FH JOANNEUM
University of Applied Sciences

Direct Peer to Peer Communication on iOS Devices

When mediator based technology is not available

Bachelor's Thesis

submitted in conformity with the requirements for the degree of

Bachelor of Science in Engineering (BSc)

Bachelor's degree programme **Software Design and Cloud Computing**

FH JOANNEUM (University of Applied Sciences), Kapfenberg

Supervisor: DI Johannes Feiner

Submitted by: Matthias Bartholomäus

February 2025

TODO: Specify the title, subtitle, author, submission date, study, language, your name, and supervisor/advisor in the main *thesis.typ* file. Then compile with *typst compile thesis.typ*. Finally, remove all TODOs (todo marcos) within your typst ource code.

Preview printed 2025-04-30.

Abstract

Modern mobile devices can make use of a wide variety of communication technologies. Besides having different applicabilities and protocols, standards like Bluetooth, WiFi or 5G need to be wireless to seamlessly transfer data. In resent years global economic demand has impacted research and development to vastly improve data transmission and hardware on smartphones. As of 2024 this led to over 4 billion smartphones users worldwide (Statista Research Department, 2024), 27% covered by iOS. Unfortunately most of the communication methods used on smartphones all rely on mediators. Be it a router in a local network or a cell tower in a cellular network, without these nodes a connection between two peers can not be established, no matter how close neighboring devices may be. However in scenarios where the required infrastructure is not available, communication between two mobile iOS devices can be established via Bluetooth or ad hoc WiFi since these do not required pre-existing infrastructure and purely rely on local radio broadcast, whereas the latter is recommended to use. Due to the latest advancements in these technologies, it is unclear how good direct Peer to Peer (P2P) networks work under different surroundings and how the choice of the transport protocol affects the connection. In this thesis, an iOS prototype is developed, that connects two peers via Apple Wireless Direct Link (AWDL) and measures metrics that describe the quality of the connection like Round Trip Time (RTT), Jitter, data speed and more. The results show that AWDL achieves the best metrics when tested in surroundings with low radio frequency pollution. Prototype measurements also show that UDP achieves the fastest data rates, with a compromise on data loss. In consideration of the findings, it can be stated that AWDL on iOS devices is not yet ready for wide area communication or building reliable mesh networks, but can be utilized for low distance applications.

Keywords: FHJ, SWD, iOS, peer-to-peer, ad-hoc, smartphone, Apple

Kurzfassung

Moderne Mobilgeräte können eine Vielzahl an Kommunikationstechnologien nutzen. Neben unterschiedlichen Anwendungsmöglichkeiten und Protokollen müssen Standards wie Bluetooth, WiFi oder 5G drahtlos sein, um Daten im modernen Kontext übertragen zu können. In den letzten Jahren hat sich die weltweite wirtschaftliche Nachfrage auf die Forschung und Entwicklung ausgewirkt, und so die Datenübertragung und die Hardware von Smartphones erheblich verbessert. Dies hat dazu geführt, dass im Jahr 2024 weltweit über 4 Milliarden Smartphones genutzt werden (Statista Research Department, 2024), 27 % davon unter iOS. Leider sind die meisten der auf Smartphones verwendeten Kommunikationsmethoden auf Infrastruktur angewiesen. Ein Router in einem lokalen Netz oder ein Sendemast in einem Mobilfunknetz, ohne diese Knoten kann keine Verbindung zwischen zwei Endgeräten hergestellt werden, egal wie nah diese sein mögen. In diesen Szenarien kann die Kommunikation zwischen zwei mobilen iOS-Geräten über Bluetooth oder Ad-hoc-WiFi hergestellt werden, da diese keine bereits vorhandene Infrastruktur benötigen und sich ausschließlich auf lokale Broadcasts stützen, wobei letztere Technologie empfohlen wird. Aufgrund der jüngsten Fortschritte bei diesen Technologien ist unklar, wie gut direkte P2P-Netzwerke in verschiedenen Umgebungen funktionieren und wie die Wahl des Transportprotokolls die Verbindung beeinflusst. In dieser Arbeit wird ein iOS-Prototyp entwickelt, der zwei Endgeräte über Apple Wireless Direct Link (AWDL) verbindet und Metriken misst, die die Qualität der Verbindung beschreiben, wie Round Trip Time (RTT), Jitter, Datengeschwindigkeit und mehr. Die Ergebnisse zeigen, dass AWDL die besten Werte erzielt, wenn es in einer Umgebung mit geringer Funkfrequenzbelastung getestet wird. Messungen des Prototypen zeigen auch, dass UDP die schnellste Datenübertragungsrate erreicht, allerdings mit einem Kompromiss bei den Datenverlusten. Ein Resümee zeigt, dass AWDL auf iOS-Geräten noch nicht für die Weitbereichskommunikation oder den Aufbau zuverlässiger Mesh-Netzwerke geeignet ist, aber für Anwendungen mit geringer Entfernung eingesetzt werden kann.

Contents

List of Figures

List of Tables

List of Listings

List of Listings

Optionally, you might add an **Acknowledgements** section (in German **Danksagung**) to say thank you or give credits to someone.

1 | Related Work

The following is a non-comprehensive discussion covering previous research of peer-to-peer technologies in the mobile context. After covering historic considerations of mobile ad hoc networks (MANET) research and device to device D2D communication in cellular networks via standards like LTE-Direct or 5G New radio (NR) Sidelink (SL), a deeper introduction to Apples ecosystem and Apple Wireless Direct Link (AWDL) is given, where a lot is based on the open wireless link (OWL) project from the TU Darmstadt. While reverse engineered the AWDL protocol, the team found several security concerns in Apple's operating systems and developed some open source applications for public use which they shared on GitHub.

1.1 History of MANET

Already back in 2001 the Proem project (Kortuem, Schneider, Preuitt, *et al.*, 2002) examined different aspects of peer-to-peer applications for mobile ad hoc networks (MANET) to enable proximity-based collaboration. In particular, Proem was an approach to provide high-level support for mobile peer-to-peer application developers and was tested by students of the University of Oregon, whilst creating an MP3 file-sharing system. They already noticed the trend for an ever-larger becoming applicability of personal mobile devices for data sharing but listed resources of mobile devices among other possible limitations. This facet has vastly changed since then and several new ideas like ShAir (Dubois, Bando, Watanabe, *et al.*, 2013), a middleware infrasructure for peer-to-peer sharing between mobile devices or mFerio (Balan, Ramasubbu, Prakobphol, *et al.*, 2009), a peer-to-peer mobile payment system have emerged.

Balan, Ramasubbu, Prakobphol, *et al.* working on mFerio already noticed the problem that mobile devices rely too heavily on static infrastructure. Back then cell phones have already become popular tools that combined calendars, address books, messaging or cameras. The increasing need to use them as a payment vehicle has become ever larger and the authors questioned the state of the art implementations back then. In particular mobile payment solution required constantly stable connections via either SMS or GSM/CDMA based technologies which were connected to a backend payment server. They noticed that these implementation, which were to heavily relying on external systems could not replace cash based systems and aimed to develop a decentraliced approach based on NFC. The goal of their larger term project aimed to create a digital wallet for cellphones which would allow users to store everything on the device which has previously been in their physical wallets, like credit cards, identification or tickets. The applicabilities of this project strongly remind of the Apple Wallet, which was introduced in iOS 6 in 2012 and also leverages NFC.

Some years later in 2013 ShAir was developed as by Dubois, Bando, Watanabe, *et al.*, a structured software engineering project written in Java that used WiFi technology on Android devices to share data between them. While Wifi-direct and Bluetooth were also accessible to the developers, they decided to use a combination of WiFi AP mode and WiFi Client mode in a random fashion to create

dynamic networks and discover nearby peers because devices would not allow the former without active user interaction. They tested the app by sharing pictures among 12 devices from several vendors using no fixed existing infrastructure. This project also strongly reminds on Apple propreitary software AirDrop which has been released by Apple in 2011.

Since then support for direct peer-to-peer connections has matured on various mobile operating systems, including iOS and its Multipeer Connectivity Framework which allows nodes to advertise itself, discover nearby advertisers and attempt to connect to detected nearby advertiser. The concept of that model motivated Newport to develop a formal definition and comparison of gossip algorithms. He describes and analyses differences in algorithm parameters and how they influence data spreading in a MANET where the goal is that messages spread to the entire network (2017). The author claims that these algorithms can help to establish peer-to-peer meshes that support infrastructure-free networking and communication. He presents the discontinued FireChat application as an example which offered group chats using smartphone peer-to-peer services such as Bluetooth, WiFi and the Multipeer Connectivity Framework. According to the author this application has been adopted in multiple governmental protest or festivals that were located out of reach of cell towers, but unfortunately did not release a new version since 2018.

1.2 D2D in cellular networks

Although a lot of research exists on D2D communication in cellular networks, most of it is done in a military use case (Gamboa, Ben Mosbah, Garey, *et al.*, 2023), like unmanned aerial vehicles (UVA) or public safety networks (Gamboa, Henderson, Garey, *et al.*, 2024), like vehicle to everything (V2X). Most of this research builds upon 5G New Radio (NR) Sidelink (SL) which has implemented protocol support for (V2X) and Proximity Services (ProSe) for public safety networks which allows user equipment (UE) to directly talk to each other without the interference of a base station (gNB).

Although approaches existed to also introduce D2D communication to the commercial markets back in 2014 by Qualcomm (Qualcomm Technologies, Inc., 2014) and Condoluci, Militano, Orsino, *et al.* back in 2015 proved that LTE-Direct, a predecessor of 5G SL, has some energy and scaling benefits over WiFi-Direct, according to Apple engineers no support for this technology is given on mobile smartphones for third party developers (eskimo1@apple.com, 2023). This is also pointed out by the authors of this critical review of mobile device-to-device communications (Desauw, Luxey-Bitri, Raes, *et al.*, 2023).

1.3 Apple Ecosystem and TU Darmstadt

From 2018 on the OWL project by Secure Mobile Networking Lab (SEEMOO) at TU darmstadt contributed several papers to research on Apple's wireless ecosystem (Stute, Kreitschmann and Hollick, 2018a). Their goal was to assess security and privacy concerns as well as enable cross-platform compatibility with other vendors. They started to investigate AWDL which is heavily used in Apple's Continuity platform. While reverse engineering the 802.11 Wifi based protocol the authors stumbled across various security concerns which they mainly focused on next to Apple's Bluetooth LE usage in following papers until 2021.

On the projects first conference the authors presented the operations of the undocumented AWDL protocol. They used binary and runtime analyses to reconstruct the daemons and frameworks involved in communicating via AWDL and found that each AWDL node announces a sequence of Availability

Windows indicating that it is ready to communicate with other AWDL nodes. In the process they also detected that AWDL connections do not feature any security mechanisms leaving authentication or encryption to the transport and application layers, which the authors claim to be an informed decision by Apple (Stute, Kreitschmann and Hollick, 2018b).

Following the initial findings on missing security considerations, the authors dedicated a separate paper on researching security and privacy issues in the AWDL protocol. The study uncovers multiple vulnerabilities related to both design flaws and implementation bugs. One of the major findings is the possibility of a man-in-the-middle (MitM) attack, which would allow an attacker to stealthily modify files transferred via AirDrop. Additionally, the study identifies denial-of-service (DoS) vulnerabilities that can disrupt communication or force the sudden crash of all nearby devices. The research also reveals privacy weaknesses that allow attackers to track users over extended periods, effectively bypassing MAC address randomization. The authors included a demonstration showing the feasibility of these attacks where the researchers developed proof-of-concept implementations using inexpensive hardware like a 20 dollar micro:bit device. Although following responsible disclosure Apple addressed one of the DoS attack vulnerabilities, the researchers also highlight that several of the identified security and privacy risks require fundamental redesigns of some of Apple's services to be fully mitigated. Overall the study highlights critical security flaws in AWDL design and implementation demonstrating a potential impact on over a billion Apple devices and emphasizing the need for stronger security measures and protocol improvements (Stute, Narain, Mariotto, *et al.*, 2019).

In 2020 Ian Beer a british computer securtiy expert and white hat hacker, inspired by the initial work of TU Darmstadt found another severe security issue in AWDL which could remotely trigger an unauthenticated kernel memory corruption that lead to all iOS devices in radio proximity to reboot. Further he describes how this issue could lead to a system state that lets an attacker run any code on nearby iOS devices and steal all user information. In his demos he forced the former flagship iPhone 11 Pro to activate the AWDL interface which is successfully exploited to steal sensitive information like emails, photos, message or even the keychain (Ian, Beer, 2020).

In 2021 the authors of the OWL project dedicated another paper to the analysis of Apple's offline file sharing service AirDrop. The authors discovered two design flows in the underlying protocol which would allow an attacker to sniff vulnerable hashes of contact information such as the phone number or email address. These hashes are particularly vulnerable to brute force attacks because of the small input number space. For example, phone numbers in Austria with exempt of the mobile operator prefix consist of only seven digits where a hash would be easily cracked within seconds on modern PCs according to the authors. After presenting security issues and their effects the authors propose an optimized private set intersection (PSI) based protocol called PrivateDrop that solves the problem of privacy preserving authentication between nearby offline devices. While preventing potential attackers to steal private user data, users still remain trackable via their UUID in the TLS certificate used during the initial handshake. Finally, the authors also claim that their proposed approach is not limited to the Apple ecosystem and could help Googles similar platform "Nearby" for Android. They also open sourced this implementation as part of their OWL project (Heinrich, Hollick, Schneider, *et al.*, 2021).

While focusing merely on AirDrop in the previous paper the authors of the OWL project dedicated another paper to a broader range of Apple's Continuity services. The authors described a guide to approach a structured analysis of the protocols involved in these services and developed a toolkit to automate parts of this mostly manual process. Based on the created tools the authors analyzed the full protocol stacks involved in various Continuity services like Handoff (HO), Universal Clipboard (UC) and Wi-Fi Password Sharing (PWS). During this process they again found several security issues which could lead to possible denial-of-service (DoS) or machine-in-the-middle (MitM) attacks. To

demonstrate their findings the authors implemented a PoC using an affordable off-the-shelf Wi-Fi card and urge readers to share similar findings with Apple to help make widely used devices more secure (Stute, Heinrich, Lorenz, *et al.*, 2021).

In yet another paper about Apples local broadcasting platform the authors of the OWL project examine worlds biggest offline finding (OF) system. In short lost devices advertise rolling public keys via Bluetooth Low-Energy (BLE) that are captured by nearby "finder devices" and sent to an Apple server with the corresponding location of the finder device. The owner of the lost device can the query the Apple server for entries sent by these finder devices to get an estimated location of his lost device. While the authors claim that this design mostly achieves Apple's specific security goals they also share two distinct design and implementation faults. These would allow Apple to correlate different users location if their locations are reported by the same finder device to let Apple form social user graphs. Moreover a malicious macOS application could retrieve and decrypt location reports of the last week as teh rolling advertisement keys are cached and stored on the filesystem as clear text (Heinrich, Stute, Kornhuber, *et al.*, 2021).

1.4 Summary

Although considerations about ad-hoc networks were dealt with very early in the history of mobile computing, it has only been recently that widespread features using local radio broadcasting were adopted. With great power comes great responsibility which Apple tends to have underestimated with respect to the great work and great findings of the OWL project by SEMOO at TU Darmstadt. The group noticed the need for research on mobile local ad hoc networks since these have vastly improved and found several new applications over the last few years especially in the Apple ecosystem, but focused mainly on demistifying the underlying protocols and analysing those with regard to security concerns.

2 | Background

This section tries to describe and familiarize with concepts of networking topologies for mobile devices. From an abstract perspective networking can be categorized into infrastructure and ad-hoc networks, one relying on mediators while the other works without intermediary infrastructure letting the participants itself form the network.

2.1 Infrastructure Networks

The national institute of standards and technology (NIST) defines infrastructure networks as “a wireless network that requires the use of an infrastructure device, such as an access point or a base station, to facilitate communication between client devices” (NIST, n.d.). Using underlying infrastructures that span over wide areas let users communicate to seemingly anywhere. This is achieved due to a widespread net of connected computers called the internet, which is defined by the internet engineering task force (IETF) as “the single, interconnected, worldwide system of commercial, governmental, educational, and other computer networks that share (a) the protocol suite specified by the IAB (RFC 2026) and (b) the name and address spaces managed by the ICANN” (Shirey, n.d.). While the user is connected he can communicate to nearly anywhere but when out of reach of the next entry point the user can not even transfer data nearby device, no matter how close these might be.

2.2 Ad-hoc Networks

The NIST defines ad-hoc networks as “a wireless network that allows easy connection establishment between wireless client devices in the same physical area without the use of an infrastructure device, such as an access point or a base station” (NIST, n.d.). Even when the next entry point to the internet is out of reach nearby devices can communicate with each other but are limited to the nodes that form this new separate network.

2.3 Satellite phones

While satellite phones seemingly solve the mentioned problems they are not widely spread in the day-to-day use and mostly used for emergency services or roadside assistance in modern iPhones (Apple Inc., 2025). Another problem that is increasingly present are space debris which have more than doubled since 2007 and is yet to increase with more and more space missions emerging. These junks of different parts of satellites or rockets can potentially destroy more satellites which again leads to more space debris or outages in GPS or satellite phoning services (European Space Agency, n.d.).

2.3.1 Starlink Direct to Cell

While Starlink operates on similar ideas they offer multiple advantages over normal geostationary satellites. While geostationary satellites orbit at 35.786 kilometers starlink satellites orbit much closer at about 550 km from the Earth reducing latency and decreasing space traffic in the geostationary field. Starlink also claims that their satellites include a collision avoidance system which notices potential collisions and actively dodges the other object (Starlink, n.d.).

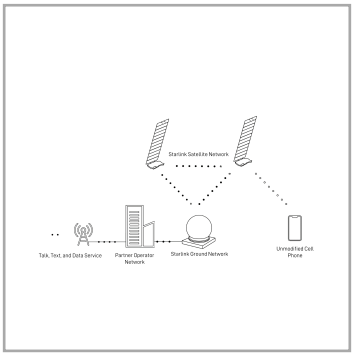

Figure 1: Abstract structure of Starlink's network.

2.4 Specific Ad-hoc technologies

While and solve the issue of dead spots, they also rely on infrastructure. The following is an incomprehensive list of ad hoc technologies.

2.4.1 WiFi

WiFi is a trademark for IEEE wireless communication standard 802.11 based technologies which already exists for over two decades. The IEEE 802.11 standard defines the protocols that are used to establish a connection with current WiFi wireless nodes, including routers or access points whereas the correlating WiFi versions is just used for marketing purposes and matches an underlying 802.11 specification (Wi-Fi Alliance, 2023; Cisco Systems, Inc., n.d.).

Generational name	Technology supported
WiFi 7	802.11be
WiFi 6	802.11ax
WiFi 5	802.11ac
WiFi 4	802.11n

The WiFi Direct trademark enables WiFi devices to connect directly without underlying infrastructure. However this specification has not been widely adopted because of high energy consumption and lack of performance where establishing a connection could take fro four to ten seconds (Camps-Mur, Garcia-Saavedra and Serrano, 2013). WiFi Direct is not available in iPhones (Quinn "The Eskimo!", 2015).

2.4.2 Bluetooth

Bluetooth a short range wireless technology enables connection between two nearby devices without relying on supporting infrastructure very similar to WiFi Direct. The protocol operates on 2.4 GHz and is features two separate standards today, Bluetooth Classic and Bluetooth Low Energy which is optimized for low energy consumption. Today Bluetooth is mostly used to connect computers to external peripherals like mice, keyboards or headphones. Using Bluetooth for data transfer is not preferred since its data rate is limited to 2 Mbps (Intel Corporation, 2022; CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY, 2021).

2.4.3 LoRaWan

LoRaWan specification is a Low Power, Wide Area networking specification created to connect IoT devices to the internet. The specification features key requirements for the IoT use such as bi-directional communication, end-to-end security or location services. It usually operates in unlicensed frequency bands and is capable of communicating up to 15 km in rural areas. While this key features would also perfectly suit iOS peer-to-peer communication no support for this technology is given on iPhones (LoRa Alliance, n.d.).

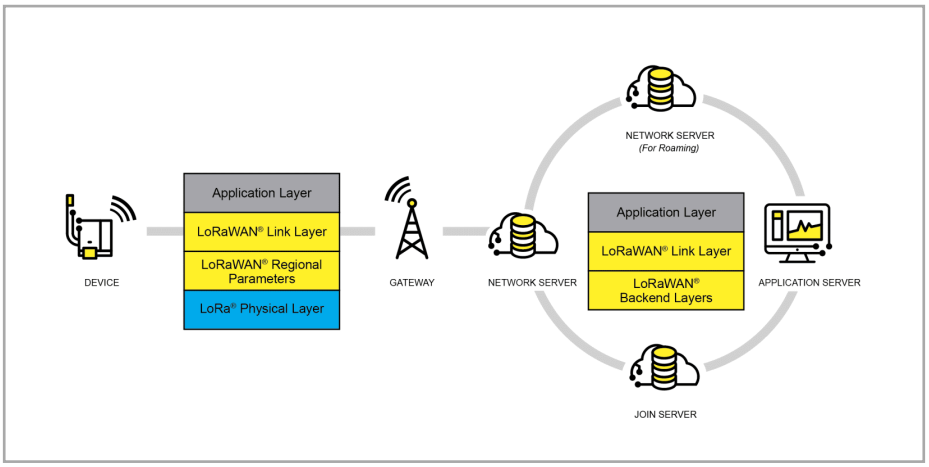

Figure 2: Abstract structure of LoRaWan network.

2.4.4 5G Sidelink

5G Sidelink (SL) the successor of LTE-Direct is capable of connecting user equipments directly without an intermediate base station (Vijitha, Weerackody, Kent, Benson and Sumit, Roy, 2023). This is generally designed for public safety or military operations used for unmanned vehicles (Barnes, Maheu and Kuzin, 2023) although approaches existed to introduce it into commercial markets (Qualcomm Technologies, Inc., 2014). Again iOS peer-to-peer communication would highly benefit from such technolgies but unfortunately no developer support for this technology is given (Apple Inc., 2024).

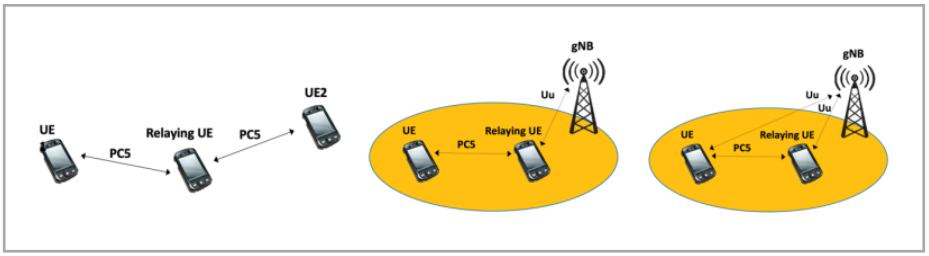

Figure 3: Abstract structure of 5G SL network.

2.4.5 NFC

Near Field Communication is a communication technology which operates at a base frequency of 13.56 Mhz. It can transfer data with a typical range of 2cm and data rates up to 1.7 Mbps. The technology is also used to connect to non powered peripherals such as bank cards (NFC Forum, n.d.). Apple makes this technology also accessible to iOS and iPadOS developers but explicitely states that it is not supported in other Apple platforms (Apple Inc., n.d.).

2.4.6 UWB

Apple allows developers to access their Ultra Wideband (UWB) interface on iPhones and Apple Watches through the Nearby Interaction framework (Apple Inc., n.d.) which is built to locate nearby devices also using the distance and direction. UWB in general is a radio technology focused on precise ranging and locating using a low energy density over a large radio spectrum (Android Developers, 2025). In Apples article about the advanced ranging capabilities of second generation UWB chips which are included in iPhone 15 and above they use a maximum distance of 50 meters (Apple Inc., n.d.).

2.5 iOS

The following part tries to familiarize with technologies used in the testing process of this thesis.

2.5.1 Bonjour

Bonjour is a former proprietary zero-configuration network protocol suite over IP that Apple has submitted to the IETF. The proposed zero-configuration solutions covers IP addressing, name-to-address translation on local networks using mulitcast DNS (mDNS) and service discovery. Using Bonjour on Apple platforms is done via appropriate frameworks leaving the responding to mDNS queries to the mDNSResponder daemon (Apple Inc., 2013).

2.5.2 IPS

The Internet Protocol Suite (IPS) is a set of networking protocols specified by the IETF also often referred to as “TCP/IP” protocol stack. It is split into five protocol layers – Application, Transport, Internet, Network Interface and Network Hardware –, however for this thesis only the first two are relevant and listed below (Shirey, n.d.).

2.5.2.1 Application Layer

The Application Layer covers the data the application program run by the user wants to transmit and only interacts with the next lower Transport Layer. Based on the applications needs data can be transferred as a continuous stream or package based where the Transport Layer handles interaction with the next Internet Layer.

2.5.2.2 Transport Layer

The Transport Layer “divides application data into packets, adds a destination address to each, and communicates them end-to-end – from one application program to another – optionally regulating the flow and ensuring reliable (error-free and sequenced) delivery.”

2.5.2.2.1 Transport Control Protocol

TCP is an internet standard, Transport layer protocol that reliably transmit data in the same order it was sent utilizing congestion and error controlling. It can be directly accessed on Apple platforms using the C based BSDSockets or the Networking Framework (Apple Inc., 2023).

2.5.2.2.1.1 Nagles Algorithm

Due to the 20 byte TCP header there has been a relatively high overhead when sending small packages which in worst case could lead to congestion collapse considering the error prevention of the TCP protocol. This algorithm inhibits the sending of new TCP segments as long as no previously transmitted data stays unacknowledged. This algorithm is enabled by default on iOS systems (Apple Inc., n.d.) and while testing the prototype has lead to highly reduced IP package number sent compared to the data slices sent from the Application Layer (Nagle, 1984).

2.5.2.2.2 User Datagram Protocol

UDP is a Transport Layer protocol that implements the "fire-and-forget" concept. Packages are sent whenever data is received from the Application Layer without guarantee that they will be delivered or that they will be received in the same order they had been sent.

2.5.2.2.3 QUIC

QUIC is a Transport Layer protocol that builds upon UDP and is oriented to replace TCP based applications since it also features congestion and error control features. Compared to UDP and TCP QUIC has built in TLS 1.3 support and does not allow non encrypted connections.

2.5.3 AWDL

Apple Wireless Direct Link was developed by Apple due to concerns regarding WiFi Alliance's WiFi Direct specification and eventually got adopted by the WiFi Alliance as the basis for Neighbor Awareness Networking (NAN) (Cheshire, 2018). It is based on IEEE 802.11 ad hoc protocol and built to let mobile devices communicate directly with each other without utilizing an intermediary access point. It is heavily used in Apple's Continuity platform (Stute, Heinrich, Lorenz, *et al.*, 2021).

2.6 Summary

3 | Concept

The following introduces the abstract design of how direct P2P communication between iOS devices is tested and measured for evaluation in this thesis. The measurement setup should try to systematically quantify how the performance of P2P iOS connection is and how it changes under different surroundings. Different approaches to solve this problem do exist, which are briefly evaluated and compared among each other.

3.1 Approaches

3.1.1 Continuity Black Box Testing

Using Apple's Continuity features to send and receive data on different iOS devices could be tested and analysed. In the simplest form this would involve selecting a particular file with a particular size and measuring the time it takes to transport this file from one device to another. The data transfer speed could be approximated using the file size and the time it took to transfer the file. Another approach to this black box testing could involve using a network sniffer to monitor connection establishment like local mDNS and security handshakes including recording and analysing the transmission process like congestion control and packet loss recovery. This could further be applied on different abstraction layers like measuring the physical radio frequency energy used or how many IP packages needed to be sent.

3.1.2 iOS Application

iOS provides several application programming interfaces (API) that allow a third party developer to access various underlying technologies to establish P2P connections. The software could directly record how much data is sent and received mitigating overhead of measurement logic. Using the frameworks provided by Apple is also an interface available to any third party developer and can therefore be implemented in any iOS application without the need to bypass any restrictions.

3.1.3 Jailbreaking

Jailbreaking is a term used to describe the bypassing of the security mechanism in iOS. This allows the user to install arbitrary third party software and gain full access to the operating system. This would allow to also access interfaces like the cellular antenna that is restricted and not accessible to a third party developer or turning off services that would interfere with testing (AO Kaspersky Lab, n.d.). This however violates Apple's iOS Software License Agreement and testing could potentially disturb restricted frequency bands that are licensed (Apple Inc., n.d.). Additionally considering the current use cases of iOS devices and restrictions of the operating system it seems unlikely that developers other than Apple could have similar interfaces in near future.

3.2 Experiment Design

After evaluating the aforementioned concepts the decision was taken to build an iOS Application establishing and intercepting the P2P connection to measure connection metrics. It is the most practicable considering the use for a wide mass, because staying in the boundaries imposed by Apple and using only first party frameworks makes developing and distributing in the App Store easier. The application needs to be installed on two nearby devices to establish a connection and transfer data. Furthermore since iPhones are typically used under various circumstances and surroundings testing should also cover representable scenarios for common places visited by iPhone users.

3.2.1 Prototype

The prototype should be installable on arbitrary iOS devices and should serve as both client and server. The client must be capable of discovering nearby peers and sending a connection request after user instruction. The server must be capable of advertising a service that clients can find and handling incoming connection requests. Both must be able to display the metrics that the applications measured to the user and should support a method to abort ongoing connections to start new advertisers/ discoverers.

3.2.2 Testing

Capturing the data of interest is done by the prototype itself. However general conditions for environmental and data variations have to be defined. Testing must be done in different surroundings distinguishing each other in the density of obstacles, radio frequency emissions or both to cover most real life scenarios. Moreover data size must vary to represent use cases for small payloads like simple message transfer to bigger payloads like sharing files. Another factor to consider is the distance between the two testing devices. All these three external factors must be tested in each possible variation forming a three dimensional matrix.

4 | Results and Evaluation

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magnam aliquam quaerat voluptatem. Ut enim aeque doleamus animo, cum corpore dolemus, fieri.

Describe (proof) how your implementation really solved the stated problem. I.e. accept or reject your hypotheses. Provide a range of input data sets. Run experiments and gather the output (of tools) to meter your prototype. For the analysis, collect the measurement-data, process (e.g. filter) data and interpret the data. Include an interpretation of the work. What do the results mean to you? State current limitations of your solution. Give (personal) interpretation where suitable. Your own opinion is relevant, but must be marked clearly as such.

4.1 Setup Experiment

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magnam aliquam quaerat voluptatem. Ut enim aeque doleamus animo, cum corpore dolemus, fieri tamen permagna accessio potest, si.

For example: During the setup the was configured for the parallel version using the value `+UseParallelGC` for the command line argument `-XX` (`java -XX:+UseParallelGC`).

Hints on dynamically reading in external data for tables in Typst:

Using the custom macro `fhjtable` it is possible to include data dynamically for table generation. The data has to be specified in as shown below:

Name	Profession	Experience (in years)
Max	Student	3
Mia	UX-Designer	7
Helga	Programmer	9

Table 2: Professional experience of the test users with databases.

Find in Table 2 the years a user has worked with different relational or nosql databases in a professional context.

4.2 Measurement

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magnam aliquam quaerat voluptatem. Ut enim aeque doleamus animo, cum corpore dolemus, fieri tamen permagna accessio potest, si.

Hints on using tables in Typst:

Somewhere in the normal text of the thesis the interpretation of data and information shown in a table must be discussed. Explain to the readers which numbers are important. Possibly, highlight unexpected or special data points.

	Min	**Max**	∅	σ
Network roundtrip time	34.6s	42.5s	38.1s	2.3s
Time for single request	2.4s	13.5s	**7.1s**	4.3s

Table 3: The numbers in the table above show the minimum, maximum, average ∅ , and standard deviation σ of the 273 measured network times in seconds.

For example: … Table 3 shows some calculated results on the roundtrip and request times measured in the experiment. The average, the minimum, the maximum and the standard deviations hint to a dramatic increase (> 13%) in performance in comparison to the old solution of 2003.

4.3 Interpretation of the Data

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magnam aliquam quaerat voluptatem. Ut enim aeque doleamus animo, cum corpore dolemus, fieri tamen permagna accessio potest, si.

For example: The customisation of the seem to have following positive and negative consequences….

Hints on dynamic calculation in Typst:

We might calculate, e.g. `#calc.max(...)`, within our document, such as max of three and seven times two is: 14.

Hints on using logic in Typst:

For example, we might use **for loop** to arrange a few images in a grid box, as shown below.

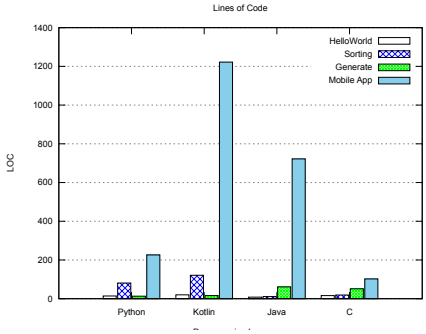

Figure 4: Compared source code by metric 1.

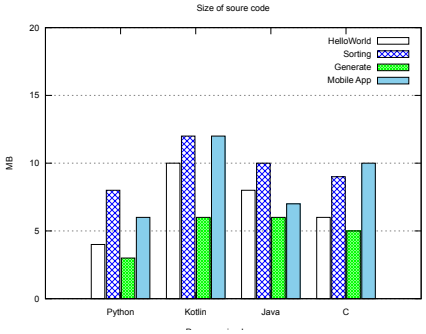

Figure 5: Compared source code by metric 2.

Hints on Charts:

Note: the charts (**vector**! images) shown have been created from raw data using the tool **gnuplot** on the command line. With `gnuplot` you can create charts by use of a textual command language. This is great for automation and it is also great for managing the source code in `git`.

5 | Conclusion and Outlook

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magnam aliquam quaerat voluptatem. Ut enim aeque doleamus animo, cum corpore dolemus, fieri tamen permagna accessio potest, si aliquod aeternum et infinitum impendere malum nobis opinemur. Quod idem licet transferre in voluptatem, ut postea variari voluptas distinguique possit.

Sum up the results achieved and give an outlook by suggesting further research by explaining how others could built on your results.

Glossary

AWDL **– Apple Wireless Direct Link** 2, 3, 4

P2P **– Peer to Peer** i, ii, 11, 12

Bibliography

Android Developers (2025) *Ultra-wideband (UWB) communication.* [Online]. 10 February 2025. https://developer.android.com/develop/connectivity/uwb [Accessed: 29 April 2025].

AO Kaspersky Lab (n.d.) *Jailbreaking – Definition und Erläuterung.* [Online]. https://www.kaspersky.de/resource-center/definitions/what-is-jailbreaking [Accessed: 29 April 2025].

Apple Inc. (2024) *Apple device support for private 5G and LTE networks.* [Online]. 25 September 2024. https://support.apple.com/en-gb/guide/deployment/depac6747317/web [Accessed: 29 April 2025].

Apple Inc. (2013) *Bonjour Concepts.* [Online]. 23 April 2013. https://developer.apple.com/library/archive/documentation/Cocoa/Conceptual/NetServices/Articles/about.html#//apple_ref/doc/uid/TP40002458-TPXREF108 [Accessed: 29 April 2025].

Apple Inc. (2025) *Connect to a satellite with your iPhone.* [Online]. 7 April 2025. https://support.apple.com/en-us/105097 [Accessed: 29 April 2025].

Apple Inc. (n.d.) *Extending advanced direction finding and ranging.* [Online]. https://developer.apple.com/documentation/nearbyinteraction/extending-advanced-direction-finding-and-ranging [Accessed: 29 April 2025c].

Apple Inc. (n.d.) *Nearby Interaction with UWB.* [Online]. https://developer.apple.com/nearby-interaction/ [Accessed: 29 April 2025b].

Apple Inc. (n.d.) *Network Framework noDelay.* [Online]. https://developer.apple.com/documentation/network/nwprotocoltcp/options/nodelay [Accessed: 29 April 2025d].

Apple Inc. (n.d.) *NFC.* [Online]. https://developer.apple.com/design/human-interface-guidelines/nfc [Accessed: 29 April 2025a].

Apple Inc. (2023) *TN3151: Choosing the right networking API.* [Online]. 19 September 2023. https://developer.apple.com/documentation/technotes/tn3151-choosing-the-right-networking-api [Accessed: 29 April 2025].

Apple Inc. (n.d.) *Unauthorized modification of iOS.* [Online]. https://support.apple.com/en-gb/guide/iphone/iph9385bb26a/ios [Accessed: 29 April 2025e].

Balan, R. K., Ramasubbu, N., Prakobphol, K., Christin, N., et al. (2009) mFerio: the design and evaluation of a peer-to-peer mobile payment system. In: *Proceedings of the 7th international conference on Mobile systems, applications, and services.* [Online]. 22 June 2009 Kraków Poland, ACM. pp. 291–304. DOI:10.1145/1555816.1555846 [Accessed: 7 December 2024].

Barnes, L., Maheu, W. & Kuzin, J. (2023) *How 5G sidelink benefits public safety and critical communications*. [Online]. 4 April 2023. https://www.qualcomm.com/news/onq/2023/04/how-5g-sidelink-benefits-public-safety-and-critical-communications [Accessed: 29 April 2025].

Camps-Mur, D., Garcia-Saavedra, A. & Serrano, P. (2013) Device-to-device communications with Wi-Fi Direct: overview and experimentation. *IEEE Wireless Communications*. [Online] 20 (3), 96–104. DOI:10.1109/MWC.2013.6549288 [Accessed: 29 April 2025].

Cheshire, S. D. (2018) *Proximity Wi-Fi*. [Online]. https://patents.google.com/patent/US20180083858A1/en [Accessed: 29 April 2025].

Cisco Systems, Inc. (n.d.) *What is WiFi?*. [Online]. https://www.cisco.com/c/en/us/products/wireless/what-is-wifi.html [Accessed: 29 April 2025].

Condoluci, M., Militano, L., Orsino, A., Alonso-Zarate, J., et al. (2015) LTE-direct vs. WiFi-direct for machine-type communications over LTE-A systems. In: *2015 IEEE 26th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*. [Online]. August 2015 Hong Kong, China, IEEE. pp. 2298–2302. DOI:10.1109/PIMRC.2015.7343681 [Accessed: 7 December 2024].

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY (2021) *Understanding Bluetooth Technology*. [Online]. 1 February 2021. https://www.cisa.gov/news-events/news/understanding-bluetooth-technology [Accessed: 29 April 2025].

Desauw, L., Luxey-Bitri, A., Raes, R., Rouvoy, R., et al. (2023) *A critical review of mobile device-to-device communication*. [Online]. https://inria.hal.science/hal-04198528.

Dubois, D. J., Bando, Y., Watanabe, K. & Holtzman, H. (2013) ShAir: extensible middleware for mobile peer-to-peer resource sharing. In: *Proceedings of the 2013 9th Joint Meeting on Foundations of Software Engineering*. [Online]. 18 August 2013 Saint Petersburg Russia, ACM. pp. 687–690. DOI:10.1145/2491411.2494573 [Accessed: 7 December 2024].

eskimo1@apple.com (2023) *Use iphone antenna without sim card - Answer*. [Online]. August 2023. https://developer.apple.com/forums/thread/97688?answerId=762404022#762404022 [Accessed: 26 March 2025].

European Space Agency (n.d.) *About space debris*. [Online]. https://www.esa.int/Space_Safety/Space_Debris/About_space_debris [Accessed: 29 April 2025].

Gamboa, S., Henderson, T. R., Garey, W., Liu, C., et al. (2024) Towards System Level Simulations of Public Safety Applications over 5G NR Sidelink. In: *2024 IEEE World Forum on Public Safety Technology (WFPST)*. [Online]. 14 May 2024 Herndon, VA, USA, IEEE. pp. 1–6. DOI:10.1109/WFPST58552.2024.00043 [Accessed: 26 March 2025].

Gamboa, S., Ben Mosbah, A., Garey, W., Liu, C., et al. (2023) System-Level Evaluation of 5G NR UE-Based Relays. In: *MILCOM 2023 - 2023 IEEE Military Communications Conference (MILCOM)*. [Online]. 30 October 2023 Boston, MA, USA, IEEE. pp. 807–814. DOI:10.1109/MILCOM58377.2023.10356291 [Accessed: 26 March 2025].

Heinrich, A., Hollick, M., Schneider, T., Stute, M., et al. (2021) PrivateDrop: Practical Privacy-Preserving Authentication for Apple AirDrop. In: *30th USENIX Security Symposium*

(USENIX Security 21). [Online]. August 2021 USENIX Association. pp. 3577–3594. https://www.usenix.org/conference/usenixsecurity21/presentation/heinrich.

Heinrich, A., Stute, M., Kornhuber, T. & Hollick, M. (2021) Who Can \textit{Find My} Devices? Security and Privacy of Apple's Crowd-Sourced Bluetooth Location Tracking System. *Proceedings on Privacy Enhancing Technologies*. [Online] 2021 (3), 227–245. DOI:10.2478/popets-2021-0045 [Accessed: 29 April 2025].

Ian, Beer (2020) *An iOS zero-click radio proximity exploit odyssey*. [Online]. 12 January 2020. https://googleprojectzero.blogspot.com/2020/12/an-ios-zero-click-radio-proximity.html [Accessed: 26 March 2025].

Intel Corporation (2022) *What Is Bluetooth® Technology?*. [Online]. 2022. https://www.intel.com/content/www/us/en/products/docs/wireless/what-is-bluetooth.html [Accessed: 29 April 2025].

Kortuem, G., Schneider, J., Preuitt, D., Thompson, T., et al. (2002) When peer-to-peer comes face-to-face: collaborative peer-to-peer computing in mobile ad-hoc networks. In: *Proceedings First International Conference on Peer-to-Peer Computing*. [Online]. 2002 Linkoping, Sweden, IEEE Comput. Soc. pp. 75–91. DOI:10.1109/P2P.2001.990429 [Accessed: 7 December 2024].

LoRa Alliance (n.d.) *What is LoRaWAN?*. [Online]. https://lora-alliance.org/about-lorawan/ [Accessed: 29 April 2025].

Nagle, J. (1984) *Congestion Control in IP/TCP Internetworks*. [Online]. (RFC896) p.RFC896. DOI:10.17487/rfc0896 [Accessed: 29 April 2025].

Newport, C. (2017) Gossip in a Smartphone Peer-to-Peer Network. In: *Proceedings of the ACM Symposium on Principles of Distributed Computing*. [Online]. 25 July 2017 Washington DC USA, ACM. pp. 43–52. DOI:10.1145/3087801.3087813 [Accessed: 7 December 2024].

NFC Forum (n.d.) *NFC Technical Overview*. [Online]. https://nfc-forum.org/learn/nfc-technology/ [Accessed: 29 April 2025].

NIST (n.d.) *Adhoc Network*. [Online]. https://csrc.nist.gov/glossary/term/ad_hoc_network [Accessed: 23 April 2025b].

NIST (n.d.) *Infrastructure Network*. [Online]. https://csrc.nist.rip/glossary/term/infrastructure_network [Accessed: 23 April 2025a].

Qualcomm Technologies, Inc. (2014) *LTE Direct Always-on Device-to- Device Proximal Discovery*. [Online]. 2014. https://www.qualcomm.com/content/dam/qcomm-martech/dm-assets/documents/lte_direct_always-on_device-to-device_proximal_discovery.pdf [Accessed: 26 March 2025].

Quinn "The Eskimo!" (2015) *iOS and Wi-Fi Direct*. [Online]. July 2015. https://developer.apple.com/forums/thread/12885 [Accessed: 29 April 2025].

Shirey (n.d.) *Internet Security Glossary, Version 2*. [Online]. https://www.rfc-editor.org/rfc/rfc4949.txt [Accessed: 26 April 2025].

Starlink (n.d.) *Satellite Technology*. [Online]. https://www.starlink.com/gb/technology [Accessed: 29 April 2025].

Statista Research Department (2024) *Number of smartphone users worldwide from 2014 to 2029 (in millions)*. [Online]. December 2024. https://www.statista.com/forecasts/1143723/smartphone-users-in-the-world [Accessed: 8 December 2024].

Stute, M., Heinrich, A., Lorenz, J. & Hollick, M. (2021) Disrupting Continuity of Apple's Wireless Ecosystem Security: New Tracking, DoS, and MitM Attacks on iOS and macOS Through Bluetooth Low Energy, AWDL, and Wi-Fi. In: *30th USENIX Security Symposium (USENIX Security 21)*. [Online]. August 2021 USENIX Association. pp. 3917–3934. https://www.usenix.org/conference/usenixsecurity21/presentation/stute.

Stute, M., Kreitschmann, D. & Hollick, M. (2018b) One Billion Apples' Secret Sauce: Recipe for the \textit{Apple Wireless Direct Link} Ad hoc Protocol. In: *Proceedings of the 24th Annual International Conference on Mobile Computing and Networking*. [Online]. 15 October 2018 New Delhi India, ACM. pp. 529–543. DOI:10.1145/3241539.3241566 [Accessed: 17 February 2025].

Stute, M., Kreitschmann, D. & Hollick, M. (2018a) *The Open Wireless Link Project*. [Online]. 2018. https://owlink.org/.

Stute, M., Narain, S., Mariotto, A., Heinrich, A., et al. (2019) A Billion Open Interfaces for Eve and Mallory: MitM, DoS, and Tracking Attacks on iOS and macOS Through Apple Wireless Direct Link. In: *28th USENIX Security Symposium (USENIX Security 19)*. [Online]. August 2019 Santa Clara, CA, USENIX Association. pp. 37–54. https://www.usenix.org/conference/usenixsecurity19/presentation/stute.

Vijitha, Weerackody, Kent, Benson & Sumit, Roy (2023) *Who Needs Basestations When We Have Sidelinks?*. [Online]. 24 February 2023. https://www.comsoc.org/publications/ctn/who-needs-basestations-when-we-have-sidelinks [Accessed: 26 March 2025].

Wi-Fi Alliance (2023) *Discover WiFi*. [Online]. 2023. https://www.wi-fi.org/discover-wi-fi [Accessed: 29 April 2025].