stored in the phone and how the mobile application and online payment service provider handles the data. If the payment is handled in a separate POS device, it is crucial the system transmits the data securely. Furthermore, as UWB operates over a longer distance compared to NFC, the system may be more vulnerable to interference and eavesdropping, even if the payment acceptance is confined to short distances. As a result, UWB payment should utilize tokenization, a method used in mobile payment applications. As elaborated in Section 3.4, smartphones do not send bank card information to a POS machine, but instead transmit a token. Even if eavesdropping were technically feasible, tokenization ensures the attacker will not be able to exploit the obtained information.

However, when building a customized payment solution for individual businesses, it may not be necessary to transmit any payment related information between devices. Many online shops offer the option to save the customers' card details on their servers, allowing seamless purchases without the need for manual input of card information for each purchase. UWB payment systems could adopt a similar approach, meaning the card information is not stored in a smartphone and sent to the system, but instead the information is stored in the system itself and is automatically retrieved upon authentication of the cardholder. This approach would make the UWB connections more secure, and instead the security lies on how the system stores the card information. Similarly, a tailored solution would eliminate the need to send payment sums and requests to the customer via UWB, as the system could simply send a notification on the user's mobile application via the internet upon identification. This way UWB is only required to transmit the user's identification number and location data to the system.

Even if the payment process seems secure, the ability to tamper position data could cause potentially harmful effects for companies and consumers using UWB-based payment systems. Researchers found that a few popular UWB RTLS solutions were using non-encrypted data communication, which enabled them to eavesdrop and alter position data of tags. This would allow an attacker to place tags on forbidden areas and cause false alarms. This could also be used to steal items by modifying a tag to appear in place while the item alongside the tag is physically removed from the area. [72]

As one of the main motivations for businesses to adopt UWB payment could be the inclusion of additional user data, it raises many ethical and privacy related questions. If a user does not have the mobile application open, can the store still collect location data from them? Will the data be anonymized? Can the user pay using UWB while declining the collection of private data? Would the businesses even be interested in using the system if customers can decline the collection of data? While this thesis did not focus on privacy or ethics, these factors are important when designing such a system. The system should be transparent and inform users that their data is being gathered and specify what data is collected. Given the system's heavy reliance on location-based features, users may be required to consent to the collection of location data to use the service. It should be recognized that extensive collection of private data could negatively impact UWB payment adoption by making the system less appealing to customers. However, it is worth noting that many modern services collect user data to some extent, meaning most consumers may not be concerned on this matter.

6.3 Limitations

The main limitation of this thesis is the small sample size. Despite only two experts being interviewed, it is noteworthy that the participants expressed similar viewpoints, suggesting that further interviews might have yielded alike results. Including more UWB experts might not have provided further insight into the topic, because the novelty of UWB payment limits the basis to form an opinion on. As P2 said, there is no global discussion on UWB payment at the moment. Still, the inclusion of more participants, particularly from the payment sector, could have enriched the study, considering that only one individual had experience in the payment industry.

Furthermore, the study could have benefited from interviewing participants in closer alignment with the topic, such as individuals directly involved in the implementation and operation of a real UWB payment system. These interviews could have provided valuable firsthand perspectives on the system's practical advantages and limitations, as well as insights into market demand. The predominance of market experts over technical experts among the interviewees may have also given a restricted understanding of the topic.

Lastly, the exclusive focus on expert interviews may have overshadowed alternative viewpoints that could have provided a more comprehensive understanding of the requirements of a UWB payment system. While the experts did touch upon the potential benefits of UWB payment from the perspective of the system's adopters and end-users, gathering statements directly from these stakeholders through user interviews could offer more valuable information, such as their experiences and preferences on a mobile payment system.

6.4 Future research

Further exploration into automatic payment systems utilizing UWB technology could offer valuable information into the potential benefits and challenges of this innovative payment method. More research in UWB radar technology could clarify the feasibility and effectiveness of its use for payment transactions, potentially unlocking solutions for secure and convenient automatic payment.

Researching how companies in various sectors could leverage UWB payment technology and gauging their interest in adopting such systems could illuminate the potential market demand and opportunities for UWB payment solutions. Additionally, studies could prioritize gathering user feedback by implementing a prototype of a UWB payment system. Understanding user preferences, concerns, and interest in mobile payment technologies could guide the design of user-friendly UWB payment solution.

Exploring the security implications and potential vulnerabilities of UWB payment systems is essential for safeguarding sensitive data and preventing fraudulent activities. While UWB security has been largely studied, future research could focus on addressing security concerns specifically on UWB's use on payment.

7 Conclusion

In this thesis, the possibility of using Ultra-Wideband technology for contactless payment is discussed. Previous studies on this innovative solution are minimal, making this thesis one of the first ones to thoroughly explore the perspective. As previously stated, UWB is simply another radio technology, but its exceptional accuracy in positioning could enhance and introduce distinctive elements to the payment process. The security features of this technology could make payment even safer.

Initially, the theoretical part of the thesis was done to acquire a comprehensive understanding of both UWB technology and payment systems. The research on UWB involved an examination of UWB's technical aspects, practical applications, the impact of the current standards and regulations, as well as a comparative analysis with similar technologies to find out the capabilities and drawbacks of UWB. Subsequently, payment systems were studied by exploring how technologies such as NFC, QR code and mobile payment work. Finally, the security aspects of UWB and the previously mentioned payment technologies were analyzed.

Four hypotheses were formulated based on the research material that this study aims to find answers to:

1. UWB technology will become more popular.

2. UWB payment will not replace bank cards.

3. UWB will become the most used mobile payment option.

4. UWB is secure for contactless payment.

Due to the innovativeness of this system, this thesis focused on gathering UWB experts' opinions through interviews. The interviews aimed to find answers to feasibility of UWB payment but also insight on expected global growth and technical challenges of the technology. The interviews were semi-structured to gather various viewpoints and were conducted remotely in Microsoft Teams. The interviews were recorded and later transcribed.

Based on the analysis of research material and interview findings, it is evident that all four hypotheses proposed in this thesis hold merit. The consensus among experts supports the anticipated rise in popularity of UWB technology. While UWB payment solutions are not expected to entirely replace traditional bank cards, given the requirement for a power source and potential internet connectivity, they are poised to establish themselves as the leading mobile payment option. This is supported by their enhanced security features, swift transactions, ease of use and low cost of implementation. Compared to current payment solutions, UWB payment offers diverse and innovative methods to pay, while providing comprehensive user data analytics. Lastly, the participants affirm UWB is suitable and secure for contactless payment. The security implications are highlighted in access control applications, where UWB is gradually replacing NFC and Bluetooth technologies.

The study on UWB payment systems has identified three fundamental components essential for the system's operation: smartphones, mobile applications and UWB anchors. Smartphones emerge as the most pragmatic choice for facilitating UWB payment transactions, given the possibility to use mobile applications for authentication and payment acceptance. The existing payment terminals are not suitable for UWB payment due to the lack of UWB support and the challenge of accommodating UWB technology in compliance with the current payment standards. However, UWB payment does not rely on these standards to work, as the technology primarily serves as a means of authentication, with the actual payment transaction processed as an online purchase. As a result, UWB payment system requires the implementation of either dedicated UWB POS devices or a UWB anchor network that communicates with consumers' smartphones. Given the prevalence of store-specific mobile applications, a practical approach to fostering the adoption of UWB payment involves integrating UWB connectivity and online payment capabilities into these existing mobile applications.

This thesis proposes several methods for how UWB payment could operate. Firstly, the proposed system could mirror the functionality of NFC technology, whereby placing a smartphone close to a POS device accepts payment. Secondly, an alternative approach involves sending a payment request to a smartphone. The anchors identify the payer, transmit a payment request to the individual, and the said customer authorizes the payment through a mobile application. Lastly, a third model envisions a scenario where the payment process transpires seamlessly without the need to operate a smartphone. The POS device identifies the paying customer, who then inputs a PIN code on the POS terminal. The POS device retrieves the requisite payment details and finalizes the transaction without the need for active smartphone engagement during the payment process.

Several constraints prevent the widespread adoption of UWB payment systems, particularly the lack of standards, global regulatory challenges, inaccessibility of UWB smartphones, and limited number of consumer applications. For UWB payment to achieve global success, the technology needs to become more available in smartphones. Notably, Apple has significantly contributed to this endeavor by integrating UWB across its latest devices, however, the absence of UWB is evident on Androids devices. To increase availability, there needs to be more incentives to include UWB in smartphones, alongside efforts to minimize design costs to make the inclusion of UWB chips possible in more affordable models.

More in-depth research into UWB payment systems will help in gaining knowledge of usability, acceptance, and potential challenges associated with this emerging payment technology. Collaborating with various experts and stakeholders can provide a holistic understanding of the market landscape and facilitate the development of tailored UWB payment solutions.

The potential applications of UWB technology are vast, however, it remains to be seen whether payment establishes as a core use case of UWB. Although UWB will not change the payment per se, its integration could streamline the steps needed for completing mobile payments, therefore evolving payment systems to become more secure, flexible and user-friendly.

References

[1] R. Triggs, "What is UWB, and why is it in my phone? Ultra wideband technology, explained", 2023. [Online]. Available: https://www.androidauthority.com/what-is-uwb-1151744/ (visited on 15.9.2023).

[2] R. S. Kshetrimayum, "An introduction to UWB communication systems", *Ieee Potentials*, vol. 28, no. 2, pp. 9–13, 2009.

[3] M. Viot, A. Bizalion, and J. Seegars, "Exploring Ultra-Wideband Technology for Micro-Location-Based Services.", *Microwave Journal*, vol. 64, no. 6, 2021.

[4] Qorvo, "Getting Back to Basics with Ultra-Wideband (UWB)", 2021. [Online]. Available: https://www.qorvo.com/resources/d/qorvo-getting-back-to-basics-with-ultra-wideband-uwb-white-paper (visited on 8.4.2024).

[5] F. Nekoogar, *Ultra-Wideband Communications: Fundamentals and Applications Fundamentals and Applications*. Prentice Hall Press, 2011.

[6] D. Coppens, A. Shahid, S. Lemey, B. V. Herbruggen, C. Marshall, and E. D. Poorter, "An overview of UWB standards and organizations (IEEE 802.15. 4, FiRa, Apple): Interoperability aspects and future research directions", *IEEE Access*, vol. 10, pp. 70 219–70 241, 2022.

[7] C. Connell, "What's The Difference Between Measuring Location By UWB, Wi-Fi, and Bluetooth?", 2015. [Online]. Available: https://www.electronicdesign.com/technologies/communications/article/21800581/whats-the-

difference-between-measuring-location-by-uwb-wifi-and-bluetooth (visited on 8.4.2024).

[8] FiRa Consortium, "Unleashing the Potential of UWB: Regulatory Considerations", 2022. [Online]. Available: https://www.firaconsortium.org/sites/default/files/2022-08/Unleashing-the-Potential-of-UWB-Regulatory-Considerations.pdf (visited on 8.4.2024).

[9] D. Spitler, "Applying Ultra-Wideband Wireless Technology for Security and Automation", 2020. [Online]. Available: https://www.securityindustry.org/2020/11/17/applying-ultra-wideband-wireless-technology-for-security-and-automation/ (visited on 8.4.2024).

[10] M. Singh, "Securing distance measurement against physical layer attacks", Ph.D. dissertation, ETH Zurich, 2021.

[11] M. Stocker, B. Großwindhager, C. A. Boano, and K. Römer, "Towards secure and scalable UWB-based positioning systems", in *2020 IEEE 17th International Conference on Mobile Ad Hoc and Sensor Systems (MASS)*, IEEE, 2020, pp. 247–255.

[12] J. Niewczas, D. Neirynck, C. McElroy, M. McLaughlin, I. Dotlic, and M. O'Duinn, "Secure Ultra Wide Band Ranging", UK Patent No. GB2600549A, 2022. [Online]. Available: https://patents.google.com/patent/GB2600549A/en (visited on 8.4.2024).

[13] S. Čapkun, "On the Security of (UWB) Distance Measurement", 2021. [Online]. Available: https://www.youtube.com/watch?v=KEqRKA9nv70 (visited on 8.4.2024).

[14] P. Leu *et al.*, "Ghost Peak: Practical Distance Reduction Attacks Against HRP UWB Ranging", in *31st USENIX Security Symposium (USENIX Security 22)*, 2022, pp. 1343–1359.

[15] R. Yassminh, "What Are the Differences between Accuracy and Precision?", 2023. [Online]. Available: https://medium.com/@ryassminh/what-are-the-differences-between-accuracy-and-precision-b4535f99f464 (visited on 8.4.2024).

[16] B. Silva, Z. Pang, J. Åkerberg, J. Neander, and G. Hancke, "Experimental study of UWB-based high precision localization for industrial applications", in *2014 IEEE International Conference on Ultra-WideBand (ICUWB)*, IEEE, 2014, pp. 280–285.

[17] FiRa Consortium, "UWB Use Cases", 2023. [Online]. Available: https://www.firaconsortium.org/discover/use-cases (visited on 28.9.2023).

[18] S. Shankland, "Apple's U1 Chip, Android Boost UWB Tech That Lets Your Phone Unlock Your Car", 2022. [Online]. Available: https://www.cnet.com/tech/mobile/apples-u1-chip-and-android-brings-uwb-location-tech-to-your-car-or-home/ (visited on 8.4.2024).

[19] B. Schoon, "Samsung expects UWB to be as big as Bluetooth, Xiaomi shows how it improves the smart home", 2020. [Online]. Available: https://9to5google.com/2020/10/12/samsung-uwb-tech-xiaomi-smart-home-demo/ (visited on 8.4.2024).

[20] Real Mi Central, "The Google Pixel 6 Pro UWB chip can be used by third-party apps", 2022. [Online]. Available: https://www.realmicentral.com/2022/02/08/the-google-pixel-6-pro-uwb-chip-can-be-used-by-third-party-apps/ (visited on 8.4.2024).

[21] BMW Group, "Android smartphones become fully fledged vehicle keys: BMW Digital Key Plus now also available on compatible Android devices.", 2023. [Online]. Available: https://www.press.bmwgroup.com/global/article/detail/T0413528EN/android-smartphones-become-fully-fledged-

vehicle-keys:-bmw-digital-key-plus-now-also-available-on-compatible-android-devices (visited on 8.4.2024).

[22] Samsung Newsroom, "Unlock a New Experience: Galaxy Users Can Now Use Secure Digital Key With the Genesis GV60", 2021. [Online]. Available: https://news.samsung.com/global/unlock-a-new-experience-galaxy-users-can-now-use-secure-digital-key-with-the-genesis-gv60 (visited on 8.4.2024).

[23] A. I. Shaik, "Samsung Wallet gets access to world's first UWB-based smart door lock", 2022. [Online]. Available: https://www.sammobile.com/news/samsung-wallet-worlds-first-uwb-digital-home-key/ (visited on 8.4.2024).

[24] N. Dahad, "Lenovo adds Novelda UWB sensor for human presence detection in ThinkPad", 2020. [Online]. Available: https://www.embedded.com/lenovo-adds-novelda-uwb-sensor-for-human-presence-detection-in-thinkpad/ (visited on 8.4.2024).

[25] B. Dowsett, "The World Cup's New High-Tech Ball Will Change Soccer Forever", 2022. [Online]. Available: https://fivethirtyeight.com/features/the-world-cups-new-high-tech-ball-will-change-soccer-forever/ (visited on 8.4.2024).

[26] P. S. Sharma, S. Vijay, and M. Shukla, "Ultra-wideband technology: Standards, characteristics, applications", *Helix-The Scientific Explorer| Peer Reviewed Bimonthly International Journal*, vol. 10, no. 04, pp. 59–65, 2020.

[27] C.-C. Chong, F. Watanabe, and H. Inamura, "Potential of UWB technology for the next generation wireless communications", in *2006 IEEE Ninth International Symposium on Spread Spectrum Techniques and Applications*, IEEE, 2006, pp. 422–429.

[28] L. Flueratoru, "Robust, Energy-Efficient, and Scalable Indoor Localization with Ultra-Wideband Technology", 2023.

[29] V. Niemelä, J. Haapola, M. Hämäläinen, and J. Iinatti, "An ultra wideband survey: Global regulations and impulse radio research based on standards", *IEEE Communications Surveys & Tutorials*, vol. 19, no. 2, pp. 874–890, 2016.

[30] ETSI, "Short Range Devices (SRD) using Ultra Wide Band (UWB); Part 3: Worldwide UWB regulations between 3,1 and 10,6 GHz", Tech. Rep. 103 181-3 V2.1.1, 2019. [Online]. Available: https://www.etsi.org/deliver/etsi_tr/103100_103199/10318103/02.01.01_60/tr_10318103v020101p.pdf (visited on 8.4.2024).

[31] C. Swedberg, "UWB Alliance Aims for Interoperability", 2019. [Online]. Available: https://www.rfidjournal.com/uwb-alliance-aims-for-interoperability (visited on 8.4.2024).

[32] K. S. Gopalan, A. Bansal, and A. R. Kabbinale, "Tracking Resurgence of Ultra-Wideband-A Standards and Certification Perspective", in *2022 14th International Conference on COMmunication Systems & NETworkS (COMSNETS)*, IEEE, 2022, pp. 894–898.

[33] omlox. "The open locating standard". (2023), [Online]. Available: https://omlox.com/ (visited on 8.4.2024).

[34] J. Li, "Research and Analysis on the Signal Regime of 802.15. 4z Protocol LRP UWB Communication and Navigation Integration", in *International Conference on Internet of Things, Communication and Intelligent Technology*, Springer, 2022, pp. 234–244.

[35] IEEE Standards Association, *802-2014–IEEE Standard for Local and Metropolitan Area Networks: Overview and Architecture*, 2014.

[36] A. Heinrich, S. Krollmann, F. Putz, and M. Hollick, "Smartphones with UWB: Evaluating the Accuracy and Reliability of UWB Ranging", *arXiv preprint arXiv:2303.11220*, 2023.

[37] IEEE 802, "IEEE 802.15 WSN™ Task Group 4ab (TG4ab) 802.15.4 UWB Next Generation", 2021. [Online]. Available: https://www.ieee802.org/15/pub/TG4ab.html (visited on 8.4.2024).

[38] FiRa Consortium, "FiRa Consortium Publishes FiRa 2.0 Technical Specifications", 2023. [Online]. Available: https://www.firaconsortium.org/news/press-releases/2023/11/fira-consortium-publishes-fira-2-0-technical-specifications (visited on 8.4.2024).

[39] T. Arsan and O. Kepez, "Early steps in automated behavior mapping via indoor sensors", *Sensors*, vol. 17, no. 12, p. 2925, 2017.

[40] S. Djosic, I. Stojanovic, M. Jovanovic, and G. L. Djordjevic, "Multi-algorithm UWB-based localization method for mixed LOS/NLOS environments", *Computer Communications*, vol. 181, pp. 365–373, 2022.

[41] K. M. Tan and C. L. Law, "GPS and UWB integration for indoor positioning", in *2007 6th International Conference on Information, Communications & Signal Processing*, IEEE, 2007, pp. 1–5.

[42] A. Waqar, I. Ahmad, D. Habibi, and Q. V. Phung, "Analysis of GPS and UWB positioning system for athlete tracking", *Measurement: Sensors*, vol. 14, p. 100 036, 2021.

[43] I. R. D. Luna, F. Liébana-Cabanillas, J. Sánchez-Fernández, and F. Muñoz-Leiva, "Mobile payment is not all the same: The adoption of mobile payment systems depending on the technology applied", *Technological Forecasting and Social Change*, vol. 146, pp. 931–944, 2019.

[44] S. den Uijl and H. J. de Vries, “Pushing technological progress by strategic manoeuvring: the triumph of Blu-ray over HD-DVD”, *Business History*, vol. 55, no. 8, pp. 1361–1384, 2013.

[45] D. Nelson, M. Qiao, and A. Carpenter, “Security of the near field communication protocol: an overview”, *Journal of Computing Sciences in Colleges*, vol. 29, no. 2, pp. 94–104, 2013.

[46] N. Juopperi, “UWB implementation and utilization in mPOS device”, M.S. thesis, University of Oulu, 2022.

[47] NXP Semiconductors, “NXP Accelerates UWB-based Mobile Payment Innovation with NTT DOCOMO and Sony”, 2020. [Online]. Available: `https://www.nxp.com/company/about-nxp/nxp-accelerates-uwb-based-mobile-payment-innovation-with-ntt-docomo-and-sony:NW-UMB-MOBILE-PAYMENT-DOCOMO-SONY` (visited on 8.4.2024).

[48] NXP Semiconductors, “NXP Collaborates with ING and Samsung to Pilot Industry’s First UWB-Based Peer-to-Peer Payment Application”, 2022. [Online]. Available: `https://www.nxp.com/company/about-nxp/nxp-collaborates-with-ing-and-samsung-to-pilot-industrys-first-uwb-based-peer-to-peer-payment-application:NW-NXP-COLLABORATES-WITH-ING-AND-SAMSUNG-TO` (visited on 8.4.2024).

[49] K. Hannula and I. Angerpuro, *Building a contactless future*, 2021. [Online]. Available: `https://futureofretail.io/blog/building-a-contactless-future` (visited on 8.4.2024).

[50] S. Chabbi, N. E. Madhoun, and L. Khamer, “Security of nfc banking transactions: Overview on attacks and solutions”, in *2022 6th Cyber Security in Networking Conference (CSNet)*, IEEE, 2022, pp. 1–5.

[51] M. King, "22 Contactless Payment Statistics for 2023", 2023. [Online]. Available: https://fitsmallbusiness.com/contactless-payment-statistics/ (visited on 6.10.2023).

[52] CFPB, "Big Tech's Role in Contactless Payments: Analysis of Mobile Device Operating Systems and Tap-to-Pay Practices", 2023. [Online]. Available: https://www.consumerfinance.gov/data-research/research-reports/big-techs-role-in-contactless-payments-analysis-of-mobile-device-operating-systems-and-tap-to-pay-practices/full-report/ (visited on 8.4.2024).

[53] M. Cocosila and H. Trabelsi, "An integrated value-risk investigation of contactless mobile payments adoption", *Electronic Commerce Research and Applications*, vol. 20, pp. 159–170, 2016.

[54] T. Bradford, F. Hayashi, and Y. L. Toh, "Developments of QR Code-Based Mobile Payments in East Asia", *Federal Reserve Bank of Kansas City, Payments System Research Briefing, June*, vol. 18, 2019.

[55] M. Fiedler, "Apple-pay, towards the acceptance of German customers", *Asian Social Science*, vol. 11, no. 22, p. 124, 2015.

[56] S. Perez, "Apple won't have to allow third-party payments on App Store as case goes to Supreme Court", 2023. [Online]. Available: https://techcrunch.com/2023/07/18/apple-wont-have-to-allow-third-party-payments-on-app-store-as-case-goes-to-supreme-court/ (visited on 8.4.2024).

[57] S. Duke, "Can Samsung Pay, Google Pay and Apple Pay work without an internet connection? | Ask Us Anything 52", 2023. [Online]. Available: https://soyacincau.com/2023/05/29/samsung-pay-google-pay-apple-pay-work-offline-without-an-internet-connection-ask-us-anything-52/ (visited on 8.4.2024).

[58] Finanssiala, "Maksutavat 2022", 2023. [Online]. Available: https://www.finanssiala.fi/wp-content/uploads/2023/02/maksutavat-2022.pdf (visited on 8.4.2024).

[59] European Central Bank, "Study on the Payment Attitudes of Consumers in the Euro Area (SPACE)", 2022. [Online]. Available: https://www.ecb.europa.eu/stats/ecb_surveys/space/shared/pdf/ecb.spacereport202212~783ffdf46e.en.pdf (visited on 8.4.2024).

[60] Danmarks Nationalbank, "Denmark is among the most digitalised countries when it comes to payments", 2022. [Online]. Available: https://www.nationalbanken.dk/media/mujcrjnf/analysis-nr-2-denmark-is-among-the-most-digitalised-countries-when-it-comes-to-payments.pdf (visited on 8.4.2024).

[61] Y. Wang, C. Hahn, and K. Sutrave, "Mobile payment security, threats, and challenges", in *2016 second international conference on mobile and secure services (MobiSecServ)*, IEEE, 2016, pp. 1–5.

[62] C. Cavaglieri, "Contactless cards explained", 2023. [Online]. Available: https://www.which.co.uk/money/banking/banking-security-and-payment-methods/contactless-cards-aoMsk0v9xBc1 (visited on 8.4.2024).

[63] P. Kieseberg *et al.*, "QR code security", in *Proceedings of the 8th International Conference on Advances in Mobile Computing and Multimedia*, 2010, pp. 430–435.

[64] K. Zetter, "New attack can unlock and start a Tesla Model Y in seconds, say researchers", 2022. [Online]. Available: https://www.theverge.com/2022/9/12/23348765/tesla-model-y-unlock-drive-car-thief-nfc-relay-attack (visited on 8.4.2024).

[65] J. Maguire, "UK car theft hotspots revealed as keyless crime reaches record high", 2021. [Online]. Available: https://www.fleetnews.co.uk/news/car-industry-news/2021/03/03/uk-car-theft-hotspots-revealed-as-keyless-crime-reaches-record-high (visited on 8.4.2024).

[66] FiRa Consortium, "UWB Secure Ranging in FiRa", 2022. [Online]. Available: https://www.firaconsortium.org/sites/default/files/2022-09/FIRA-Whitepaper-UWB-Secure-Ranging-August-2022_0.pdf (visited on 8.4.2024).

[67] C. Welch, "Google delays its upgraded, more expansive Find My Device network", 2023. [Online]. Available: https://www.theverge.com/2023/7/27/23810052/google-find-my-device-delay-apple-unknown-tracker-alerts-stalking (visited on 8.4.2024).

[68] L. Sun, P. Liu, Y. Wang, and D. Yang, "Integrity protection to support secure ranging in IR-UWB", 2022. [Online]. Available: https://mentor.ieee.org/802.15/dcn/22/15-22-0072-00-04ab-integrity-protection-to-support-secure-ranging-in-ir-uwb.pptx (visited on 8.4.2024).

[69] M. Cheraghinia *et al.*, "A Comprehensive Overview on UWB Radar: Applications, Standards, Signal Processing Techniques, Datasets, Radio Chips, Trends and Future Research Directions", *arXiv preprint arXiv:2402.05649*, 2024.

[70] S. Skaria, A. Al-Hourani, and R. J. Evans, "Deep-learning methods for hand-gesture recognition using ultra-wideband radar", *IEEE Access*, vol. 8, pp. 203 580–203 590, 2020.

[71] Icograms, "Icograms Designer", 2024. [Online]. Available: https://icograms.com/designer (visited on 8.4.2024).

[72] B. Toulas, "RTLS systems vulnerable to MiTM attacks, location manipulation", 2022. [Online]. Available: https://www.bleepingcomputer.com/

news/security/rtls-systems-vulnerable-to-mitm-attacks-location-manipulation/ (visited on 8.4.2024).

Appendix A Interview Questions

UWB in general

- What are the most interesting aspects of UWB?
- What is the reason there is not more UWB applications?
- Is there any truly unique use case for UWB that is not possible with any other technology?
- On consumer level, UWB is mainly now used for data transfer and device locating. Is there something else where UWB could be used in daily life?
- On consumer level, the focus seems to be in using UWB in smartphones. Could there be other type of UWB devices for consumers in the future?
- Do you think UWB will replace some of the current technologies, like Bluetooth or NFC?
- GPS is the go-to technology for outdoor positioning, do you think in the future all indoor positioning applications will use UWB?

HRP and LRP

- HRP UWB is currently used more than LRP. Why are most of the companies using HRP UWB?

- As HRP is more popular, are there any use cases for LRP or should you always use HRP?
- Many studies conduct that LRP is secure, while HRP is not that secure. Will that cause a problem when implementing secure systems, as for example smartphones use HRP?

UWB payment

- When UWB use cases are discussed, there is always a mention that UWB can be used for contactless payment. Why is there currently no UWB payment system?
- In payment context, is there something UWB could add that is not possible with the current technologies?
- NFC payment has been available on smartphones for a long time, but at least in Finland, bank cards are still the most used payment method. Would people really use UWB payment if it was available on their smartphones?
- Realistically, to achieve secure payment, what would be the range of UWB payment?
- UWB has been said that it would allow hands-free payment, for example that you could leave your phone in your pocket. Isn't this a big security risk, as the user doesn't have to verify the payment and instead it does it automatically?
- Is current UWB sufficient for secure payment, or is there something that should be done, like changes in regulations or new standards?

Bonus question

- Do you think in the future everyone will know what UWB is, similarly how pretty much everyone knows what GPS or Bluetooth is?

Appendix B Haastattelukysymykset

UWB yleisesti

- Mitkä ovat kiinnostavimmat ominaisuudet UWB tekniikassa?
- Miksi kuitenkin UWB ei ole tällä hetkellä yleisessä käytössä?
- Onko UWB:lla jotain uniikkia käyttökohdetta, joka ei ole mahdollista muille tekniikoilla?
- Kuluttajapuolella UWB:ta käytetään lähinnä laitteiden paikantamiseen ja datan siirtoon. Onko jotain muita käyttökohteita missä UWB voisi auttaa jokapäiväisessä elämässä?
- Kuluttajapuolella tunnutaan painottavan UWB:n käyttämistä älypuhelimissa. Voisiko tulevaisuudessa olla joitain muitakin kuluttajalaitteita, jotka käyttävät UWB:ta?
- Tuleeko UWB mielestäsi korvaamaan jonkun nykyisen teknologian, kuten Bluetoothin tai NFC?
- GPS on tavanomaisin teknologia ulkona paikantamiseen. Tuleeko mielestäsi tulevaisuudessa kaikki sisäpaikannussysteemit käyttämään UWB:ta?

HRP ja LRP

- HRP UWB on tällä hetkellä yleisempi kuin LRP. Miksi monet yritykset käyttävät HRP UWB?

- Koska HRP on yleisempi, onko mitään syytä käyttää LRP vai pitäisikö aina käyttää HRP?

- Monet tutkimukset ovat todenneet LRP turvalliseksi, kun taas HRP ei ole niin turvallinen. Tuleeko tämä aiheuttamaan ongelmia turvallisen systeemin luomisessa, koska esimerkiksi älypuhelimet käyttävät HRP?

UWB maksaminen

- Kun UWB käyttökohteista puhutaan, lähimaksaminen mainitaan aina yhtenä käyttökohteista. Miksi UWB maksujärjestelmiä ei ole olemassa?

- Voisiko UWB tuoda jotain uutta maksamiseen, mikä ei ole mahdollista nykyisillä teknologioilla?

- NFC maksaminen on ollut pitkään mahdollista älypuhelimissa, mutta ainakin Suomessa tavallinen pankkikortti on edelleen käytetyin maksumetodi. Käyttäisikö ihmiset oikeasti UWB:ta maksamiseen, jos se olisi mahdollista älypuhelimissa?

- Mikä on realistinen etäisyys UWB maksamiselle, jotta se olisi turvallinen?

- UWB:n sanotaan mahdollistavan maksamisen ilman käsiä (hands-free), esimerkiksi voisit pitää älypuhelinta taskussa. Eikö tämä ole iso turvallisuusriski, sillä käyttäjän ei tarvitse vahvistaa maksua vaan se tapahtuu automaattisesti?

- Voiko UWB:ta tällä hetkellä käyttää turvalliseen lähimaksamiseen, vai pitäisikö jotain sitä ennen tehdä, esimerkiksi muuttaa kansainvälisiä regulaatioita tai tuoda uusia standardeja?

Bonuskysymys

- Tuleeko tulevaisuudessa kaikki tietämään mikä UWB on, samantapaisesti kuten nyt melkein kaikki tietävät, mikä GPS ja Bluetooth ovat?