FERDINAND PORSCHE
FERN FH

5G Mobilfunkstandard und deren Auswirkung auf österreichische WLAN-Provider

Masterarbeit

Eingereicht von: **Ing. Marijan Grabovac, BA**

Matrikelnummer: 51807400

im Fachhochschul-Masterstudiengang Wirtschaftsinformatik

der Ferdinand Porsche FernFH GmbH

zur Erlangung des akademischen Grades

Master of Arts in Business

Betreuung und Beurteilung: Christoph Jungbauer, BA MA MA

Zweitgutachten: Dipl.-Ing.in Eszter Geresics-Földi, BSc MSc

Wien, April 2022

Ehrenwörtliche Erklärung

Ich versichere hiermit,

1. dass ich die vorliegende Masterarbeit selbständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt habe. Alle Inhalte, die direkt oder indirekt aus fremden Quellen entnommen sind, sind durch entsprechende Quellenangaben gekennzeichnet.
2. dass ich diese Masterarbeit bisher weder im Inland noch im Ausland in irgendeiner Form als Prüfungsarbeit zur Beurteilung vorgelegt oder veröffentlicht habe.
3. dass die vorliegende Fassung der Arbeit mit der eingereichten elektronischen Version in allen Teilen übereinstimmt.

Wien, April 2022

Unterschrift

Kurzzusammenfassung: 5G Mobilfunkstandard und deren Auswirkung auf österreichische WLAN-Provider

Neue Drahtlostechnologien und deren technologischen Entwicklungen, befürworten eine stetige Verbesserungen für die Nutzenden selbst. Im neuen WLAN-Standard Wi-Fi 6 und im neuen Mobilfunkstandard 5G, werden beispielsweise höhere Datenraten, höhere Geschwindigkeiten, verbesserte Latenzzeiten, uvm. erzielt. Für diese beiden Drahtlostechnologien existieren eine Vielzahl an unterschiedlichen Anwendungsgebieten. Unter anderem zählen öffentliche WLAN-Hotspots in Restaurants oder Einkaufszentren dazu. Bei der Nutzung eines österreichischen WLAN-Hotspots herrschen Gefahren und Risiken für die Nutzer*Innen. Hacker*Innen können die Datenkommunikation abfangen und mitlesen. Abhilfen werden durch neue Protokolle und neue Verschlüsselungen geschaffen. Ob ein österreichsicher WLAN-Hotspot genutzt wird, hängt von verschiedenen Faktoren ab. Daraus resultiert die wissenschaftliche Forschungsfrage: Welche Bedingungen müssen erfüllt sein, damit Nutzer*Innen österreichische WLAN-Provider gegenüber dem Mobilfunkstandard 5G vorziehen? Damit diese Frage beantwortet werden kann, wurde eine Mixed-Methods Forschung angewandt. In der qualitativen Forschungsmethode wurden Expert*Innen Interviews und in der quantitativen Forschungsmethode wurde ein Online-Fragebogen durchgeführt. Anschließend erfolgte eine Auswertung der beiden Forschungsmethoden, welche sich ergänzten. Dabei stellte sich heraus, dass österreichische WLAN-Hotspots aufgrund des angebotenen kostenlosen Service und um das eigene Datenvolumen zu sparen genutzt werden. In Bezug auf den Sicherheitsaspekt und den aufgestellten Hypothesen, konnte kein Unterschied bei den Nutzer*Innen festgestellt werden.

Schlagwörter:

WLAN, Wi-Fi6, 5G, Mobilfunk, Sicherheit, Verschlüsselung, Mixed-Methods

Abstract: 5G mobile radio standard and its impact on Austrian WLAN providers

New wireless technologies and their technological development approve for the users a continuous improvement. Higher data rates, higher speeds, improved latency, etc., are achieved by the newest WLAN standard WiFi-6 and in the fifth-generation mobile network. For these two wireless technologies exist a lot of different application areas. This includes public WLAN hotspots in restaurants or shopping centres and other locations. If users use an Austrian WLAN hotspot, so there exist risks and dangers for them. Hackers can intercept and read the data communication. Affirmative reliefs are created by new protocols and new encryptions. If is an Austrian WLAN hotspot used, it depends on various factors. The scientific research question is: What conditions must be fulfilled, to prefer Austrian WLAN hotspots to the 5G mobile communications standard for the users? A mixed-methods research, which include a quantitative and quality research method answered the question. Experts were interviewed and an online questionnaire was hold. After that an evaluation of the two research methods was carried out. Austrian WLAN hotpots are used because of the free service and to save own data volume. Moreover, no difference was found between the users in relation of security.

Keywords:

WLAN, Wi-Fi6, 5G, cellular, security, encryption, mixed-methods

Vorwort

An erster Stelle möchte ich mich recht herzlich an meinem Betreuer Christoph Jungbauer, BA MA MA bedanken, der mich von Beginn an und bis zum Schluss meines Masterlehrgangs mit seiner Expertise überzeugt hat, ebenso während meiner Masterarbeit mit seinem Fachwissen tatkräftig unterstützt und exzellent betreut hat.

Danke auch an alle Expertinnen und Experten, die an meiner Befragung teilgenommen haben und die mich mit ihrem Fachwissen unterstützt haben, denn ohne ihrer Informationsbereitschaft und wertvollen Beiträge wäre es nicht möglich gewesen, die Faktoren für die Akzeptanz zu ermitteln. Ebenso bedanke ich mich auch an alle Personen, welche bei der Onlineumfrage mitgewirkt haben.

Mein besonderer Dank gilt meinen Eltern, meinen Schwestern, meinen Schwiegereltern und meinen restlichen Familienangehörigen. Ein weiterer Motivator war mein Schwager, der leider zu früh von uns ging. Einen besonderen Dank widme ich jedoch meiner Ehegattin und meinen drei kleinen Kindern. Sie war mein Fels in der Brandung und hatte immer ein offenes Ohr für mich. Die letzten Jahre waren sehr schwer, es gab einige Hochs und Tiefs, doch gemeinsam haben wir jede Schwierigkeit gemeistert und jetzt stehen wir gemeinsam am Berggipfel. Ich danke dir, danke vom ganzen Herzen!

Einen weiteren Dank möchte ich auch meinem Freund und Studienkollegen Sascha aussprechen. Am Beginn des Studiums haben wir uns kennengelernt und im Laufe der Jahre schafften wir es stets uns gegenseitig aufzumuntern und zu motivieren. Die gemeinsamen Studienjahre waren eine besondere und eine unvergessliche Zeit.

Marijan Grabovac
Himberg, 25.04.2022

Inhaltsverzeichnis

1 Einleitung

Heutzutage existieren verschiedene technologische Zugänge um miteinander über das Internet auf der ganzen Welt zu kommunizieren. Drahtlostechnologien sind zurzeit kaum wegzudenken. Es gibt mittlerweile ca. 6,3 Milliarden Smartphone-Nutzer*Innen weltweit, dies entspricht 80,76% der Weltbevölkerung (Statista 2021). Die Drahtlosnetztechnologien WLAN (Wireless Local Area Network) oder Mobilfunk fungieren als Schnittstelle zwischen dem Smartphone und dem Internet.

1.1 Problemstellung

Im Zeitalter der Digitalisierung schreitet die Entwicklung neuer Technologien immer schneller voran. Technologien welche heute als Stand der Technik gelten, sind in ein paar Jahren wieder veraltet und werden durch neuere Technologien ersetzt. Das betrifft auch die Drahtlostechnologien WLAN und Mobilfunk. Wi-Fi6 (IEEE 802.1 ax) ist der neueste WLAN-Standard aktuell am Markt, welcher nicht nur durch seine höhere Datenrate hervorsticht, sondern auch aufgrund der effizienten Nutzung des Frequenzspektrums (QAM - Quadraturamplitudenmodulation) eine Verbesserung für die Endverbrauchenden darstellt. Die wichtigsten Erneuerungen sind OFDMA (Orthogonal Frequency Division Multiple Access) und MU MIMO (Multi-User Multiple Input/Multiple Output). (Khorov u. a., 2019)

Um die Sicherheit von Wi-Fi6 zu erhöhen, wurde die neue Verschlüsselungsmethode WPA3 (Wi-Fi Protected Access) seitens Wi-Fi Alliance freigegeben. Wi-Fi Alliance ist ein Verband der WLAN-Geräteherstellenden, welcher die Zertifizierung nach strengen Testmethoden und Auflagen durchführt. Nach einem positiven Zertifizierungsprozess, dürfen die WLAN-Router das Wi-Fi Logo am Gerät auftragen (Wi-Fi Alliance, 2020). WPA3 bietet einen verbesserten Schutz im Vergleich zu WPA2 an, da der Pre Shared Key (PSK) durch Simultaneous Authentication of Equals (SAE) abgelöst wird. SAE ist eine Variante des Dragonfly-Handshakes, bei dem die Angriffsversuche das Auslesen der Passwörter verhindern. (D. Harkins, Ed. & Aruba Networks, 2015)

Zusätzlich wurde ein weiteres Protokoll namens Enhanced Open entwickelt, um eine verschlüsselte Verbindung mit einer unsicheren WLAN-SSIDs, wie z.B. an öffentlichen WLAN-Hotspots (Gastronomie, Restaurant, usw.) zu ermöglichen. Die Grundlage des Protokolls bildet Opportunistic Wireless Encryption (OWE). (D. Harkins, Ed. u. a., 2017)

Technische Fortschritte gibt es auch beim Mobilfunknetz. Die fünfte Generation bietet eine sehr hohe Bitrate, sehr geringe Latenzzeiten und sehr hohe Verbindungsdichten an. Eine weitere Verbesserung ist die 5G Core Architektur mit Service Based Architecture (SBA) und den darunter liegenden Techniken wie Network Function Virtualisation (NFV) und Software Defined Networking (SDN). (Trick 2020, S.2-3)

Mit der fünften Mobilfunkgeneration gibt es auch ein weiteres Update bzgl. der Antennen-Arrays in Hinblick auf MIMO, da New Radio (NR) eine weitere physikalische Schicht besitzt, welche eine Millimeterwellenkommunikaton ermöglicht. Aufgrund dieser physikalischen Schicht sind die Latenzzeiten geringer geworden und dadurch wird zusätzlich eine höhere Datenübertragung ermöglicht. (Roger Piqueras Jover & Vuk Marojevic, 2019)

Bei der Betrachtung der beiden Drahtlostechnologien (5G vs. Wi-Fi6) ist zu erkennen, dass es wesentliche Verbesserungen bei der Datenübertragung und eine bessere Ausnutzung der Funkkanäle gibt. In Bezug auf die Sicherheit gibt es neue Authentifizierungsprotokolle und Verschlüsselungsmethoden, wie beispielsweise 5G Authentication and Key Agreement (5G-AKA) welches für mehr Sicherheit beim Roaming sorgt. (Roger Piqueras Jover & Vuk Marojevic, 2019)

Können diese Verbesserungen im Mobilfunk die Existenz der österreichischen WLAN-Provider bewahren? Etliche österreichische Unternehmen konnten sich im WLAN-Segment einen Namen und einen Platz am Markt schaffen. Diese bieten Gastronomen, Hotelinhabenden, Veranstaltenden, Einkaufszentren, öffentlichen Personalverkehr und anderen Unternehmen bzw. deren Kundschaft gratis WLAN als Service an. Außerdem werden auch Unternehmensstandorte, mit einer Punkt-zu-Punkt Funkverbindung (WLAN-Bridge) aufgrund hoher Herstellungskosten für kabelgebundenes Internet vernetzt. Ebenfalls bieten Betreiber der kritischen Infrastrukturen nach der Richtline 2008/114/EG (Der Rat der Europäischen Union, 2008), wie beispielsweise die ASFINAG und die ÖBB, ihrer Kundschaft gratis WLAN als Service auf Rastplätzen bzw. Raststationen (Asfinag Maut Service GmbH, 2021) und am Bahnhof oder während der Fahrt im Zug gratis an (ÖBB, 2021).

Infolgedessen wurde im Jahr 2017 von der Europäischen Kommission das Förderungsprogramm Wifi4EU ins Leben gerufen. *„Die Initiative soll die Einrichtung kostenloser öffentlicher WLAN-Hotspots in Städten und Gemeinden in der ganzen EU unterstützen: auf öffentlichen Plätzen sowie in Parks, Krankenhäusern und sonstigen öffentlichen Räumen“* (Europäische Kommission, 2021). Die EU stellt 120 Millionen Euro für die Finanzierung der Initiative zur Verfügung.

Es ist zu erkennen, dass gratis WLAN an öffentlichen Orten eine hohe Akzeptanz vorweisen kann. Um einige Megabyte bzw. Gigabyte an Datenvolumen beim eigenen Mobilfunkvertrag zu sparen, wird das gratis WLAN-Service schnell angenommen. Jedoch sind diese Hotspots in der Regel unverschlüsselte Verbindungen und somit leichte Ziele für Hacker*Innen (A-SIT Zentrum für sichere Informationstechnologie – Austria, 2021). Die Betreibenden des Mobilfunks rollen das 5G Netz immer weiter aus und locken mit moderaten Tarifen die Kundschaft an.

In der oben beschriebenen Problemstellung lässt sich herauslesen, dass die Zukunft für die österreichischen WLAN-Provider ungewiss ist.

1.2 Forschungsziel

Das Ziel dieser Arbeit ist es zu untersuchen, ob durch die Einführung des neuen Mobilfunkstandards 5G, es zu einer Reduktion bzw. zum Aussterben der WLAN-Provider und deren Nutzer*Innen in Österreich kommen kann. Um weitere Lehren ziehen zu können, sollen die Drahtlostechnologien 5G und Wi-Fi6 miteinander verglichen werden. Einerseits wird WLAN für Inhouse und Mobilfunk für Outdoor verwendet, jedoch kommen beide Drahtlostechnologien in beiden Umgebungen zum Einsatz. Womöglich kann eine von den beiden Drahtlostechnologien die Akzeptanz der anderen verringern.

Die Zukunft des öffentlichen WLAN ist ungewiss, da einige Faktoren Einfluss auf die Nutzung und Akzeptanz haben, wie beispielsweise die Sicherheit der jeweiligen Drahtlostechnologie, die Geschwindigkeit, usw. Umso mehr steht die Sicherheit im Fokus der beiden genannten Drahtlostechnologien, da neue Verschlüsselungsmethoden zum Einsatz kommen und deren Auswirkung auf die Nutzer*Innen unbekannt sind. In der wissenschaftlichen Arbeit soll auf die potentiellen Gefahren der beiden genannten Drahtlostechnologien auf Kosten der WLAN-Provider und der Nutzer*Innen hingewiesen werden. Des Weiteren soll geprüft werden, ob es durch den Rollout vom 5G Mobilfunknetz Auswirkungen der Nutzer*Innen in Zusammenhang mit den WLAN-Providern haben wird und welche Faktoren dafür verantwortlich sind.

Rechtliche Aspekte für das Betreiben von WLAN-Hotspots oder von Mobilfunkmasten sind nicht Teil der vorliegenden Masterarbeit. Der Fokus der Forschungsarbeit bezieht sich auf die technologischen Weiterentwicklungen der jeweiligen Drahtlostechnologien. Um die Forschungsarbeit nicht zu sprengen, werden auch nur der Mobilfunkstandard 5G bzw. Wi-Fi6 und deren Sicherheitsprotokolle bearbeitet.

1.3 Forschungsfrage

Welche Bedingungen müssen erfüllt sein, damit Nutzer*Innen österreichische WLAN-Provider gegenüber dem Mobilfunkstandard 5G vorziehen?

1.4 Methodik der Arbeit

Um die vorliegende Forschungsfrage beantworten zu können, wird im ersten Schritt eine intensive facheinschlägige Literaturanalyse durchgeführt. Mit Hilfe dieser Literaturrecherche werden die technischen Aspekte der beiden Standards in WLAN- und Mobilfunksegment auf Stand der Technik ausgearbeitet. Darauffolgend werden im zweiten Schritt der wissenschaftlichen Arbeit im empirischen Teil, zwei verschiedene Arten der Befragungen durchgeführt.

Erstens werden qualitative Inhaltsanalysen (Expert*Inneninterviews mit WLAN-Provider und Mobilfunkanbietenden) nach Mayring durchgeführt (Mayring, 2008, S. 50–60). Für die Befragung können nur bestimmte Expert*Innen herangezogen werden, welche die entsprechenden Kriterien erfüllen. Zum Beispiel langjährige Mitarbeit bei Wi-Fi Providern bzw. bei Mobilfunkanbietenden. Aufgrund der durchgeführten Expert*Inneninterviews, gilt es die Faktoren aus Perspektive der Expert*Innen für das Betreiben öffentlicher WLAN-Hotspots zu identifizieren und darzustellen. Unteranderem soll geklärt werden, welche Faktoren für die Existenz ausschlaggebend sind.

Zweitens werden quantitative Online-Fragenbögen Endbenutzer*Innen zur Verfügung gestellt, um die Erfahrungen der Nutzenden des öffentlichen WLAN widerzuspiegeln und anschließend ausgewertet. Der Online-Fragebogen beinhaltet nur geschlossen Fragen, welche zu beantworten sind (Kotler & Bliemel, 2001, S. 199). Der Online-Fragebogen wird unteranderem am Campus der FernFH zur Verfügung gestellt. Zusätzlich werden weitere teilnehmende Personen mittels digitalen Kommunikationskanälen (E-Mail) kontaktiert und der Online-Fragebogen an diese versendet.

Zur Bestimmung der definierten Faktoren sollen die Expert*Inneninterviews und Online-Fragebögen dienen. Die Kombination der qualitativen und quantitativen Forschung, soll zu Kausalitäten und zu neuen Erkenntnissen in der wissenschaftlichen Arbeit führen.

1.5 Aufbau der Arbeit

Diese Masterarbeit ist in folgende sechs Kapitel aufgeteilt:

In Kapitel 1 (**Einleitung**) werden die eigene Motivation bzw. die Beweggründe hinter dieser wissenschaftlichen Arbeit beschrieben. Zunächst wird auf die Problemstellung eingegangen und anschließend mit einer Forschungsfrage definiert. Des Weiteren wird die Methodik erläutert, wie die wissenschaftliche Arbeit beantwortet werden soll.

Kapitel 2 (**WLAN**) beinhaltet nach kurzer Erläuterung die Entstehung des heutigen WLAN, sowie die unterschiedlichen WLAN-Begriffe. Analog dazu erfolgt die Evolution des WLAN-Standards 802.11 mit seinen technologischen Weiterentwicklungen in den letzten Jahren. Unter anderem wird ausführlich auf den neuesten WLAN-Standard Wi-Fi6 mit seinen technologischen Verbesserungen eingegangen. Zusätzlich werden die neuen Sicherheitsprotokolle erläutert, welche für eine sichere Authentifizierung der Clients dienen.

Das dritte Kapitel (**Mobilfunk** geht auf die Definition des Mobilfunks und der Mobilfunkfrequenzbänder samt deren Regulierung ein. Unter anderem wird die Evolution des Mobilfunkstandards der Vergangenheit und des heutigen Mobilfunkstandard 5G beschrieben. Der Mobilfunkstandard 5G beinhaltet technologische und sicherheitsrelevante Verbesserungen im Standard und im Protokoll, welche für die Nutzer*Innen zum Einsatz kommen.

In Kapitel 4 (**Vorgangsweise und Methode**) wird die Vorgangsweise und die Methode der wissenschaftlichen Arbeit veranschaulicht. In Zusammenhang der angewandten Methodik kommt es zur Operationalisierung der aufgestellten Forschungsfrage und der Hypothese. Die Auswahlkriterien der Expert*Innen Interviews und der Proband*Innen der Online-Umfrage werden ausführlich beschrieben. Abschließend wird die Durchführung der quantitativen und qualitativen Forschungsmethode illustriert.

Die Evaluierung der Forschungsfrage erfolgt in Kapitel 5 (**Ergebnisse und Schlussfolgerungen**). Ergebnisse der durchgeführten Experten*Innen Interviews und der Online-Umfrage werden analysiert, dargestellt und interpretiert. Gefolgt von einer Zusammenfassung der resultierenden gewonnen Erkenntnisse.

Abschließend erfolgt in Kapitel 6 (**Conclusio**) das Fazit und der Ausblick der hier vorliegenden Masterarbeit.

Die nachfolgende Abbildung 1, zeigt den Aufbau der hiervorliegenden wissenschaftlichen Forschungsarbeit.

Abbildung 1 - Aufbau der Arbeit

2 Einführung in die Drahtlostechnologie WLAN

Um ein einheitliches Verständnis über den Begriff WLAN zu bekommen, widmet sich dieses Kapitel der Evolution des WLAN, deren technologischen Weiterentwicklungen mit dem WLAN-Standard Wi-Fi6 und den neuen Sicherheitsprotokollen.

2.1 Grundlagen des WLAN

Das erste Drahtlosnetzwerk wurde im Jahr 1940 von Hedy Lamarr und George Antheil erfunden. Ziel dieses Drahtlosnetzwerkes war es, die eigenen Torpedos vor der gegnerischen Entdeckung von Steuer- und Störsignalen zu schützen. Es war unter dem Namen Frequency Hopping bekannt und hatte eigentlich einen militärischen Zweck. (Schäfers & Walde, 2018, S. 23)

Einige Jahre später, wurden in den 1960er-Jahren die nächsten Schritte in die Richtung der drahtlosen Datenübertragung geforscht. Die Universität von Hawaii entwickelte das sogenannte Aloha-Netzwerk. Mittels des Aloha-Netzwerks wurden sieben Campus-Standorte auf vier verschiedenen Inseln mit dem Zentralrechner aus Oahu untereinander vernetzt. Die bisher teuren verlegten Telefonleitungen wurden nicht mehr benötigt, wodurch es zu einer Kostenreduktion kam. (Rech, 2012, S. 4)

Allerdings hatte das Drahtlosnetzwerk drei nachfolgende Nachteile (Rech, 2012, S. 4):

- Eine geringe Reichweite
- Sehr geringe Datenrate
- Nur proprietäre Produkte waren für den Aufbau eines Drahtlosnetzwerks möglich

Um die oben genannten Probleme zu lösen, wurde durch die IEEE (Institute of Electrical and Electronics Engineers) der 802.11-Standard entwickelt (vgl. Kapitel 2.2). Die IEEE ist ein weltweiter Fachverband von Ingenieur*Innen, welche für die Standardisierung von Techniken, Hardware und Software verantwortlich sind. (Schäfers & Walde, 2018, S. 19)

Die Mitgliederanzahl liegt bei etwa 380.000 Personen und diese agieren aus 150 verschiedenen Ländern. Ausarbeitung, Verabschiedung und Veröffentlichungen von Standards im Netzwerkbereich sind die primären Ziele des Konsortiums (Rech, 2012, S. 5). Im nachfolgenden Kapitel 2.1.2 und 2.1.1 wird der Begriff WLAN bzw. Wi-Fi erklärt, um ein besseres Verständnis für die Lesenden zu generieren.

2.1.1 Erklärung des Begriffs Wi-Fi

Im Sprachgebrauch wird für WLAN auch das Synonym Wi-Fi verwendet. Wi-Fi steht für Wireless Fidelity und bedeutet auf Deutsch übersetzt kabellose Übertragung. Der Begriff ist eigentlich ein Markenbegriff von der Wi-Fi Alliance, welche die WLAN-Geräte nach dem 802.11-Standard zertifizieren. Aufgrund der Zertifizierung von Wi-Fi Alliance, ist eine Kompatibilität zwischen den einzelnen Wi-Fi Produkten der Herstellenden gewährleistet. (Schäfers & Walde, 2018, S. 19)

Damit der Lesefluss in der hier vorliegenden wissenschaftlichen Arbeit vereinfacht wird, werden beide Begriffe verwendet, da diese ein Synonym für beide Bezeichnungen bilden.

2.1.2 Erklärung des Begriffs WLAN

WLAN steht für Wireless Local Area Network und bedeutet auf Deutsch übersetzt, drahtloses lokales Netzwerk. Es verbindet das lokale Netzwerk und ermöglicht es Daten untereinander an die verbundenen Geräte zu übermitteln. (Rech, 2012, S. 3)

Im WLAN kommen verschiedene Komponenten zum Einsatz, damit ein Verbindungsaufbau überhaupt ermöglicht ist (Schäfers & Walde, 2018, S. 33–37):

- **Wireless Network Interface Controller (WNIC):** Ermöglicht es die drahtlosen Signale zu empfangen bzw. zu versenden und ist daher zwingend notwendig.
- **Stations (STA):** Unter Stations werden die Clients wie beispielweise Smartphone, Laptop, usw. verstanden.
- **Access Point (AP):** Der Zugang zum drahtlosen Netzwerk erfolgt über den sogenannten Access Point, welcher auch als Wireless Access Point (WAP) oder WLAN-Router bekannt ist.
- **Authentication Server (AS):** Dieser Server ist für die Authentifizierung der Clients verantwortlich und kommt in den meisten Unternehmensnetzwerken zum Einsatz.
- **Distribution System (DS):** Um die drahtlose und die kabelgebundene Kommunikation im Netzwerk zu ermöglichen, wird ein DS benötigt. Die Kommunikation erfolgt über Ethernet oder Glasfaser.
- **WLAN-Controller (WLC):** Mittels eines WLCs besteht die Möglichkeit, die WAPs zentral zu managen. Neue WLAN-Namen, sogenannte SSIDs (Service Set Identifier) können problemlos angelegt werden. Eine Adaptierung der

Sicherheitskonfiguration kann zentral ausgerollt werden. Des Weiteren kann ein Authentication Server für die Authentifizierung in einem WLAN aktiviert werden.

2.1.3 Definition der WLAN-Provider

Gier (2006, S. 46) beschreibt den WLAN-Provider als einen Hotspot in einer großen und öffentlichen WLAN-Umgebung, der aus Access Points, Antennen und aus einem Abrechnungsserver besteht. Der Zugriff erfolgt mittels WLAN-fähigen Endgeräten, wie beispielsweise Smartphones oder Laptops. Öffentliche WLAN-Hotspots sind in Einkaufszentren, in der Gastronomie, in Schulen, an Universitäten, in Hotels, an Flughäfen, an Bahnstationen und an Autobahn-Raststätten zu finden. Ein weiteres Einsatzgebiet sind auch drahtlose Netzwerke in Unternehmen. Dadurch wird den Geschäftspartnern oder den eigenen Mitarbeiter*Innen ein flexibler Internetzugang ermöglicht.

Folglich existieren unterschiedliche Arten von WLAN-Hotspots, wie beispielsweise (Gier, 2006, S. 47–50):

- **Public Hotspot:** Das WLAN-Service wird für Benutzer*Innen kostenpflichtig betrieben, welche von öffentlichen Benutzergruppen verwendet werden kann, um ins Internet zu gelangen.
- **Post Paid:** Nach Benutzung des WLAN-Service erfolgt eine Abrechnung nach verbrauchten Minuten oder Stunden, je nachdem wie die Abrechnung vom Betreiber eingestellt wurde.
- **Pre Paid:** Vor der Nutzung des WLAN-Service, erwerben die Benutzer*Innen einen Voucher und zahlen eine bestimmte Zeiteinheit, z.B. Minuten oder Stunden.
- **Used-Time:** Hier erfolgt die Verrechnung nach tatsächlich verbrauchten Zeiteinheiten. Wird beispielsweise ein Guthaben von einer Stunde erworben und es werden nur fünfzehn Minuten verbraucht, so bleibt ein Restguthaben von 45 Minuten übrig.
- **Voucher:** Es wird den Benutzer*Innen ein Voucher samt Benutzername und Passwort übergeben, in dem eine bestimmte Zeiteinheit für das Internetsurfen gutgeschrieben ist.

WLAN-Provider werden auch als WISP (Wireless Internet Service Provider) bezeichnet und stellen einen drahtlosen Internetzugang zur Verfügung. Der Begriff ist für eine Firma, eine Organisation oder eine Person, welche überregional WLAN-Hotspotlösungen anbietet und eine zentrale Verrechnung mittels eines Radius-Servers durchführt. (Gier, 2006, S. 52)

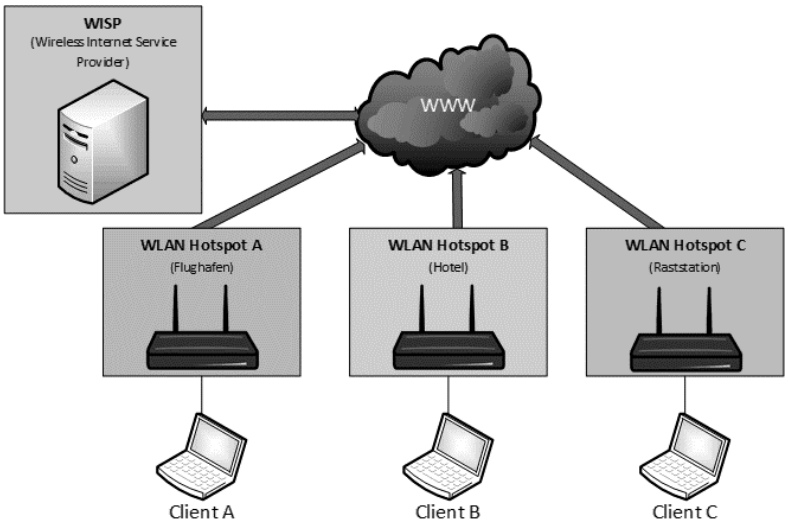

Abbildung 2 – WISP (Anlehnung an Gier, 2006, S. 52)

2.1.4 Das WLAN-Frequenzband

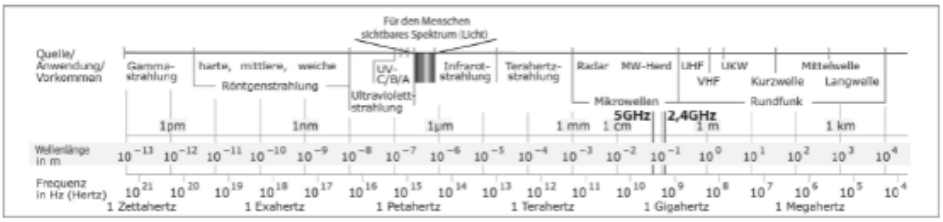

Abbildung 3 - Elektromagnetisches Spektrum (Schäfers & Walde, 2018, S. 19)

Elektromagnetische Wellen sind gekoppelte elektrische und magnetische Transversalwellen, die im freien Raum übertragen werden. Die Auswahl der Frequenz für die drahtlose Datenübertragung ist im 2,4 GHz und 5GHz Frequenzband definiert und liegt im niederfrequenten Mikrowellenspektrum (,vgl. Abbildung 3). In Europa ist die Sendeleistung auf 100mWatt reguliert. (Schäfers & Walde, 2018, S. 19–21)

WLAN funktioniert in den zwei unlizenzierten Frequenzbändern, 2,4 GHz und 5 GHz. Der tatsächliche Frequenzbereich liegt bei 2,4 GHz zwischen 2,400 und 2,4835 GHz. Beim 5 GHz Frequenzband existieren vier verschiedene Bereiche (Edgeworth u. a., 2019, S. 485–486):

- 5,150 bis 5,250 GHz
- 5,250 bis 5,350 GHz
- 5,470 bis 5,725 GHz
- 5,725 bis 5,825 GHz

2.2 Evolution des WLAN-Standards 802.11

Am 26.Juni 1997 wurde der Grundstandard 802.11 definiert und dieser beinhaltet für die drahtlose Datenübertragung einen MAC-Layer (Media Access Control) und drei PHY-Layer (Physical) (Rech, 2012, S. 6). Diese zwei Layer sind die untersten Schichten im OSI-Schichtmodel (Open Systems Interconnection), welches auch als OSI-Layer bekannt ist. Das OSI-Schichtmodell enthält sieben verschiedene Schichten. Die erste Schicht (PHY-Layer) ist für die Übertragung, die Codierung und die Modulation des Signals verantwortlich. Um Fehler bei einer Datenübertragung zu erkennen, kommt das CRC-Verfahren (Cyclic Redundancy Check) zum Einsatz. Es wird eine Prüfsumme errechnet und erkennt dabei die Fehler bei der Datenübertragung. Diese Überprüfung geschieht in der zweiten Schicht (MAC-Layer) des OSI-Schichtmodells. Zusätzlich werden die Formate des WLAN-Frames, der Fragmentierung und die Managementfunktion implementiert. Dieser Standard 802.11 ermöglicht eine maximale Bruttodatenrate von 2 MBit/s (Megabit pro Sekunde) und operiert im 2,4 GHz-Band (Gigahertz). (Schäfers & Walde, 2018, S. 23)

Der 802.11a-Standard wurde am 16.September 1999 veröffentlicht. Eine Datenübertragung von 54 Mbit/s ist aufgrund des Modulationsverfahren OFDM (Orthogonal Frequency-Division Multiplexing) möglich (, vgl. Kapitel 2.3.1). Darüber hinaus operiert dieser Standard das erste Mal im 5 GHz-Band. (Schäfers & Walde, 2018, S. 23)

Im gleichen Jahr am 09.Dezember 1999, wurde ein weiterer WLAN-Standard veröffentlicht. 802.11b arbeitet im 2,4 GHz-Band und verwendet DSSS (Direct Sequence Spream Spectrum) als Modulationsverfahren. Es ist eine Datenübertragung bis zu 11 MBit/s möglich (Aguilera, 2018, S. 14) und es ist somit genauso schnell wie die Grundversion des drahtgebundenen Ethernets, welche eine Datenübertragung von 10MBit/s erreicht (Rech, 2012, S. 6).

Wie im vorigen beschriebenen Standard 802.11a, ist es nun möglich im Standard 802.11g eine Datenübertragung bis zu 54 MBit/s über 2,4 GHz zu erzielen. Diese Standarderweiterung erfolgte am 12.Juni 2003. Es ist lediglich auf eine Sendeleistung von 20 dBm (100 mW) zu achten (Rech, 2012, S. 7), um die Produkte ohne rechtlichen Problemen und Einschränkungen in Europa betreiben zu können (Schäfers & Walde, 2018, S. 24).

Der erste große Durchbruch in Bezug auf die Schnelligkeit bei einer Drahtlosübertragung wurde mit dem 802.11n WLAN-Standard geschaffen. Veröffentlicht wurde dieser am 11.September 2009 und ist auch unter dem Synonym High-Throughput-Erweiterung bekannt. Änderungen im PHY-Layer und MAC-Layer waren der Grund, dass eine bessere Performance bei der Datenübertragung erzielt werden konnte. Mittels Einführung der MIMO-Technologie (Multiple Input and Multiple Output) im 802.11n WLAN-Standard, war es möglich, gleichzeitig zwischen zwei WLAN-Geräten mehrere Signale zu senden. 4x4 MIMO bedeutet, dass maximal vier Antennen senden und vier Antennen empfangen können. Zusätzlich sind beide Frequenzbänder 2,4 GHz und 5GHz für die drahtlos Kommunikation möglich, dies wird auch als Dual Band bezeichnet (Schäfers & Walde, 2018, S. 25). Datenraten bis 600MBit/s sind theoretisch möglich, aber kaum realisierbar. In der Praxis kommen 3x3 MIMO Antennen zum Einsatz. (Rech, 2012, S. 9) Eine detaillierte Beschreibung der MIMO-Technologie erfolgt in Kapitel 2.3.2.

Erstmals können statt wie bisher 20 MHz-Channels, auch 40 MHz-Channels als Übertragungskanäle benutzt werden, wodurch eine bessere Codierung mit weniger Overhead bei Bits pro Hertz möglich ist. (Schäfers & Walde, 2018, S. 24)

Im Dezember 2013 wurde der neue WLAN-Standard 802.11ac von der IEEE veröffentlicht. Der Standard arbeitet nur im 5 GHz Frequenzband und erzielt eine theoretische Bruttogeschwindigkeit bis zu 6,9 GBit/s. Um jedoch die Bruttogeschwindigkeit zu erreichen, sind einige technische Spezifikationen am WLAN-Router notwendig, welche aber vom offiziellen 802.11ac WLAN-Standard abweicht. Von den Herstellenden werden diese Geräte dennoch produziert und am Markt angeboten (Schäfers & Walde, 2018, S. 26) Der reale maximale Datendurchsatz beträgt bis zu 3600MBit/s (Aguilera, 2018, S. 16).

Very-High-Throughput ist ein weiteres Synonym für den 802.11ac WLAN-Standard. Es verwendet die Kanalbreite zwischen 80 und 160 MHz. Zusätzlich wird Downlink MU-MIMO mit bis zu vier Antennen unterstützt und die Modulationstechnik 256-QAM (Quadrature Amplitude Modulation) angewandt (, vgl. Kapitel 2.3.3.). (Aguilera, 2018, S. 15)

Um einen verbesserten Datendurchsatz, eine bessere Reichweite und die Implementierung von Stromsparfunktionen zu erzielen, wurde im Jahr 2018 der neue WLAN-Standard 802.11ax von der IEEE veröffentlicht. Aufgrund des neuen Modulationsverfahren OFDMA (Orthogonal Frequency Division Multiple Access) statt wie bisher OFDM, kommt es zur effizienten Kanalnutzung und es kann theoretisch ein maximaler Datendurchsatz bis zu 9,6 GBit/s erzielt werden und ist um 37% schneller als der Vorgänger 802.11ac (Henry u. a., 2020, S. 464–457). Der reale max. Datendurchsatz beträgt allerdings 8 GBit/s (Aguilera, 2018, S. 16). Im nachfolgenden Kapitel 2.3 wird der neue WLAN-Standard 802.11ax detaillierter erläutert.

Die nachfolgende Abbildung 4 visualisiert die technischen Spezifikationen der oben angeführten WLAN-Standards und fasst diese zusammen.

Standard	Jahr	Max. Datendurchsatz	Frequenzband	Modulationstechnik	Modulation	Kanalbreite	MIMO
802.11a	1999	54 Mbit/s	5 GHz	64-QAM	OFDM	20 MHz	1x1
802.11b	1999	11 MBit/s	2,4 GHz	-	DSSS	20 MHz	1x1
802.11g	2003	54 MBit/s	2,4 GHz	64-QAM	OFDM	20 MHz	1x1
802.11n	2009	65 bis 450 MBit/s	2,4 und 5 GHz	64-QAM	OFDM	20, 40 MHz	Bis zu 3x3
802.11ac	2013	290 bis 3600 MBit/s	5 GHz	256-QAM	OFDM	20, 40, 80, 160 MHz	Bis zu 4x4 downlink MU
802.11ax	2018	600 bis 8000 MBit/s	2,4 und 5 GHz	1024-QAM	OFDMA	20, 40, 80, 160 MHz	Bis zu 8x8 dowlink/uplink MU

Abbildung 4 - Evolution des WLAN-Standards IEEE802.11 (Anlehnung an Aguilera, 2018, S. 13)

2.3 Wi-Fi6

Wie bereits in Kapitel 2.2 erwähnt, kam es bei den WLAN-Standards immer wieder zu einigen technologischen Verbesserungen, sowie auch im neuen WLAN-Standard 802.11ax, welcher auch als Wi-Fi 6 bekannt ist. Im Jahr 2018 gab es das erste Mal mehr WLAN-fähige Endgeräte als Menschen auf dem Planeten. Dementsprechend ist zu entnehmen, dass dieser Trend weiter anhalten wird, da immer mehr IOT-Geräte (Internet of Things) mit dem Internet verbunden werden. Laut Cisco (, 2021) wird es im Jahr 2023 im Verhältnis zur gesamten Weltpopulation dreimal so viele IP-fähige Endgeräte geben.

Infolgedessen wird es einen stärkeren Datenbedarf geben, wodurch die aktuellen Mobilfunktechnologien einen Flaschenhals für die gestiegenen Datenübertragungen darstellen. Videostreaming in Full HD bzw. 4K Auflösung und Online-Gaming sind die wesentlichen Treiber der Erhöhung der Datenmengen. (Aguilera, 2018, S. 57–58)

Die meisten Drahtloskommunikationen treten in Städten mit Mobilgeräten auf, welche durch die Geometrie der Gebäude, die Übertragung der Wellen reflektieren und eine Auswirkung auf die Qualität haben. Existiert zwischen dem Sendenden und dem Empfangenden kein Hindernis, dann erhält der Empfangende ein besseres Signal. Man spricht hier von Line-of-Sight (LoS), einer direkten Sichtverbindung. Sobald ein Hindernis, wie beispielsweise eine Ziegelmauer zwischen dem Sendenden und dem Empfangenden existiert, kommt es zur Verringerung des Signals um 5dB. Non-Line-of-Sight (NLoS) ist der Begriff für diesen Zustand, welcher auch ein Problem für Indoor WLAN-Standorte darstellt. (Aguilera, 2018, S. 59)

Der wesentliche Treiber der Designweiterentwicklung des WLAN-Standards 802.11ax ist, dass die Endgeräte in unterschiedlichen Bereichen und Umgebungen eingesetzt werden, wie beispielsweise Flughäfen, Massenveranstaltungen, Einkaufszentren, Outdoor-Hotspots und in dicht besiedelten Wohnobjekten. Es wird eine Vielzahl an WLAN-Accesspoints für die Abdeckung benötig, jedoch operieren diese in überlappenden Kanälen. Ziel ist es die Durchsatzdichte bzw. Datenrate in solchen Umgebungen zu erhöhen. (Khorov u. a., 2019, S. 197)

Wie bereits einleitend erklärt, steigt die Anzahl der IoT-Geräte stetig in WLAN-Umgebungen an. IoT-Geräte besitzen eine Batterie, welche durch Abfragen der Zustände der Sensoren entladen wird. Das Ziel ist es, den Energieverbrauch zu verringern und zu optimieren. Nicht nur IoT-Geräte besitzen Sensoren (Lichtsensor, Kamera, Touchscreen) und Aktoren (4k Displays, Fotoblitz), sondern auch WLAN-fähige Endgeräte. All diese Probleme und Anforderungen stellen die Verbesserung des neuen WLAN-Standards 802.11ax dar. Die wichtigsten Erneuerungen sind OFDMA, DL und UL MU-MIMO (Downlink and Uplink MU-MIMO), BSS Coloring (Basic Service Set), 1024-QAM und TWT (Target Wake Time). (Aguilera, 2018, S. 62–72)

2.3.1 Modulationsverfahren OFDMA (Orthogonal Frequency Division Multiple Access)

Beim bisherigen Modulationsverfahren OFDM mussten die Benutzenden bei der Übertragung von Daten warten, solange der Kanal belegt war. Unter den Standards 802.11a/g/n/ac ist ein 20 MHz Kanalband in 64 Unterkanäle (Subcarrier) geteilt worden. Jeder Unterkanal ist vom anderen Unterkanal 312.5 kHz entfernt und überträgt dort die Bits. Eine Übertragung pro Bit benötigt 3.2 µs, zusätzlich 0.4 oder 0.8 µs für Wachstandardintervalle (guard interval), sollten bedeutungslose Echos oder Reflektionen zum Hauptsignal zurückkehren. Diese haben jedoch keine Auswirkung auf die Übertagungsnachricht. (Henry u. a., 2020, S. 467)

OFDMA hat 256 Unterkanäle im 20 MHz Kanalband und besitzt einen Abstand von 78.125 kHz zu den anderen Unterkanälen. Die Übertragung dauert im Gegensatz zu OFDM länger, da diese auf 12.8 µs vergrößert wurde. Wachstandardintervalle wurden auf 0.8 µs, 1.6 µs und 3.2 µs definiert. Dank dieser Anpassung ist es möglich die Bits parallel zu senden, welche auch einen besseren Widerstand gegen Frequenzstörungen besitzen. Viermal so viele Unterkanäle in OFDMA, ermöglichen einen höheren Datendurchsatz. Mittels OFDMA steigt der Datendurchsatz um 10 bis 20% zu seinem Vorgänger und ist für Outdoor- und Indoorumgebungen mit einer hohen Kanalbelegung nützlich. (Henry u. a., 2020, S. 467)

Mit der OFDMA-Technik werden die Unterkanäle in eine Ressourceneinheit (RU) gruppiert und der Absendende kann die beste RU auswählen für jeden einzelnen Empfangenden, wodurch der Datendurchsatz gesteigert wird (, vgl. Abbildung 5). (Khorov u. a., 2019, S. 200)

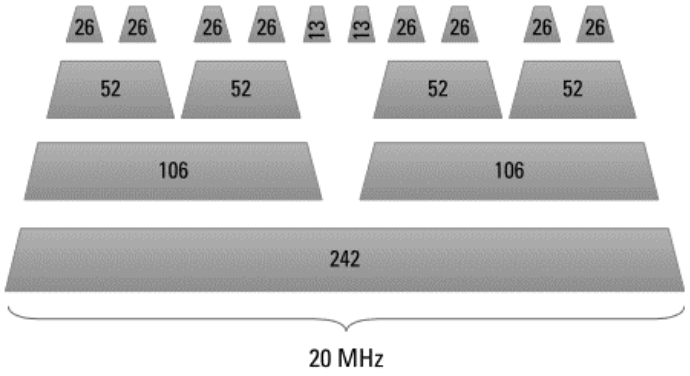

Abbildung 5 - Ressourceneinheit (RU) in 20 MHz Frequenzband (David Coleman & Lawrence C. Miller, 2018, S. 14)

Die nachfolgende Abbildung 6, illustriert den Vergleich zwischen den beiden Technologien OFDM und OFDMA. Im oberen Teil vom Bild, sendet eine Station (STA) bzw. ein WLAN-fähiges Endgerät zum jeweiligen Zeitfenster (Time) über die belegte Frequenz (Frequency). Die Übermittlung der Daten erfolgt nach der Reihe. Im unteren Teil vom Bild, sendet eine STA pro Unterkanal zu unterschiedlichen Zeitfenstern, dadurch ist ein paralleles Senden und Empfangen möglich. (Aguilera, 2018, S. 64–65)

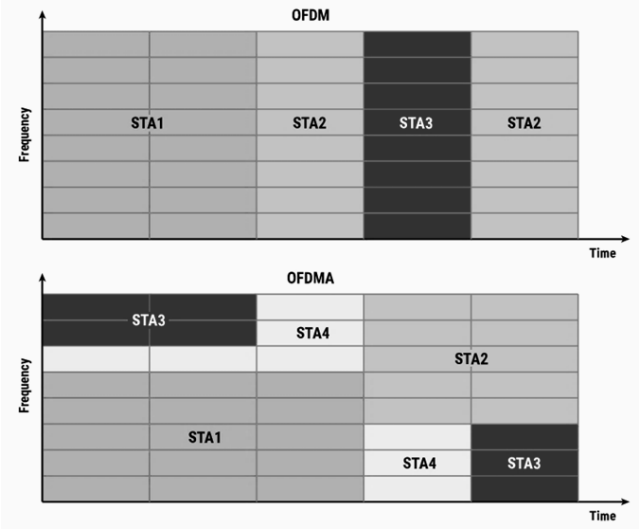

Abbildung 6 - OFDM vs. OFDMA (Aguilera, 2018, S. 64)

Zusammenfassend kann gesagt werden, dass bei OFDM nur ein Endgerät zum bestimmten Zeitpunkt kommunizieren kann. Die Datenübertragung des Signals erfolgt nacheinander. Bei OFDMA wiederum, können die Daten unabhängig vom belegten Kanal versendet werden, da diese in Unterkanäle (RU) geteilt werden. Eine gleichzeitige Kommunikation ist möglich und es wird eine effiziente Frequenznutzung durch OFDMA erzielt.

2.3.2 DL und UL MU-MIMO

Am Beginn der Drahtlosübertragung verwendeten WLAN-fähige Endgeräte einen Eingang und einen Ausgang, welcher auch als Single-In und Single-Out (SISO) Begriff bekannt ist. Ab dem 802.11n Standard kamen die ersten MIMO Systeme zum Einsatz. (Edgeworth u. a., 2019, S. 505)

802.11ac brachte in seiner zweiten Welle seiner Veröffentlichung Downlink MU-MIMO zum Vorschein. Da die Kollisionsdomäne innerhalb des Funkkanals getrennt wird, ist eine Multi-Antennen und Multi-User Kommunikation möglich. Bisher sendete der WLAN-Accesspoint den Datenverkehr iterativ zu seinen verbundenen Endgeräten. Ein gleichzeitiges Senden der Daten war zu diesem Zeitpunkt nicht möglich. Bei Downlink MU-MIMO hingegen, können die Daten gleichzeitig an alle Endgeräte versendet werden. (Aguilera, 2018, S. 20–21)

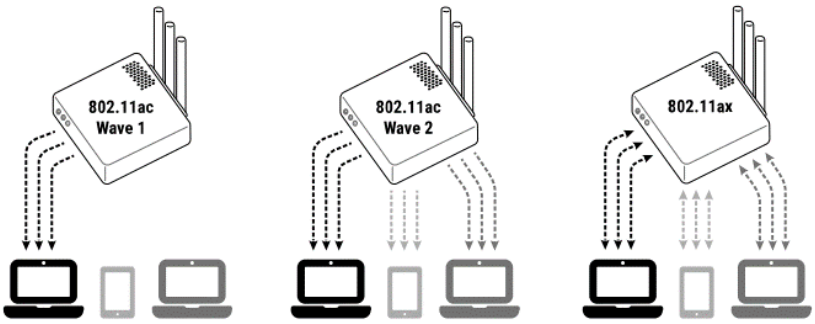

Abbildung 7 - MU-MIMO Vergleich (Aguilera, 2018, S. 21)

Downlink und Uplink MU-MIMO erlaubt ein gleichzeitiges Senden und Empfangen an alle verbundenen Endgeräte (, vgl. Abbildung 7). Bis zu 74 WLAN-fähige Endgeräte können damit bedient werden. Wird Uplink MU-MIMO nicht unterstützt, so müssen die Endgeräte nacheinander die Daten über den Kanal versenden (, vgl. Tabelle 1). (Oran Sharon & Yaron Alpert, 2018, S. 6)

Ressource Unit (RU)	20 MHz Kanal	40 MHz Kanal	80 MHz Kanal	160 MHz Kanal
26 Unterkanäle	9	18	37	74
52 Unterkanäle	4	8	16	32
106 Unterkanäle	2	4	8	16
242 Unterkanäle	1	2	4	8
284 Unterkanäle	-	1	2	4
996 Unterkanäle	-	-	1	2

Tabelle 1 - Ressourceneinheit mit Unterkanälen (Anlehnung an Khorov u. a., 2019, S. 204)

2.3.3 1024-QAM (Quadrature Amplitude Modulation)

Um die Bitströme in Symbole umzuwandeln, verwendet die Quadrature Amplitude Modulation zwei orthogonale Transformationsimpulse. Kommt es zu einer Verunreinigung in der Luft, besser gesagt zu einem Rauschen, dann wird mittels der Orthogonalität das Symbol am Empfangsmodul wiedergewonnen. Eine wichtige Kennzahl für die Qualität der Drahtlosübertragung stellt der Begriff Signal to Noise and Interference Ratio (SNIR) dar. Dieser bildet sich aus der Beziehung zwischen dem Signal und dem Rauschen plus der Interferenzstärke. (Aguilera, 2018, S. 44–45)

1024-QAM bedeutet, 1024 verschiedene Signalpositionen davon 256 in jedem Quadranten. In der QAM-Übertragungstechnik variiert die Übertragungsrichtung und die Intensität der Unterkanäle so, dass die Spitzen des Signals mit der Zielposition übereinstimmen. Zu jedem Symbol welches das Ziel darstellt, wird eine imaginäre vertikale und horizontale Linie gebildet, die aus dem Zentrum der vier Quadranten verläuft (,vgl. Abbildung 8). (Henry u. a., 2020, S. 465–466)

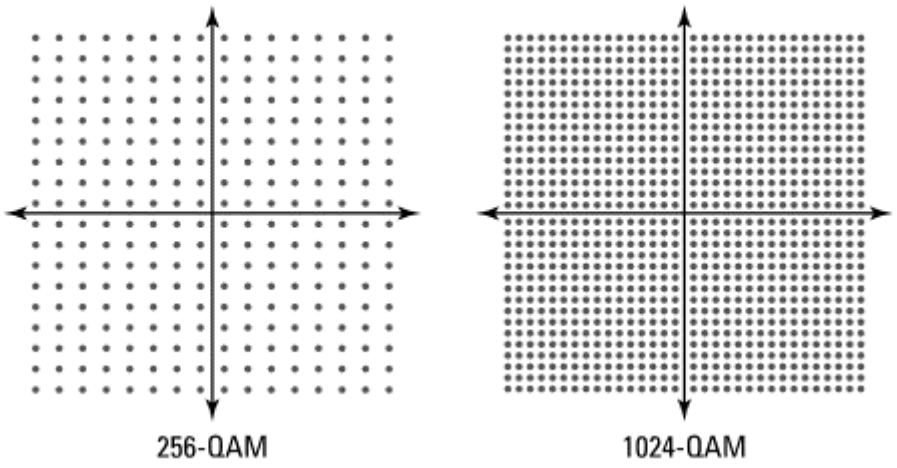

Abbildung 8 - QAM Übertragungstechnik (David Coleman, 2021, S. 50)

Insofern kann man festhalten, dass aufgrund der höheren Modulation und der effizienten Nutzung des Frequenzspektrums, eine höhere Datenrate erzielbar ist. Dieses ist jedoch auch von optimalen Bedingungen wie beispielsweise Rauschen, Signalstärke und Abstand zwischen WLAN-Accesspoint und Endgerät abhängig.

2.3.4 BSS Coloring

Ein weiteres Feature von 802.11ax ist das sogenannte Basic Service Set (BSS) coloring. In dichten Umgebungen ist es zu erwarten, dass zwei oder mehrere WLAN-Accesspoints am gleichen Kanal, vor allem in 80 MHz oder 160 MHz-Kanälen, senden. Sollten Richtantennen oder ein Hindernis zwischen WLAN-Accesspoints sein, dann hören diese sich gegenseitig nicht. Clients in einer hohen Dichte mit dieser Konstellation, werden jedoch darunter leiden, da Datenkollisionen (CSMA/CA) vom Nachbar WLAN-Accesspoint beim Empfangen oder beim Senden zum eigenen WLAN-Accesspoint auftreten werden. Um die Datenkollision zu verhindern, können Clients in 802.11ax ein BSS Kollisionsreport senden. Der WLAN-Accesspoint markiert alle Frames und bittet die Clients seine Frames ebenfalls in einer bestimmten Reihe von Bits zu markieren (, vgl. Abbildung 9). In diesem Fall wird vom Coloring gesprochen, sozusagen eine Art des zellspezifischen Labels oder einfärben. Die Clients verringern die Sensitivität, um etwaigen Signaleingang von anderen WLAN-Accesspoints zu ignorieren. Unter der Annahme, dass der lokale WLAN-Accesspoint näher ist als die der Nachbar WLAN-Accesspoints. Bei der Datenübertragung erkennen die Clients ihre eigene Farbe und die des nichtzuständigen Fremdnetzes. Sendet der Nachbar WLAN-Accesspoint auf seiner eigenen Farbe, dann kann der eigene WLAN-Accesspoint ungestört Daten senden bzw. empfangen oder das Signal vom fremden WLAN-Accesspoint ignorieren. Demgemäß erlaubt dieser Mechanismus eine höhere Zelldichte und eine bessere Ausnutzung der überlappenden BSS. (Henry u. a., 2020, S. 467)

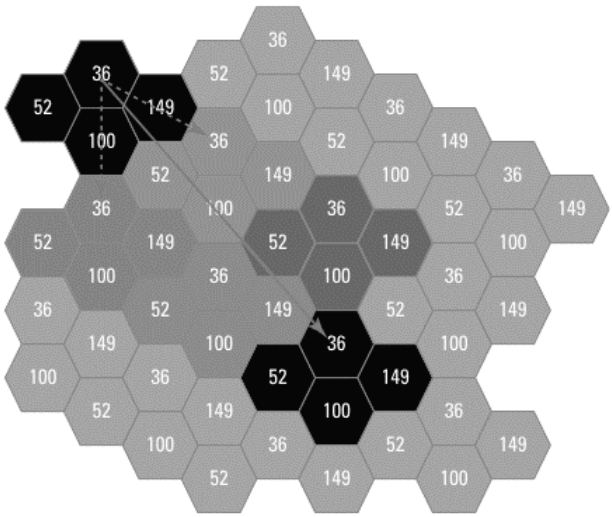

Abbildung 9 - BSS Coloring (David Coleman & Lawrence C. Miller, 2018, S. 20)

2.3.5 Target Wake Time (TWT)

Zusätzlich wurde ein Energiesparmechanismus im neuen Standard 802.11ax implementiert. Der WLAN-Accesspoint meldet dem Client wie oft dieser aufwachen und nur bei Bedarf eine Datenübertragung durchführen soll. Die Verbindung zwischen WLAN-Accesspoint und Client bleibt weiterhin bestehen, da der Client den eingehenden Traffic aufrechterhält. Sobald der WLAN-Accesspoint eine Rückmeldung benötigt, sendet dieser den Traffic retour. Dieser Prozess ermöglicht es, Energie bei batteriebetriebenen Geräten (Smartphones und IoT) zu sparen. Die längste Schlafperiode von batteriebetriebenen Geräten beträgt maximal fünf Jahre. (Henry u. a., 2020, S. 470)

Als Beispiel einer IoT TWT-Verbindung wir die Abbildung 10 herangezogen. Die Sensoren (Clients) melden nach einem aufgetretenen Event an den verbundenen WLAN-Accesspoint den benötigten Wert.

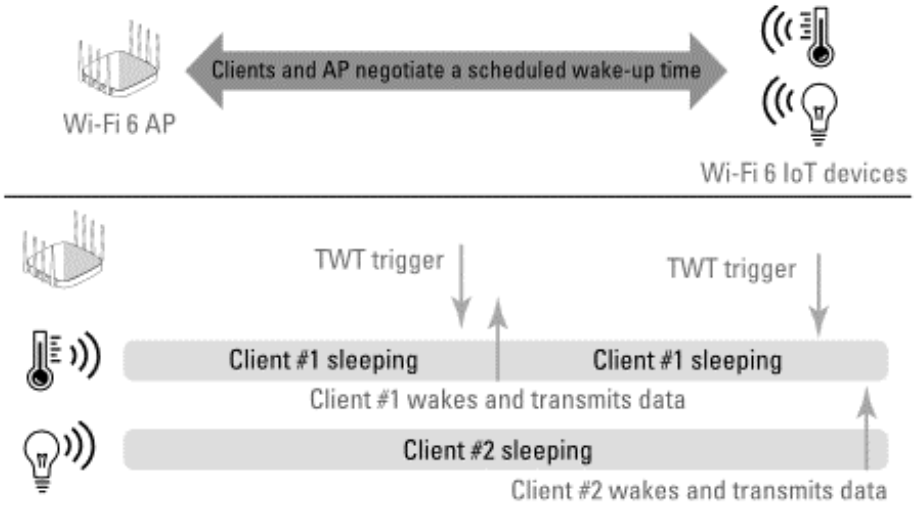

Abbildung 10 - TWT IoT Beispiel (David Coleman, 2021, S. 48)

2.4 Sicherheitsaspekte im WLAN-Standard 802.11ax

Die Grundlage für Sicherheitsmechanismen in Kommunikationsprotokollen bilden die drei Bereiche in der Informationssicherheit, welche auch unter dem Begriff CIA-Triade (Confidentially, Integrity and Availability) bekannt sind:

- **Confidentially (Vertraulichkeit):** Unter dem Begriff Vertraulichkeit wird sichergestellt, dass Informationen nicht von Dritten unberechtigt eingesehen werden kann. Daten dürfen nicht weitergegeben oder veröffentlichen werden. (Dieter Burgartz & Ralf Röhring, 2014, S. 16)
- **Integrity (Integrität):** Die Korrektheit bzw. die Unversehrtheit der Daten gehört sichergestellt. Es sollen jegliche unautorisierte Modifikationen der Daten verhindert werden, dies impliziert auch vor Datenverlust zu schützen. (Schäfers & Walde, 2018, S. 70)
- **Availability (Verfügbarkeit):** Die Nutz- und Verfügbarkeit der Daten stehen jederzeit bei Bedarf zum Abruf. Eingesetzte IT-Anwendungen und IT-Infrastrukturen müssen die Ressourcen jederzeit zur Verfügung stellen können. (Dieter Burgartz & Ralf Röhring, 2014, S. 16)

Zusätzlich hat der Begriff Authentizität eine wichtige Rolle in der Informationssicherheit, hierdurch wird eine eindeutige Zuordnung einer Information zum Absendenden zugeordnet. Ein Kommunikationspartner gibt somit tatsächlich vor, dass dieser der Absendende ist. (Schäfers & Walde, 2018, S. 70)

WLAN besitzt keine physische Trennung von Datenpaketen, während diese drahtlos übertragen werden. Sollten Hacker*Innen in Funkreichweite sein, so können diese die übertragenen Daten abfangen, mitlesen oder verändern. Aufgrund der Reflektionen kann WLAN auch an undenkbaren Orten, wie beispielsweise außerhalb der Wohnung oder Firmengeländen reflektiert werden. Eine Verschlüsselung der Kommunikation ist unvermeidlich und ein wichtiger Faktor in der Informationssicherheit. (Schäfers & Walde, 2018, S. 69)

Für die Verschlüsselung der Kommunikation wird entweder der symmetrische oder der asymmetrische Verschlüsselungsalgorithmen angewandt. Beim symmetrischen Algorithmus wird ein Schlüssel benötigt, der dem Sendenden und dem Empfangenden bekannt ist. Dieser Schlüssel wird für das Ver- und Entschlüsseln eingesetzt. Allerdings existieren beim asymmetrischen Algorithmus zwei Schlüssel, der Public Key (öffentlicher Schlüssel) und der Private Key (privater Schlüssel). Zum Verschlüsseln der Nachricht dient der öffentlich bekannte Public Key. Um die Nachricht zu entschlüsseln, wird der Private Key benötigt. (Schäfers & Walde, 2018, S. 70)

2.4.1 Sicherheitsbedrohungen im WLAN

Es existiert eine Vielzahl an unterschiedlichen potenziellen Gefahrenquellen im WLAN, sei es bei der Nutzung oder auch beim Betreiben von WLAN-Hotspots. Laut BSI (Bundesamt für Sicherheit in der Informationstechnik) (2021, S. 2–4) wurden nachfolgende Bedrohungen oder Schwachstellen in den IT-Grundschutz-Bausteinen NET: Netze und Kommunikation identifiziert:

- **Ausfall oder Störung eines Funknetzes:** Denial-of-Service-Angriffe mittels elektromagnetischer Funkwellen die im selben Frequenzspektrum strahlen, können das Funknetz stören.
- **Fehlende oder unzureichende Planung des WLAN-Einsatzes:** Bei der Planung eines WLANs soll die Verschlüsselung dem Stand der Technik entsprechen.
- **Ungeeignete Auswahl von Authentisierungsverfahren:** Sicherheitslücken können durch die falsche Auswahl von Authentisierungsverfahren und -mechanismen auftreten.
- **Fehlerhafte Konfiguration der WLAN-Infrastruktur:** Fehlerhafte Konfigurationen am WLAN-Accesspoint oder an anderen WLAN-Komponenten können zu unsicheren Kommunikationen oder sogar zum Totalausfall führen.
- **Unzureichende oder fehlende WLAN-Sicherheitsmechanismen:** Ältere WLAN-Komponenten unterstützen oft nicht den neuesten Stand der Technik und sind daher unzureichend bis kaum geschützt.
- **Abhören der WLAN-Kommunikation:** Daten die über das WLAN übertragen werden, können abgefangen und mitgehört werden, falls diese nicht oder unzureichend verschlüsselt sind.
- **Vortäuschung eines gültigen Access Points (Rogue Access Point):** Hacker*In geben sich als Teil der WLAN-Infrastruktur aus, in dem diese die

SSID des eigenen WLAN angeben. Der WLAN-Accesspoint strahlt stärker als der echte WLAN-Accesspoint und ermöglicht es dem Angreifenden die Kommunikation mitzulesen. Rogue Access Points sind beliebte Angriffsvektoren von Hacker*Innen.

- **Ungeschützter LAN-Zugang am Access Point:** Wird der Zugang zur Switchinfrastruktur ermöglicht, können angreifende Personen die Ethernetverbindung mitlesen.
- **Hardware-Schäden:** Bei Hardwareschäden kann es zu einem Komplettausfall der Funkverbindung kommen. Vorsätzliche Beschädigungen oder Schäden durch Witterung und Blitzeinschläge sind im Outdoorbereich relevant.

Hacker*Innen haben zwei Möglichkeiten eine Informationsbeschaffung durchzuführen. Erstens durch WLAN-Sniffing, in dem der WLAN-Verkehr mitgehört wird, ohne selbst Daten zu produzieren. Sniffer-Angriffe werden daher schwer entdeckt, da beim Angriff keine Spuren hinterlassen werden. Zweitens mittels aktiven Scanning, in dem mittels Probe Request via Broadcast versucht wird, weitere Informationen zu ermitteln. Der Angreifende stellt vereinfacht dargestellt eine Frage an den anzugreifenden WLAN-Accesspoint, ob jemand hier ist und welche Ports antworten (Schäfers & Walde, 2018, S. 134–136)

Ein weiterer aber nicht außer Acht zu lassender Angriffsvektor ist das Social Engineering. Angreifende Personen können sich als Technicker*In ausgeben und so Zutritt zur Infrastruktur verschaffen. Dieser kann einen Rogue Access Point platzieren und außerdem weitere Angriffe vorbereiten. Um Informationen zu gewinnen, werden gezielt menschliche Eigenschaften genutzt, die später dazu dienen Computer oder Netzwerke zu kompromittieren. Zu den menschlichen Eigenschaften zählen beispielsweise Hilfsbereitschaft, Sympathie, Vortäuschen von Knappheit bzw. Zeitdruck und Autoritätshörigkeit. (Schäfers & Walde, 2018, S. 149)

2.4.2 WPA3-Personal

Wi-Fi Protected Access 3 (WPA3) ist der Nachfolger von WPA2, der als Reaktion zum KRACK-Angriff stattgefunden hat. Angreifende nutzen eine Designschwäche während des 4-Way-Handshakes aus und können den Schlüssel erlangen. Ein Mitlesen des Datenverkehrs oder zu manipulieren ist möglich. (Mathy Vanhoef & Frank Piessens, 2017)

Statt dem bisher eingesetzten Preshared Key (PSK) wird in WPA3-Personal die Authentifizierungsmethode Simultaneous Authentication of Equals (SAE) eingesetzt. SAE basiert auf Dragonfly Key Exchange, einer Passwort-authentisiertem Diffie-Hellman Schlüsselerstellung, welcher als RFC7664 (Request for Comments) von der Internet Research Task Force (IRTF) definiert wurde. SAE ist resistent gegen aktive Angriffe, passive Angriffe und offline Wörterbuchangriff. Das Endgerät oder die Endbenutzenden müssen die Kenntnis des Passwortes ohne Offenlegung nachweisen können, welches auch als Zero-Knowledge-Proof-Key Exchange bekannt ist. (D. Harkins, Ed. & Aruba Networks, 2015)

Die Passphrase wird zwischen WLAN-Komponenten nicht ausgetauscht und bietet daher einen großen Schutz vor Bruteforce Wörterburchangriffen. SAE ist sicherer als PSK, da jede Seite beweist, dass diese das Passwort kennt, ohne es offenzulegen. (David Coleman, 2021, S. 72)

Im SAE-Prozess existiert ein Commitment Message Exchange (Verpflichtungsnachrichtenaustausch) und ein Confirmation Message Exchange (Bestätigungsnachrichtenaustausch). Um jedes Drahtlosgerät zu einem einmaligen Erraten der Passphrase zu zwingen, ist das Commitment Message Exchange verantwortlich. Die korrekte Passworterratung wird mittels Confirmation Message Exchange durchgeführt. Für die Authentifizierung und den Schlüsselaustausch wird ein deterministisch berechnetes geheimes Passwort verwendet. Nach erfolgreichem Abschluss des SAE-Prozesses, wird ein einzigartiges Pairwise Master Key (PMK) abgeleitet und auf dem Wireless Accesspoint bzw. Client installiert. PMK bildet die Grundlage für den 4-Way-Handshake, um einen dynamischen verschlüsselten Schlüssel zu generieren. Die SAE-Authentifizierung wird vor der Association (Zuordnung) durchgeführt. Nach Abschluss der Association, kann der WLAN-Accesspoint und der Client einen 4-Way-Handshake durchführen. Es wird ein dynamisch generierter Schlüssel (Pairwise Transient Key, kurz PTK) erstellt, welcher den Unicast-Datenverkehr verschlüsselt, (vgl. Abbildung 11). (David Coleman, 2021, S. 72)

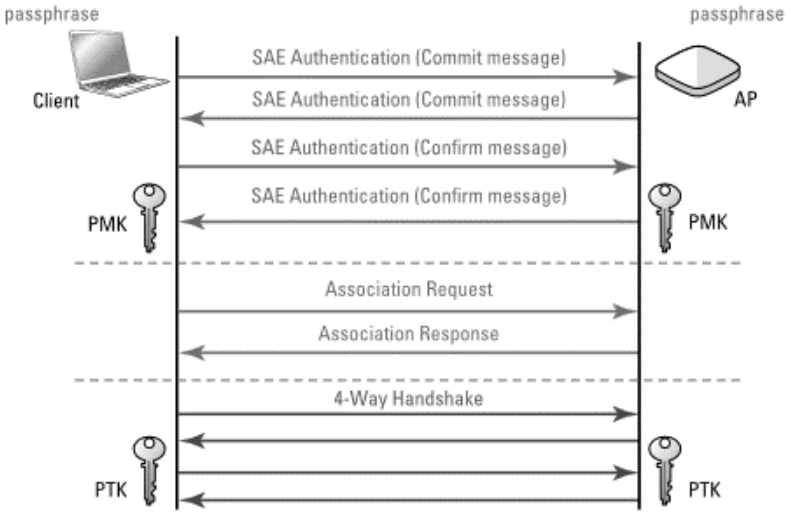

Abbildung 11 – Simultaneous Authentication of Equals (SAE) (David Coleman, 2021, S. 72)

Der oben beschriebene Vorgang, beschreibt den WPA3-Personal Only Modus für Clients die WPA3 unterstützen. Wird WPA3 vom Client nicht unterstützt, kann mittels der Rückwärtskompatibilität zu WPA2-Personal eine Verbindung zum gleichen WLAN-Accesspoint wie der WPA3-fähige Client durchgeführt werden. Die beiden Clients verwenden die gleiche Passphrase, der WPA2-Client verwendet PSK und der WPA3-Client verwendet SAE. Für den WPA3-Client muss das Protected Management Frame (PMF) aktiv sein, für den WPA2-Client jedoch nicht. Dieser Vorgang wird als WPA3-Personal Transition bezeichnet. (Wi-Fi Alliance, 2020)

2.4.3 WPA3-Enterprise

Um das Sicherheitslevel in Unternehmen oder kritischen Bereichen nicht zu verringern, wird weiterhin 802.1x/EAP für die Authentifizierung empfohlen. 802.1x ist ein Standard zur Authentifizierung der das Protokoll Extensible Authentication Protocol (EAP) verwendet. Die Authentifizierung der Clients wird mittels eines Radiusservers durchgeführt. WPA3-Personal ist eher für den heimischen Gebrauch oder Unternehmen in Betracht zu ziehen, die aktuell WPA2 verwenden. WPA2 mit 802.1x/EAP bietet fast die gleiche Sicherheit, wie WPA3-Enterprise. (David Coleman, 2021, S. 73)

Für sensible, sicherheitskritische Umgebungen bietet WPA3-Enterprise einen optionalen 192-Bit-Sicherheitsmodus an. Es wird das 256-Bit-Galois/Counter-Protokoll (GCMP) verwendet, um eine authentifizierte Verschlüsselung bereitzustellen. Zur Schlüsselableitung und Schlüsselbestätigung kommt 384-Bit-Hashed Message Authentication Mode (HMAC) mit Secure Hash-Algorithm (HMAC-SHA384) zum Einsatz. Elliptic Curve Digital Signature Algorithm (ECDSA) mit einer elliptischen 384-Bit-Kurve für die Authentifizierung und Elliptic Curve Diffie-Hellman (ECDH) für die Schlüsselerrichtung. (Wi-Fi Alliance, 2021)

2.4.4 Enhanced Open

Das von der Wi-Fi Alliance Enhanced Open zertifizierte Verfahren, verbessert den Datenschutz in öffentlichen Netzwerken. Die Zertifizierung basiert auf dem Opportunistic Wireless Encryption (OWE) Standard von der IETF mit der Kennung RFC8110. OWE unterstützt Elliptic Curve Cryptography (ECC) und Finite-Field-Kryptographie (FFC) als Kryptographieverfahren. (D. Harkins, Ed. u. a., 2017)

Unverschlüsselte und offene WLANs sind bei WLAN-Provider sehr stark verbreitet und bieten keinerlei Schutz den Benutzenden dieser Services an. Diese Netzwerke sind daher beliebte Angriffsziele von Hacker*Innen. In dem Glauben, dass eine PSK-Verschlüsselung sicherer ist als ein offenes Netzwerk, wurden etliche Zugänge für die Benutzenden erschwert, da diese ein Passwort für den Zugriff eingeben mussten. Wie in Kapitel 2.4.2 beschrieben, kann der 4-Way-Handshake von Hacker*In beobachtet und ausgelesen werden. Ist der Angriff schon erfolgt, besteht die Möglichkeit, ein Deauthenticate Frame an einen verbundenen WLAN-Client oder an den WLAN-Accesspoint zu senden. Dieser resetiert den 4-Way-Handshake und definiert einen neuen Schlüssel. (D. Harkins, Ed. u. a., 2017)

Bei jedem Benutzenden des WLAN, wird eine einzigartige individuelle Verschlüsselung zwischen Client und WLAN-Accesspoint durchgeführt. Zuerst wird die Authentifizierung und die Assoziation durchlaufen, abschließend generiert der 4-Way-Handshake-Prozess die Schlüssel für die Verschlüsselung. Ein Vorteil des Enhanced Open ist, dass die Clients kein Passwort vor dem Einloggen ins Netzwerk eingeben müssen. Der Datenschutz wird aufgrund der Verschlüsselung der Data Frames in 802.11 gewährleistet, sowie böswillige Abhörangriffe abgewehrt werden. (David Coleman, 2021, S. 74–75)

Enhanced Open hat keine Authentisierung und ist daher empfindlich gegen Man-in-the-Middle Attacken mittels Fake WLAN-Accesspoints. Nach einem erfolgreichen Verbindungsaufbau zwischen WLAN-Accesspoints und Clients ist die Verbindung fälschungssicher.

3 Mobilfunk der fünften Generation

In Kapitel 2 wurde die Drahtlostechnologie WLAN und deren technologischen Verbesserungen inklusive des Sicherheitsaspekts beschrieben. Dieses Kapitel beschäftigt sich mit der Drahtlostechnologie Mobilfunk und seinen technologischen Verbesserungen. Zunächst werden die Grundlagen samt der Evolution erläutert. Anschließend wird der neue Mobilfunkstandard 5G inklusive seiner Sicherheitsansätze und der Weiterentwicklungen des Standards beschrieben.

3.1 Grundlagen des Mobilfunks

Ursprünglich bestanden die ersten drahtgebundenen Fernsprechnetze in einem Public Switched Telephone Network (PSTN) zwischen zwei Gesprächspartnern auf einer analogen Basis. Für den analogen Kommunikationsablauf existieren drei verschiedene Phasen. An erster Stelle wird die Verbindung aufgebaut, danach werden die Nutzdaten übertragen und zuletzt wird die Verbindung nach dem Telefonat abgebaut. (Trick, 2020, S. 4)

Als Grundlage der analogen Sprachübertragung dient das leitungsvermittelnde Kommunikationsnetz (Circuit Switching). Beide Gesprächspartner besitzen eine exklusive Punkt-zu-Punkt Verbindung. Die Signale werden nach der erfolgreichen Verbindung übertragen und zwischen den Teilnehmenden ausgetauscht. Nach Ende des Gesprächs ist die Verbindung wieder frei. Im Mobilfunk und im Festnetz ist diese Vorgehensweise identisch. Die analogen Kanäle wurden im Laufe der Zeit digitalisiert. In Deutschland fand die Digitalisierung Mitte der 80er Jahre statt und es wurden die ersten ISDN-Anschlüsse (Integrated Services Digital Network) eingeführt. Erstmals wurde die Sprache zwischen Gesprächspartnern digital übertragen. (Sauter, 2015, S. 2)

Circuit Switching kommt im ersten digitalen Mobilfunknetzen (2G) zum Einsatz (,vgl. Kapitel 3.2). Circuit Switching ist eine verbindungsorientierte Kommunikation mit physikalisch geschalteten Nutzdatenkanälen. Die Nutzdaten besitzen eine fixe Bitrate (64 kbit/s), welche in zeitlich verschachtelten Zeitschlitzen (Timeslots) mit einer festen Länge (8 Bit) zusammengefasst in einem Rahmen übermittelt werden. Bei 32 Timeslots zu 64 kbit/s, können 2,048 MBit/s übertragen werden. (Trick, 2020, S. 8)

2008 kamen die regionalen Standard-Organisationen aus Europa, Amerika und Japan zusammen und gründeten die Third-Generation Partnership Project (3GPP). Dies war ein wichtiger Meilenstein der erfolgreichen mobilen Kommunikation weltweit. Die Interoperabilität zwischen unterschiedlichen Geräten und den verschiedenen Mobilfunkanbietenden in der ganzen Welt wurde geschaffen. Aufgrund neuer Anforderungen der Services und der Weiterentwicklungen der technologischen Spezifikationen, werden diese fortlaufend von 3GPP standardisiert. (Dahlman u. a., 2021, S. 2–3)

3.1.1 Definition von Mobilfunkbetreibenden

„Ein Mobilfunknetzbetreiber (Mobile Network Operator, Abk.: MNO) ist ein Unternehmen, das ein öffentliches Mobilfunknetz betreibt und darauf Dienstleistungen für Privat- und Geschäftskunden anbietet. Zu diesem Zweck beantragt oder erwirbt (z. B. mittels einer Versteigerung) diese Telefongesellschaft bei staatlichen Stellen eine Sendelizenz. Anschließend baut der Lizenznehmer eine Infrastruktur auf (heute in den allermeisten Fällen ein GSM-, UMTS- oder ein LTE-Netz), die ein der Lizenz entsprechendes bestimmtes geographisches Gebiet abdeckt. Die zur Verfügung gestellten Dienste werden entweder mit einer Prepaid-Karte oder mittels einer monatlichen Rechnung (Postpaid), die meistens auch eine Grundgebühr beinhaltet, abgerechnet“ (DBpedia, 2021).

Wie in Kapitel 2.1.3 beschrieben, existieren auch bei den Mobilfunkbetreibenden verschiedene Vergütungsmethoden. Den Nutzer*Innen des Mobilfunks steht es frei, welche Variante sie auswählen möchten. Anders als bei WLAN, müssen die Mobilfunkbetreibenden Sendelizenzen erwerben, da diese in lizenzierten Frequenzbändern fungieren (, vgl. Kapitel 3.1.2).

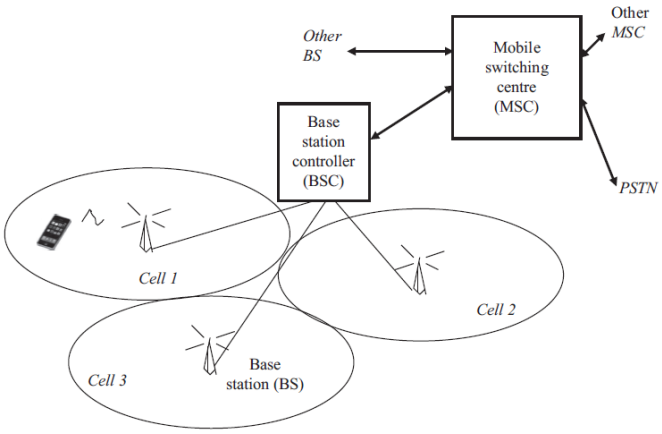

Abbildung 12 - Konzept eines Mobilfunknetzes (Valdar, 2017, S. 22)

In einer Funkzelle (engl. Cell) sind die Endgeräte mit einer Basisstation (engl. Base station, kurz BS) verbunden. Das Zugangsnetzwerk (engl. Access Network, kurz AN) besteht aus mehreren Funkzellen, welche in einem Umkreis zwischen einem bis zehn Kilometer aufgestellt sind. Frequenzen und Funkkanäle werden für die Telefonate der Endgeräte vorbelegt und bei aktiven Telefonaten an die Gesprächsteilnehmenden durch den Basisstationskontroller (engl. Base station controller, kurz BSC) weitergeleitet. Basisstationskontroller bedienen mehrere Funkzellen und sind entweder per Glasfaser oder Punkt-zu-Punk Mikrowellen Funksystemen an Basisstationen angebunden. Diese sind mit einer hohen Übertragungsrate verbunden, um den Datenverkehr abzuarbeiten. Innerhalb einer Funkzelle kann sich das Endgerät problemlos bewegen. Wenn das Endgerät am Rande einer Funkzelle mit einer schwachen Signalstärke verbunden ist oder es sich in eine andere Funkzelle begibt, so wird dies vom BSC erkannt und eine Übergabe zur nächsten Funkzelle durchgeführt. Die Übergabe wird ohne eine Unterbrechung bei einem aktiven Telefonat durchgeführt. Sollte in der neuen Funkzelle der Funkkanal belegt sein, wird das Telefonat abgebrochen. Authentifizierung, Vermittlung der Mobilfunkgespräche und Terminalstandortverwaltung werden mit Hilfe der Mobilfunkvermittlungsstelle (engl. Mobile switching centre, kurz MSC) durchgeführt (‚vgl. Abbildung 12). (Valdar, 2017, S. 22–23)

3.1.2 Mobilfunkfrequenzband und deren Regulierung

In der Vergangenheit waren die Frequenzbänder für die erste und zweite Mobilfunkgeneration bei den Frequenzen zwischen 800 MHz und 900 MHz vergeben. Das 2 GHz-Band kam bei der dritten Generation in Verwendung. Neue und bisher ungenutzte Frequenzbänder werden für neue Mobilfunkgenerationen, wie beispielsweise 4G und 5G freigeben. Bestehende und schon genutzte Frequenzbänder von anderen Mobilfunkgenerationen kommen in den neueren Generationen zum Einsatz. (Dahlman u. a., 2021, S. 26)

Die Festlegung der Frequenzbänder für verschiedene Funkdienste wird von der International Telecommunication Union (ITU) im Rahmen der WRC (World Radiocommuncation Conference) beschlossen. Angesichts der knappen Auswahl an Frequenzspektren, ist diese Arbeit ein wichtiger Bestandteil für die Vergabe von Lizenzen in den länderspezifischen Regulationen. (Trick, 2020, S. 129)

Aufgaben der ITU sind die Zuweisungen der globalen Funkfrequenzen und der Satellitenlaufbahnen, zusätzlich werden technische Standards entwickelt. Die ITU ist ein integraler Bestandteil der Vereinten Nationen. Deren Ziel ist es, die Infrastruktur in unterversorgten Gemeinden zu verbessern und das Recht der Menschen auf Kommunikation zu fördern. (Penttinen, 2015, S. 23–24)

Es gibt seitens 3GPP eine Unterteilung in nieder- und höherfrequenteren Frequenzbereichen (Trick, 2020, S. 129):

- **Frequency Range 1 (FR1):** Liegt im Frequenzbereich zwischen 410 und 7125 MHz, und umfasst den bisherigen 2G- bis 4G-Frequenzbereich. Im niederfrequenten Frequenzbereich können große Reichweiten erzielt werden und eine Durchdringung von Funkhindernissen wie beispielsweise Hauswänden ist möglich. FR1 eignet sich ideal für IoT-Geräte und Maschinenkommunikation (,vgl. Tabelle 2).
- **Frequency Range 2 (FR2):** In FR2 liegt der Frequenzbereich zwischen 24,25 und 52,6 GHz und spezifiziert ganz neue Frequenzspektren für den Mobilfunk. Der Einsatz wird im lokalen Bereich verwendet, da nur kurze Reichweiten möglich sind und starke Beeinträchtigungen durch Hindernisse, wie beispielsweise Nebel, Niederschlag und auch durch den Mensch auftreten können (,vgl. Tabelle 3).

Die möglichen Frequenzbereiche sind von 3GPP per Standard vorgegeben, aber die nationalen Regulierungsbehörden stellen den Mobilfunkbetreibenden die lizenzierten Frequenzbereiche zur Verfügung. In Österreich ist Telekom-Control-Kommission (TKK) innerhalb der Rundfunk und Regulierungs-GmbH (RTR) für die Vergabe der lizenzierten Frequenzbereiche verantwortlich. Im März 2019 fand die erste Versteigerung von 5G-Spektren in Österreich statt. Es gab eine landesweite Vergabe an drei Mobilfunkbetreibende und auch regionale Zuweisungen an vier Provider. Zugewiesen wurden die Frequenzbereiche zwischen 3,4 und 3,6 GHz (regional) und zwischen 3,6 GHz und 3,8 GHz (landesweit).

Die nachfolgende Tabelle 2 und Tabelle 3, illustrieren die Frequenzbänder gemäß 3GPP für den 5G-Standard. 5G-Funkübertragunstechnik NR (New Radio) und der Uplink- (UL) bzw. der Downlinkbereich (DL) vom Endgerät zur BS sind aufgeschlüsselt.

NR Frequenzband	UL Bereich [MHz]	DL Bereich [MHz]	Regionen
N1	1920 – 1980	2110 – 2170	Europa, Asien
N2	1850 – 1910	1930 – 1990	Amerika (Asien)
N3	1710 – 1785	1805 – 1880	Europa, Asien (Amerika)
N5	824 – 849	869 – 894	Amerika, Asien
N7	2500 – 2570	2620 – 2690	Europa, Asien
N8	880 – 915	925 – 960	Europa, Asien
N20	832 – 862	791 – 821	Europa
N28	703 – 748	758 – 803	Asien/Pazifik
N38	2570 – 2620	2570 – 2620	Europa
N41	2496 – 2690	2496 – 2690	US, China
N50	1432 – 1517	1432 – 1517	
N51	1427 – 1432	1427 – 1432	
N66	1710 – 1780	2110 – 2200	Amerika
N70	1695 – 1710	1995 – 2020	
N71	663 – 698	617 – 652	Amerika
N74	1427 – 1470	1475 – 1518	Japan
N75	-	1432 – 1517	Europa
N76	-	1427 – 1432	Europa
N77	3300 – 4200	3300 – 4200	Europa, Asien
N78	3300 – 3800	3300 – 3800	Europa, Asien
N79	4400 – 5500	4400 – 5500	Asien
N80	1710 – 1785	-	
N81	880 – 915	-	
N82	832 – 862	-	
N83	703 – 748	-	
N84	1920 – 1980	-	

Tabelle 2 - FR1-Frequenzbänder gemäß 3GPP-Standard (Anlehnung an Dahlman u. a., 2021, S. 33–34)

NR Frequenzband	UL und DL Bereich [MHz]	Regionen
N257	26500 – 29500	Asien, Amerika (Global)
N258	24250 – 27500	Europa, Asien (Global)
N259	39500 – 43500	Global
N260	37000 – 40000	Amerika (Global)
N261	27500 – 28350	Amerika

Tabelle 3 - FR2-Frequenzbänder gemäß 3GPP-Standard (Anlehnung an Dahlman u. a., 2021, S. 34)

3.2 Evolution des Mobilfunkstandards

Die erste Generation des Mobilfunks (1G), wurde im Jahr 1978 von der Nippon Telephone and Telegraph (NTT) in Tokio vorgestellt und ist analog basierend. Advanced Mobile Phone System (AMPS) und Total Access Communication Systems (TACS) waren die beliebtesten analogen zellularen Architektursysteme und verwendeten Frequency Division Multiple Access (FDMA) zur Sprachübertragung. (Prasad, 2014, S. 1) Beim FDMA-Modulationsverfahren sind die Frequenzbänder in Blöcke unterteilt. Die Sende- und Empfangsfrequenzblöcke sind gepaart und belegen diesen über den gesamten Zeitraum während der Übertragung. (Valdar, 2017, S. 257–258)

Anfang der 1990er-Jahren begann die Einführung des ersten digitalen Mobilfunknetzes, das sogenannte 2G (die zweite Generation). 2G nutzt die GSM-Technik (Global System for Mobile Communications), welche ebenfalls auf der analogen Technik beruht. Diese besteht aus einem leitungsvermittelten Core-Network (CN) GSM und einem Access Network (AN). Das bestehende CN ist um einen paketvermittelten Teil, das GPRS (General Packet Radio Service) erweitert und ermöglicht die Nutzung des Internetprotokolls. Mittels der EDGE-Technologie (Enhanced Data Rates for GSM Evolution) ist es nun möglich, IP mit einer mittleren Bitrate zu transportieren. Dies setzt aber die Migration des AN voraus. (Trick, 2020, S. 1–2)

3G, die dritte Generation des Mobilfunks wurde zu Beginn der 2000er-Jahre veröffentlicht. Aufgrund der Einführung von HSPA (High-Speed Packet Access) war es das erste Mal möglich, schnellen Internetzugang zu gewähren (Dahlman u. a., 2021, S. 1). Zuvor wurde noch UMTS (Universal Mobile Telecommunications System) eingeführt und dies brachte unter der Nutzung von der W-CDMA-Technik (Wideband-Code Division Multiple Access) ein leistungsfähigeres AN und deutlich höhere Bitraten. (Trick, 2020, S. 2) W-CDMA besitzt eine effiziente Nutzung des verfügbaren Spektrums. Mittels Cell breathing variiert die Sendeleistung der Basisstationen je nach Bedarf der momentanen Verkehrsdichte. (Valdar, 2017, S. 272)

Heutzutage ist die vierte Generation (4G) neben den oben angeführten Vorgängerversionen im Einsatz. Mittels LTE (Long Term Evolution) wurde eine Zugangsnetztechnik standardisiert, die pro Funkzelle 100 MBit/s ermöglicht. Erstmalig wird die ganze Telefonieübertragung per IP als Übermittlungsprotokoll durchgeführt. Veröffentlicht wurde der LTE-Standard im Jahr 2008. (Trick, 2020, S. 30–31)

Im Gegensatz zu den Entwicklungen der vorhergehenden Mobilfunkgenerationen unterscheidet sich die Entwicklung der fünften Mobilfunkgeneration (5G) zu den anderen deutlich. Die Entwicklung wurde von vielen Anwendungsfällen getrieben und nicht von der technischen Perspektive wie bei den bisherigen. Aus den verschiedenen Anwendungsfällen wurden die Anforderungen abgeleitet und anschließend für die bevorstehende Umsetzung die Technik spezifiziert (Trick, 2020, S. 104). Ein vertiefender Einblick in den Mobilfunkstandard 5G erfolgt in Kapitel 3.3.

3.3 Der 5G-Mobilfunkstandard

Wie bereits in Kapitel 3.2 kurz erwähnt, waren die verschiedenen Anwendungsfälle für die Entwicklung der fünften Mobilfunkgeneration verantwortlich. Trick (2020, S. 109) beschreibt die Hauptanforderungen der Anwendungsfälle an den 5G-Standard folgendermaßen:

- 1 Gbit/s bis 10Gbit/s Datenraten für die virtuelle Realität bei Büroanwendungen
- Beispielsweise in einem Stadion 9 GByte/Stunde Datenvolumen in der Hauptverkehrsstunde und Datenvolumen 500 GByte/Monat in einem dichtbesiedelten Gebiet
- Für Verkehrsanwendungen Ende-zu-Ende Latenzzeiten unter 5 ms
- Für Sensoren und Aktoren eine Batterielaufzeit von 10 Jahren
- Bis zu 300.000 verbundene Geräte pro Access Point
- Energieverbrauch und Kosten wie bei 4G
- Sehr hohe Verfügbarkeit (99,999%) für Smart Grid- und Verkehrsanwendungen

Aus den obengenannten Hauptanforderungen sind drei verschiedene 5G-Serviceklassen entstanden (Osseiran, 2016, S. 32):

- **Erweiterte mobile Breitbandkommunikation (Extreme Mobile BroadBand, kurz xMBB):** Garantiert hohe Datenraten und niedrige Latenzen bei sehr weiten Reichweiten. Zusätzlich bietet xMBB ein einheitlicheres Erlebnis im gesamten Abdeckungsbereich und eine gleichmäßige Leistungsverringerung bei steigender Anzahl der Nutzer*Innen.
- **Massenweise Kommunikation von Maschinen (Massive Machine-Type Communication, kurz mMTC):** Bietet eine drahtlose Konnektivität für eine Vielzahl von netzwerkfähigen Geräten mit einer effizienten Übertragung kleinerer Datenmengen an. Die großflächige Abdeckung ist wichtiger als die Datenrate.

- **Extrem zuverlässige Maschinen Kommunikation (Ultra-reliable Machine-Type Communication, kurz uMTC):** Sorgt für eine ultrazuverlässige Kommunikationsverbindung mit einer geringen Latenz für Netzwerkdienste mit extremen Anforderungen wie beispielsweise beim autonomen Fahren. Die Zuverlässigkeit und die geringe Latenz sind hier priorisiert.

Weltweit gab es zahlreiche Forschungsprojekte zur fünften Generation. Ebenso die von der Europäischen Kommission und der ICT-Industrie (Information and Communication Technology) initiierten Projekte. Im Rahmen einer Studie von 3GPP, wurden die bisherigen Ergebnisse, Erfahrungen und Standardisierungsarbeiten für 74 Anwendungsfälle in fünf Kategorien der bisherigen Forschungsprojekte zusammengefasst. Erweiterte mobile Breitbandkommunikation, Zeitkritische Kommunikation, Massenweise Kommunikation von Maschinen, Netzbetrieb und Verbesserung der Fahrzeug-zu-X Kommunikation bilden die fünf Kategorien (, vgl. Abbildung 13). (Trick, 2020, S. 112)

Abbildung 13 - Anwendungskategorien und Use Case für 5G (Anlehnung an Trick, 2020, S. 113)

Die nachfolgende Übersicht (, vgl. Tabelle 4) zeigt laut Trick (, 2020, S. 113–114) vier verschiedene Anwendungskategorien mit den resultierenden Anforderungen im User*Innenbereich.

Kategorie	Generelle Anforderungen
eMBB (Enhanced Mobile Broadband)	• Sehr hohe Datenraten, bis zu 10 Gbit/s pro Nutzer • Geringe Verzögerungen • Hohe Verkehrsdichte, pro km² im Tbit/s-Bereich • Hohe Verbindungsdichte, bis zu 2500 Endgeräte/km² • Mobilität von 0-500 km/h • Keine besonderen Anforderungen an Verfügbarkeit und Positionsgenauigkeit
CriC (Critical Communications) Bzw. **URLLC** (Ultra-Reliable and Low Latency Communications)	• Keine besonderen Anforderungen an Datenrate und Mobilität • Sehr geringe Verzögerungen, < 1 ms Ende-zu-Ende • Sehr hohe Verfügbarkeit • Hohe Verbindungsdichte, < 1000 Endgeräte (z.B. Sensoren)/km² • Sehr hohe Positionsgenauigkeit, ≤ 10 cm
MIoT (Massive Internet of Things) Bzw. **mMTC** (Massive Machine Type Communications)	• Keine besonderen Anforderungen an Datenrate, Verzögerungszeit, Verfügbarkeit und Mobilität • Effiziente Kommunikation, da Endgeräte mit rel. geringen HW-Ressourcen und/oder Batteriebetrieb • Sehr hohe Verbindungsdichte, bis zu 1 Mio. Endgeräte (z.B. Sensoren)/km² • Hohe Positionsgenauigkeit, ≤ 50 cm
eV2X (Enhancement of Vehicle-to-Everything)	• Mittlere Datenrate, im Bereich 10 Mbit/s • Sehr geringe Verzögerungen, ≤ 1ms Ende-zu-Ende • Sehr hohe Verfügbarkeit, nahe 100% • Mittlere Verkehrsdichte • Mittlere Verbindungsdichte, > 10.000 Fahrzeuge • Hohe Mobilität, bis 500 km/h • Sehr hohe Positionsgenauigkeit, ≤ 10 cm

Tabelle 4 - Generelle Anforderungen an den Anwendungskategorien (Anlehnung an Trick, 2020, S. 113–114)

3.3.1 Schlüsselfaktoren für 5G

Im September 2015 veröffentlichte der Radiosektor der ITU-R (International Telecommunication Union, Radiocommunication Sector) seine wegweisende IMT-Vision (International Mobile Telecommunications) für 2020. IMT-2020 beinhaltet etliche Use Case und die verschiedenen 5G-Serviceklassen (,vgl. Kapitel 3.3). (Trick, 2020, S. 110)

Dahlman u. a. (, 2021, S. 17–19) fasst die oben genannten Anwendungsfälle (, vgl. Abbildung 13) in acht Schlüsselfunktionen von der ITU-R grafisch zusammen und setzt diese mit der IMT-Advanced in Vergleich. IMT-Advanced bildet die Vorgabe für 4G.

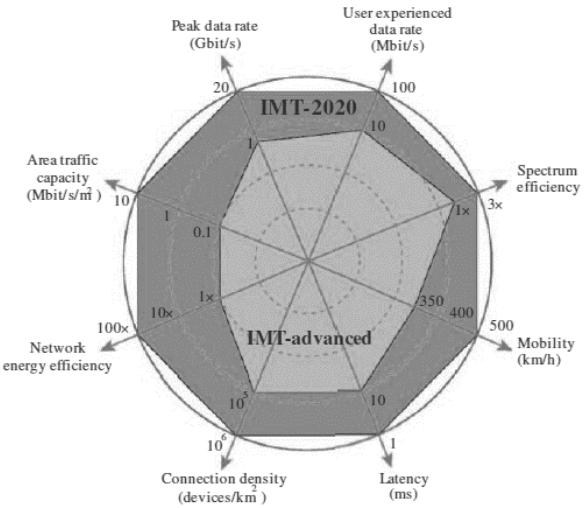

Abbildung 14 - Schlüsselfaktoren laut ITU-R (Dahlman u. a., 2021, S. 16)

Die Spitzendatenrate (Peak Data Rate) pro Nutzer*In bei idealen Bedingungen liegt bei bis zu 20 Gbit/s. In städtischen und vorstädtischen Gebieten gilt eine Zieldatenrate von 100 Mbit/s und in Innenräumen in der Nähe von 5G-Hotspots 1Gbit/s zu erreichen. Diese wahrgenommene Datenrate von den Nutzenden (User experienced data rate) wird in großen Abdeckungsbereichen für die Mehrheit der Nutzer*Innen erreicht. Die Spektrumeffizienz ist ein wesentlicher Parameter für die Dimensionierung von Netzen, diese wird in durchschnittlichen Datendurchsatz pro Hz und pro Zelle angegeben. Es gilt die Spektrumeffizienz bei 5G im Vergleich zu 4G dreifach zu erhöhen. Eine 100-fache Steigerungen der Verkehrskapazität (Area Traffic Capacity) gegenüber 4G ist angestrebt. In Bezug auf die Energieeffizenz bei Funkzugängen (Network Energy Efficiency), darf der Energieverbrauch nicht höher werden. Für die Anwendungskategorie URLLC geht man von einer 10-fachen Reduzierung der Latenzzeit (Latency) aus. Insbesondere die Mobilität bei Hochgeschwindigkeitszügen die eine Geschwindigkeit von 500 km/h erreichen oder auch bei kritischen Fahrzeugkommunikationen, ist auf eine niedrige Latenz zu achten.

3.3.2 Network Function Virtualisation (NFV)

Im Prinzip wird die Netzfunktion von dedizierten und teuren Hardwarekomponenten auf Software Appliances implementiert bzw. virtualisiert, die beispielsweise in einer Cloud-Umgebung laufen. Hierdurch ist es für die Mobilfunkbetreibende einfacher auf neue Anforderungen zu reagieren (, vgl. Tabelle 4) und neuere Dienste schneller auf den Markt zu bringen. Benötigte Ressourcen wie beispielsweise Netzwerk, Datenspeicher und Rechenleistung, können unverzüglich und skaliert zur Verfügung gestellt werden. Liyanage (, 2018, S. 45) fasst die Virtualisierung der Netzfunktionen grafisch zusammen:

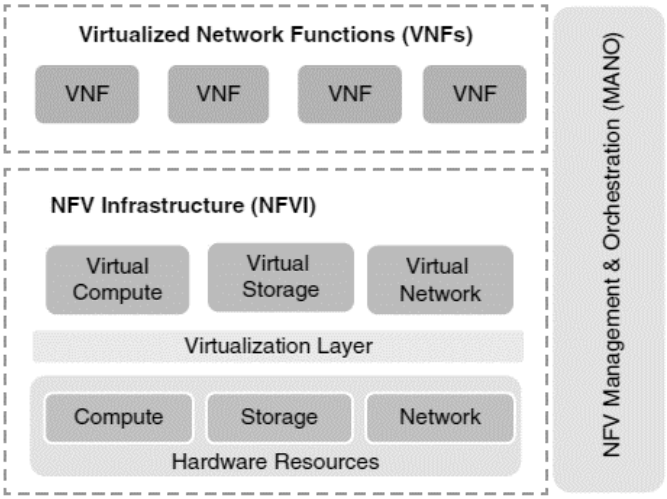

Abbildung 15 - Network Function Virtualisation (NFV) (Liyanage u. a., 2018, S. 45)

Der Einsatz von NFV bringt den Mobilfunkbetreibenden zahlreiche Vorteile (Trick, 2020, S. 71):

- Geringere Hardwarekosten
- Hohe Skalierbarkeit
- Mehrere Mobilfunkbetreibende können die gleiche Hardware nutzen
- Software-Upgrades werden vereinfacht
- Netzkonfiguration in Echtzeit an den aktuellen Verkehr anpassen
- Homogene Hardware-Plattform

3.3.3 Software Defined Networking (SDN)

Das Migrieren von Netzfunktionen und dynamischen Instanziierungen der NFV, bringen neue Anforderungen an Ethernet bzw. IP-Transportnetze. In bestimmten Netzsituationen wie beispielsweise eine Verkehrslastspitze, müssen Datenpakete und Datenflüsse, dynamisch verlagert und/oder neu skaliert werden. SDN wird als die Schlüsseltechnologie im neuen Mobilfunkstandard 5G gesehen. (Trick, 2020, S. 78-79)

Ein SDN zeichnet sich durch die Trennung der Applikationsebene (Application Layer), der Datenebenen (Infrastracture Layer) von der Steuerungsebene (Control Layer) (vgl. Abbildung 16). Aufgrund der Trennung der Steuerungs- und Datenebene, kann die Netzwerkinfrastruktur nach Bedarf aufgebaut werden. Dadurch kommt es zu einer Steigerung der Effizienz von den Ressourcen und diese bildet die Basis für Network-as-a-Service (NaaS). (Liyanage u. a., 2018, S. 44)

Der SDN-Controller ist die zentrale logische Steuerung, welche über OpenFlow die eigentliche Protokollverarbeitung, also was mit einem Flow geschieht, entscheidet. Ein Flow ist eine Folge von zusammengehörenden Datenpaketen. Betreffend Flexibilität und Kosten, steuert ein SDN-Controller über das Southbound Interface die Netzwerkgeräte in der Datenebene. SDN-Applikationen können über API-Schnittstellen (Appplication Programming Interface) den SDN-Controller programmieren. Fast in Echtzeit können kurzfristige Netzdienste nach Bedarf implementiert werden. Beispiele für SDN-Applikationen sind Switching, Routing, Load Balancing und Security. (Trick, 2020, S. 80)

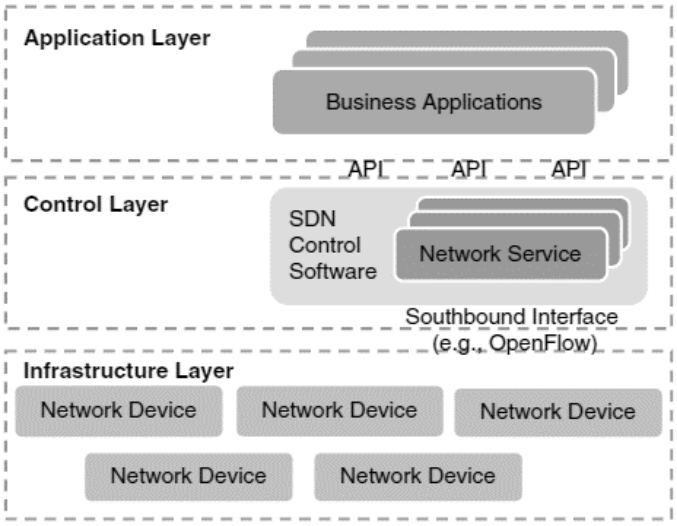

Abbildung 16 - SDN-Architektur (Liyanage u. a., 2018, S. 45)

In Anbetracht der Flexibilität, Offenheit und Programmierbarkeit ist SDN der beste Technologiekandidat für die Entwicklung von 5G-Netzen. Mobilfunkbetreibende werden den Lebenszyklus neuer Dienste und Innovationen daher auf dem Markt verkürzen.(Liyanage u. a., 2018, S. 44)

3.3.4 Zugangsnetze der fünften Generation

Der Mobilfunkstandard 4G verwendet das gleiche Modulationsverfahren OFDMA im UL und DL in bestimmten Frequenzbereichen, wie der Wireless Standard Wi-Fi6 (,vgl. Kapitel 2.3.1). Allerdings kommt beim 5G-Mobilfunkstandard das Filtered-OFDM (F-OFDM) zum Einsatz. F-OFDM ist stark an das OFDM angelehnt, (vgl. Kapitel 2.3.1). Bei bestimmten Unterfrequenzen werden zusätzliche Filter zur Anpassung an verschiedene Anwendungsszenarien gelegt. Die Dauer eines zyklischen Präfixes wird in Abhängigkeit vom Unterträgerfrequenzabstand gewählt. Zur Auswahl stehen 15, 30, 60, 120 und 240 kHz. Im Frequenzband FR1 werden die Unterfrequenzabstände bis 60 kHz und im

Frequenzband FR2 ab 60kHz verwendet. Der Unterschied zu Wi-Fi6 ist, dass ein Modulationsverfahren bis zu 256-QAM zum Einsatz kommt. (Trick, 2020, S. 154–156)

In Anbetracht der hohen Datenrate und der Kapazität des 5G-Mobilfunkes, sind höhere Frequenzen notwendig um das Ziel zu erreichen (‚vgl. Kapitel 3.1.2). Als beste technologische Lösung kommt die Millimeterwellenkommunikaton (mmWave) zum Zug. Die Wellenlänge beträgt zwischen 1 mm und 10 mm im Frequenzbereich zwischen 30 bis 300 GHz. Bislang kam diese Technologie nur in Innenräumen zum Einsatz, da es bei höheren Frequenzen zu hohen Ausbreitungsverlusten kommt. (Liyanage u. a., 2018, S. 38)

Verbesserung der spektralen Effizienz und die Verdichtung der Netze durch kleine Zellen, ermöglichen es anhand mmWave dieses zu erreichen. Durch die Nutzung von mmWave wird die Verfügbarkeit großer zusammenhängender Frequenzblöcke und durch die Einführung von Beamforming, die Spektrumeffizienz gesteigert (Osseiran, 2016, S. 137). Jedes 5G-Mobilfunksystem im Millimeterwellenbereich benötigt Beamforming mit adaptiven Antennengruppen, da es ansonsten zu einem großflächigen Verlust der Frequenzen kommt. (Osseiran, 2016, S. 139)

Massive MIMO beinhaltet mehrere Antennensystem für das Senden und/oder Empfangen der Funksignale. Darum kann eine höhere Datenrate übertragen werden. Wie auch in Wi-Fi6 ist MU-MIMO ein Bestandteil des 5G-Standards (‚vgl. Kapitel 2.3.2). Der sogenannte Gruppengewinn, welches durch Senden und/oder Empfangen mit mehreren Antennen erreicht wird, impliziert eine größere Empfangsleistung. Eine höhere Funkkanaldämpfung wird durch die größere Empfangsleistung überbrückt gegenüber einzelnen Antennensystemen. Störende Intersymbolinterferenzen, welche durch Reflexionen und Abschattungen auftreten, können mithilfe der MIMO-Technologie verringert werden. (Trick, 2020, S. 157)

In einem massive MIMO-System sind große Anzahlen (ca. 100 oder mehr) an individuellen steuerbaren Antennen enthalten. Osseiran (, 2016, S. 208) hat ein massive MIMO-System grafisch zusammengefasst. Durch die vielen Antennen können Nachrichten für mehrere Benutzer*Innen auf der gleichen Zeitfrequenz versendet, die Signale fokussiert, und/oder die Interferenzen innerhalb einer Zeile minimiert werden.

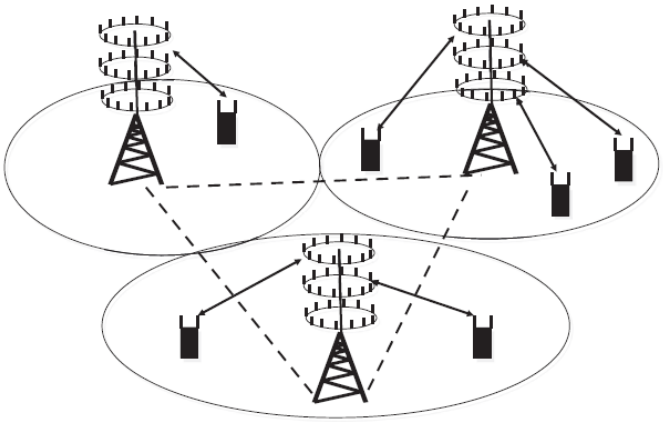

Abbildung 17 – massive MIMO-Basisstationen (Osseiran, 2016, S. 209)

3.3.5 Die Netzarchitektur der fünften Generation

Die obengenannten Anforderungen in der Einleitung (,vgl. Kapitel 3.3) und die Schlüsselfaktoren (,vgl. Kapitel 3.3.1) bringen große Herausforderungen an das 5G-Netz. Um die zum Teil extremen Anforderungen an den neuen Mobilfunkstandard 5G zu erfüllen, wird das Konzept des Service Based Architecture (SBA) eingesetzt. Das Designprinzip deckt die gesamte Anforderungspalette ab, es kommt ein anforderungsspezifisches Teilsystemen aus modularen Netzfunktionen (NF) zur Anwendung. Es existieren Module für das Access Network- (AN), die Core Network-Funktionen (CN), die Control Plane (CP) mit den Signalisierungs- und Steuerungsprotokollen und die User Plane (UP) für die Nutzdaten. Je nach Bedarf werden die Funktionsmodule zusammengestellt, kombiniert und bilden feingranulare Netzfunktionen. Netzfunktionen sind in einem Repository bereitgestellt und werden über APIs abgerufen. (Trick, 2020, S. 137)

Die 5G-Systemarchitektur sieht eine strukturelle Trennung von Hardware und Software vor. NFV, SDN und SBA bilden die Basis der 5G-Netzarchitektur und beinhalten nachfolgende Schlüsselprinzipien (ETSI TS, 2018, S. 18–19):

- Funktionstrennung von der UP und der CP, ermöglicht eine unabhängige Skalierbarkeit, die Weiterentwicklung und flexible Anwendbarkeit bei zentralen oder auch bei verteilten Standorten
- Modularisierung des Funktionsdesigns, um flexible und effiziente Netzschichten (Network Slicing) zu ermöglichen (, vgl. Kapitel 3.3.6)

- Abläufe sollten als Dienste definiert werden, damit ihre Wiederverwendung möglich ist, wo immer dies machbar ist
- Direkte Interaktion der Netzfunktion mit anderen Netzfunktionen ermöglichen, falls erforderlich. Die Architektur schließt nicht aus, dass die Verwendung einer Zwischenfunktion, welche bei der Weiterleitung von Nachrichten der Steuerungsebene notwendig ist
- Zwischen dem AN und dem CN müssen die Abhängigkeiten minimiert werden. Das konvergente CN soll mit verschiedenen AN-Typen integriert werden
- Einen einheitlichen Authentifizierungsrahmen unterstützen
- Bei zustandslosen Netzfunktionen wird die Rechenressource von der Speicherressource entkoppelt
- Unterstützung des gleichzeitigen Zugriffs auf lokale und zentralisierte Dienste. Um Dienste mit geringen Latenzen zu unterstützen, können die UP-Funktionen beim AN bereitgestellt werden
- Roaming sowohl mit geroutetem Verkehr im Heimatnetz als auch mit lokalem Breakout-Verkehr im besuchten Netz

Basierend auf den Schlüsselprinzipien und den stark divergierenden Anforderungen, muss das 5G-Netz unterschiedlichste Dienste an verschiedenen Orten bereitstellen. Die 5G-Architektur sieht eine strukturelle Trennung von Hardware und Software vor. Aufgrund der Integration der SDN und NFV-Technologien können die Aspekte der Netzfunktion, der wertsteigernde Fähigkeiten und alle Verwaltungsfunktionen zur Orchestrierung in der 5G-Netzarchitektur abgedeckt werden. (Rachid El Hattachi u. a., 2015, S. 45)

Es existieren drei verschiedene Schichten, ein E2E-Management (End-to-End) und eine Orchestrierungseinheit (,vgl. Abbildung 19). Jeder dieser Schichten besitzt ein eigenes Aufgabengebiet (Rachid El Hattachi u. a., 2015, S. 46):

- **Infrastructure resources layer:** Besteht aus physischen Ressourcen eines konvergenten fixen Mobilnetzes. Es beinhaltet eine Vielzahl an Zugangsknoten und Cloud-Knoten, welche Rechen- und Speicherleistung zur Verfügung stellen. 5G-Endgeräte als auch Netzwerknoten sind ebenfalls Bestandteil dieser Schicht. Die 5G-Endgeräte können als Relais oder auch als Rechen- bzw. Speicherleistung fungieren, da diese mehrere konfigurierbaren Funktionen haben. Demzufolge zählen diese auch als Teil der konfigurierbaren Infrastrukturressource. Die

Infrastrukturressourcen sind mittels E2E-Managements und Orchestrierungseinheiten über eine entsprechende API-Schnittstelle zugänglich.

- **Business enablement layer:** Ist eine Bibliothek, die alle notwendigen Netzfunktionen in modularen Architekturbausteinen, einschließlich der Softwaremodule realisierten Funktionen bereitstellt. Anhand des Repository werden die Funktionen an den gewünschten Ort und die notwendigen Konfigurationsparameter für bestimmte Teile des Netzes abgerufen. Dementsprechend wird auf unterschiedliche Anforderungen und spezifische Bedürfnisse am 5G-Netz reagiert.
- **Business application layer:** Enthält spezifische Anwendungen und Dienste des Mobilfunkbetreibenden, Unternehmen oder Dritten, die das Netz nutzen. Mittels der Schnittstelle zur E2E-Management und Orchestrierungseinheit, wird beispielsweise eine Network Slice (‚vgl. 3.3.6) erstellt.
- **E2E management and orchestration:** Über diese Schnittstelle sind die Anwendungsfälle und die Geschäftsmodelle an den tatsächlichen Netzschichten definiert. Alle notwendigen Konfigurationen und Infrastrukturressourcen werden per Schnittstelle verwaltet. Eigene MVNOs können über APIs ihre eigene Netzabschnitte erstellen und verwalten. Da es sich um eine Sammlung modularer Funktionen handelt, ist eine monolithische Funktionalität nicht gegeben.

Verschiedene Zugangsnetze die sogenannten RATs (Radio Access Technology), sind über das Access Network (AN) an die Infrastructure Resources Layer angebunden. (Trick, 2020, S. 145)

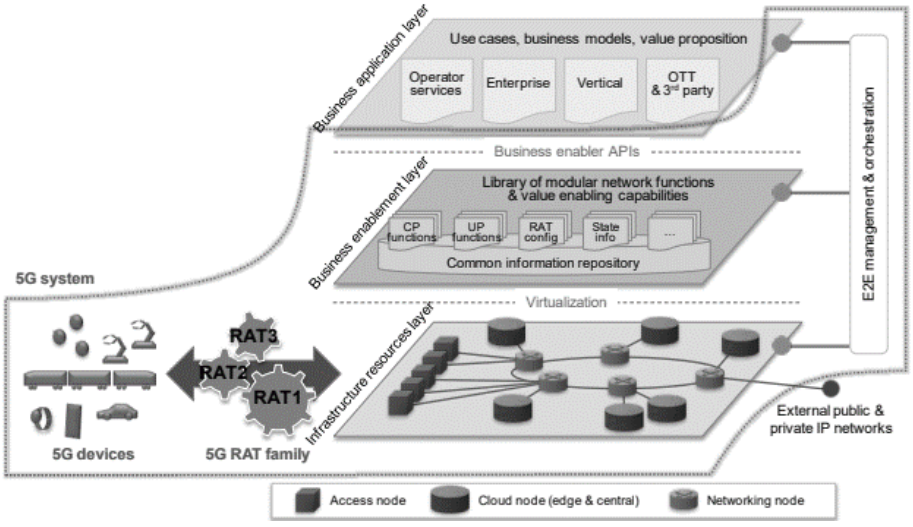

Abbildung 18 - 5G-Netzarchitektur (Rachid El Hattachi u. a., 2015, S. 45)

3.3.6 Network Slicing

Um mehrere logische Netze auf einer gemeinsamen physischen Infrastruktur zu betreiben, wird das Konzept des Network Slicing angewendet. Allgemein wird Network Slicing als eine logische Instanziierung des Netzes zwischen einer Reihe von Netzgeräten und einigen Backend-Anwendungen von Diensten für Endbenutzende beschrieben. (ETSI GR, 2017, S. 56)

Trick (, 2020, S. 183–184) beschreibt Network Slicing als Bildung von zwei oder von mehreren logischen Netzen, welche es ermöglicht mehrere Mandanten, wie beispielsweise Mobilfunkbetreibende oder MVNO (Mobile Virtual Network Operator) für verschiedene Anforderungen zu betreiben. Eine Netzwerkschicht wird für das autonome Fahren und eine andere Netzwerkschicht für eine IoT-Landschaft verwendet. Es werden logische Kommunikationsnetze mit unterschiedlichen Eigenschaften für die Endbenutzer*Innen parallel betrieben (‚vgl. Abbildung 19).

Die Zugangsnetze bestehen aus spezifischer Hardware, welche für die Übertragungstechnik verantwortlich sind. Darunter fallen Router, Switche, Rechenleistung und Speicherressourcen, welche vorzugsweise in zentralen Rechenzentren aber auch beim Zugangsnetz (Edge) platziert sind. Eine Virtualisierungsplattform in Kombination mit einer physikalischen Netzinfrastruktur bilden eine Infrastracture-as-a-Service (IaaS) für virtuelle Netzfunktionen (VNF). (Trick, 2020, S. 182–183)

Die Idee des Network Slicing basiert auf dem Konzept, dass Netzschichten die Anforderungen von verschiedenen Diensten abdecken (ETSI GR, 2017, S. 57):

- Bereitstellung der Konnektivität zwischen den Endpunkten (Terminals oder Netzgateways)
- Sofern erforderlich, die Verarbeitung des Datenverkehrs zwischen den Endpunkten
- Bereitstellung von eigenen Netz- und Dienstverwaltungsfunktionen in Echtzeit
- Bereitstellung von Betriebsunterstützungssysteme

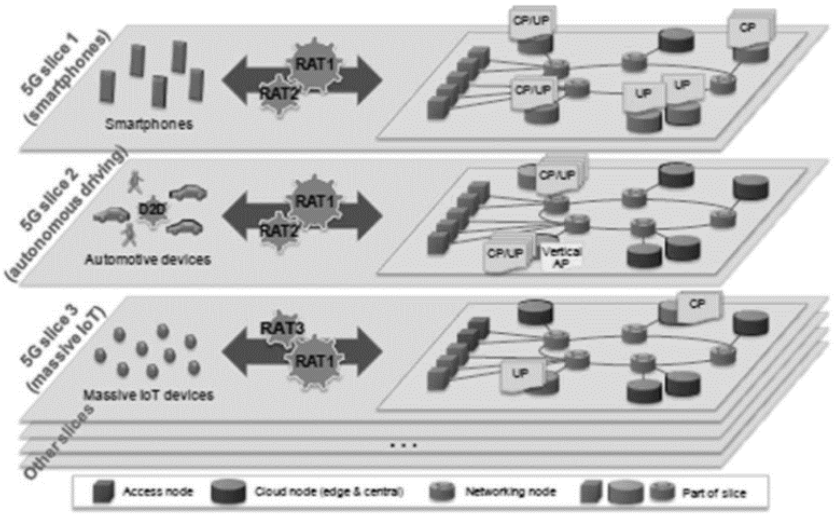

Abbildung 19 - 5G Network Slices (ETSI GR, 2017, S. 57)

3.4 Sicherheitsaspekte im 5G-Mobilfunkstandard

In Anbetracht der großen Einsatzgebiete und der unterschiedlichen Anwendungen von 5G, ist der Bedrohungsvektor sehr breit gefächert. Die Motivation den Mobilfunkstandard 5G zu bedrohen oder gar anzugreifen ist sehr hoch, da etliche Anforderungskategorien abgedeckt sind. Kriminelle Personen, organisiertes Verbrechen oder staatlich geförderte Motive können hinter den Angriffen stecken. Hacker*Innen können das Netz infiltrieren und ausspionieren. Ist der Einbruch in das System gelungen, kann ein Schaden in einem unbestimmten Ausmaß erfolgen. Betroffen können beispielsweise die Endbenutzer*Innen bzw. deren Endgeräte, Sensoren, autonome Fahrzeuge, Unternehmensnetzwerke und der Mobilfunkbetreibende sein (,vgl. Abbildung 20). Bedrohungen ans 5G-Netz bestehen aus verschiedenen Angriffsvektoren, von den Endgeräten der Benutzer*Innen bis hin zur 5G-Netzwerkinfrastruktur. Daneben existiert eine Vielzahl an unterschiedliche Bedrohungstypen. Malwares, Bots, DDoS-Attacken (Distributed Denial of Service) oder Man-in-the-Middle-Attacken, stellen einen Bruchteil der verschiedenen Bedrohungsszenarien dar. Die Sicherstellung der kompletten Komponenten ist eine große Herausforderung an den Mobilfunkstandard der fünften Generation. (Liyanage u. a., 2018, S. 66–67)

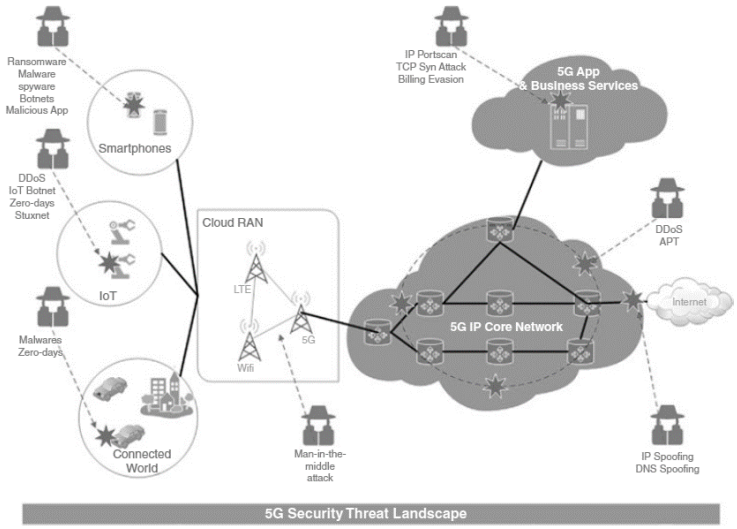

Abbildung 20 - 5G Sicherheitsbedrohungslandschaft (Liyanage u. a., 2018, S. 67)

DDoS-Attacken können den Betrieb von Geräten bei kritischen Infrastrukturen wie beispielsweise Energie, Gesundheit, Verkehr und Telekommunikation stören. Lebensbedrohliche Folgen können enormen Schaden an den Menschen und einen finanziellen Verlust hervorrufen. Bei sogenannten DDoS-Angriffen werden die physischen und die logischen Ressourcen von geografisch verteilten Standorten angegriffen, es kommt zu einer Überlastung der Dienste. (Liyanage u. a., 2018, S. 79)

Bei Man-in-the-Middle-Angriffen werden die Kommunikationswege abgefangen und dadurch die Authentifizierungsdaten erlangt. Der Inhalt des anfallenden Datenaustausch ist für den Angreifenden lesbar. (Liyanage u. a., 2018, S. 291)

Besondere Bedrohungen in den IoT-Subnetzen und -Systemen entstehen durch Botnetze aus gekaperten IoT-Endgeräten, Zero Day-Attacken, Würmern und DDos. Bei Zero Day-Attacken werden bisher unbekannte Schwachstellen ausgenützt und eine Kombination von mehreren Angriffstypen verwendet. Würmer reproduzieren sich selbst und haben das Ziel, die systemkritische Infrastruktur anzugreifen. Auf der 5G-Applikationsebene sind als Bedrohungen das Port Scanning und die Abrechnungsbetrugsversuche zu erkennen. Das 5G-Core Netzwerk ist besonders durch sogenannte APTs (Advance Persistent Threats) gefährdet. Dabei handelt es sich um komplexe Angriffsszenarien die mehrstufig unter Nutzung und Kombination mit mehreren komplexen und verschleierten Mechanismen ausgeführt werden. Diese Angriffe sind schwer zu erkennen, da bei einem Misserfolg diese sich selbständig weiterentwickeln. (Trick, 2020, S. 211–212)

3.4.1 Sicherheitsbedrohungen im Mobilfunk 5G

Da 5G auch wie sein Vorgänger IP-Basierend aufgebaut ist, sind die potenziellen Gefahrenquellen auf den mobilen Endgeräten ident. Die nachfolgende Bedrohungen sind beim Vorgänger identifiziert und betreffen den Nachfolger 5G ebenfalls (Liyanage u. a., 2018, S. 66):

- **Unsicheres Betriebssystem:** Angreifende können Schwachstellen in mobilen Betriebssystemen ausnutzen, sofern diese nicht gepatcht oder upgegradet sind
- **Herunterladen von unautorisierten Applikationen:** Applikationen die nicht aus einem verifizierten Store heruntergeladen werden, können Schadsoftware enthalten
- **Unsichere Applikationen bzw. Spyware:** Sensible Daten der Endbenutzer*Innen. können aus unsicheren Applikationen entwendet werden
- **Virus:** Ein bösartiger Softwarecode, der Funktionen oder Dateien am mobilen Endgerät beschädigt
- **Malware:** Bösartige Applikationen verbreiten sich von selbst und verursachen einen netzwerkweiten Schaden

Liyanage u.a. (, 2018, S. 152–153) beschreibt allgemein die nachfolgenden Sicherheitsbedrohungen für den 5G-Mobilfunkstandard:

- **Abfangen von Nachrichten:** Die angreifende Person fängt die Informationen mittels der Kontroll- und Datensignalisierungen ab. Der Inhalt wird nicht gelöscht oder geändert, sondern nur gelesen.
- **Angriffe auf Basis von Daten:** Hacker*Innen zielen auf die Informationen in den 5G-Kommunikationsystemen und richten einen Schaden an, indem die Daten gelöscht oder verändert werden.
- **Angriffe auf Basis von Nachrichten:** Kontroll- bzw. Datensignale, die zum und vom 5G-Netz fließen, werden abgeändert und unterbrechen somit die Kommunikation.
- **Unberechtigter Zugriff auf der Hardware**: Modifizierte Basisstationen können als Man-in-the-Middle-Angriffe genutzt werden. Des Weiteren kann mittels eines am Switch verbundenen physischen Kabel, ein erheblicher Schaden entstehen. Indem die Kontroll- bzw. Datensignale manipuliert werden.

- **Probleme auf der physikalischen Schicht:** Absichtlich erzeugte künstliche Störungen im Funkbereich, können die Kommunikation stören. Ein zu hohes SNIR blockiert die Kommunikation.
- **Probleme mit Medium Access Control (MAC):** Die Endgeräte der Benutzer*Innen werden in einer spezifischen Zelle vom Angreifenden beobachtet. Bei einem Angriff kann die Bandbreite von den Benutzer*Innen anhand eines falschen Bufferstatus reduziert werden.

Nachdem die Netzwerkkomponenten virtualisiert und Software-Defined-Networking ein Bestandteil der 5G-Infrastruktur sind, ergeben sich hier eine Vielzahl an verschiedenen Angriffsvektoren (Zhu u. a., 2017, S. 11–13):

- **Abhängigkeiten vom eingesetzten Hypervisor:** Die komplette NFV-Infrastruktur kann durch eine Sicherheitslücke in der Software gekapert werden. Eine geeignete Verschlüsselung und ein regelmäßiges Patchen sind notwendig.
- **Elastische Netzwerkgrenzen:** Virtuelle und physische Funktionen werden kombiniert und die Grenze zwischen beiden Welten ändert sich. Die Änderung in der NFV-Infrastruktur erschwert es, wirkungsvolle Sicherheitsfunktionen bereitzustellen.
- **Dynamisches Verhalten:** Dynamische Adaptionen der Sicherheitsfunktionen sind notwendig, da Funktionen und die Netzwerktopologien sich ständig in der NFV-Infrastruktur ändern.
- **Unautorisierter Zugriff im SDN-Application Layer:** Zugriff erfolgt über unautorisierte Applikationen und implementieren betrügerische Regeln ein, die durch mangelnde Umsetzung von Richtlinien hervorgerufen werden.
- **Unautorisierter Zugriff im SDN-Control Layer:** Durch unautorisierte Controller und Anwendungen, kann der unerlaubte Zugriff stattfinden. Schädliche Anwendungen können betrügerische Regeln implementieren und eine DoS-Attacke auf die Controller-Switchkommunikation initiieren.
- **Unautorisierter Zugriff im SDN-Data Layer:** Datenlecks aus der Ermittlung von Regeln, sogenannte Side-Channel-Attacken auf den Input oder Weiterleitungsrichtlinien, ermöglichen den unbefugten Zugriff auf die Steuerung bzw. auf die Daten.
- **Unautorisierter Zugriff über das Southbound-Interface in SDN:** Konfigurationsfehler von TLS (Transport Layer Security) können schädliche Anwendungen in der Control Layer-Ebene einspielen. Eine Kommunikationsflut kann den Controllerswitch überfluten.

3.4.2 5G-AKA

Es existieren zwei Authentifizierungsprotokolle im neuen Mobilfunkstandard 5G, das 5G-AKA-Protokoll und das EAP-AKA-Protokoll (,vgl. Kapitel 3.4.3). AKA steht für Authentication and Key Management. Beide Protokolle sind für den sicheren Austausch eines kryptografischen Schlüssels zuständig und haben den Zweck, dass zwischen dem Endgerät und dem 5G-Netz eine sichere Authentifizierung stattfindet. Zusätzlich wird ein Schlüsselmaterial bereitgestellt, welches zwischen dem Endgerät und dem verbundenen Netz verwendet werden kann. Durch das primäre Authentifizierungs- und Schlüsselvereinbarungsverfahren, wird ein Ankerschlüssel (K_{SEAF}) erzeugt. Aus diesem Ankerschlüssel kann für verschiedene Sicherheitskontexte der gleiche Schlüssel bereitgestellt werden, neue Authentifizierungen sind nicht notwendig. (3GPP, 2021, S. 39)

Der eigene Mobilfunkbetreibende entscheidet welche Authentifizierungsmethode im Heimatnetz verwendet wird, da der Authentifizierungsvorgang bei beiden Protokollen sehr ähnlich aufgebaut ist (3GPP, 2021, S. 39). Beide Authentifizierungsmethoden besitzen fünf verschiedene Sicherheitsentitäten. Diese bilden sich aus Authentication Server Function (AUSF), Security Anchor Function (SEAF), User Equipment (UE), und Unified Data Management (UDM) bzw. Authentication Credential Repository and Processing Function (ARPF) (3GPP, 2021, S. 23–24).

Es existieren zwei Phasen bei der Authentifizierung mit 5G-AKA und EAP-AKA. Die erste Phase ist bei beiden Protokollen ident. Das Endgerät (UE) sendet eine Nachricht an den SEAF und beginnt den Authentifizierungsprozess. Die IMSI (International Mobile Subscriber Identity) wird nicht im Klartext übertragen und stellt eine Sicherheitsverbesserung gegenüber dem Mobilfunkstandard 4G dar. IMSI ist für die Identifizierung des Endgeräts (UE) verantwortlich und besteht aus 15 Zahlen, die Zahlen liegen zwischen null und neun. Am Beginn wird ein verschlüsselter Identifikator, der sogenannte GUTI (Globally Unique Temporary Identity) an den SAEF übermittelt. SAEF leitet nach Erhalt der Registrierungsanforderung, die Authentifizierung an den AUSF weiter. Der AUSF überprüft, ob die Registrierungsanforderung berechtigt war. Nach der durchgeführten Prüfung wird die Authentifizierungsinformation an den UDM/ARPF übermittelt und dieser entscheidet am Ende des Authentifizierungsprozess, die jeweilige Authentifikationsmethode. (3GPP, 2021, S. 41–42)

Im 5G-AKA-Protokoll sendet das Endgerät (UE) nach erfolgreicher Authentifizierung aus einem besuchten Gästenetz an das Heimatnetz, den Nachweis bzw. die Bestätigung der erfolgreichen Authentifizierung. Zuvor wird die im Prozess kalkulierte Hash Response mit der zu erwartenden Hash Expected Response verglichen. Dieser wird in der AUSF mit Hilfe des SHA-256-Algorithmus berechnet. (3GPP, 2021, S. 44–46)

3.4.3 EAP-AKA

Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA) ist im RFC 5448 definiert und ist eine Überarbeitung des RFC 3748 Extensible Authentication Protocol (EAP). Das Neue an EAP-AKA ist, dass es eine neue Schlüsselableitungsfunktion besitzt. Mittels dieser Erneuerung werden die Schlüssel an den Namen des Zugangnetzes gebunden. Kompromittierte Zugangspunkte und Schlüssel werden hierdurch begrenzt und verhindert. 3GPP hat eine Reihe von Anwendungen im AKA-Mechanismus überarbeitet, einige von denen sind im Funkzugangsnetz auf nativer Verkapselung implementiert. (Arkko u. a., 2009)

Jede Änderung der Schlüsselableitung muss für beide Seiten im Protokoll eindeutig sein. Darunter ist zu verstehen, dass keine alten Geräte an neuen Geräten angeschlossen werden, um eine fehlerhafte Schlüsselableitung durchzuführen oder eine Fehlermeldung zu erhalten. SHA256 wird als Hash-Funktion eingesetzt. Der IMSI besteht aus acht Zeichen der ASCII-Zeichenfolgen. (Arkko u. a., 2009)

Das im Heimatnetz enthaltene AUSF bzw. UDM erhält eine Bestätigung, sobald das Endgerät (UE) erfolgreich authentifiziert wurde. Zuvor muss die EAP-Response/AKA-Challenge erfolgreich verifiziert werden. (3GPP, 2021, S. 43–44)

4 Vorgangsweise und Methode

Im folgenden Kapitel wird die Vorgangsweise und die Methode der durchgeführten empirischen Analyse näher erläutert. Zuvor wird auf die Forschungsfrage und die daraus resultierende Hypothese eingegangen. Des Weiteren wird beschrieben, wie die Durchführung der Erhebung mittels der Mixed-Methods-Forschung erfolgt.

4.1 Forschungsfrage und Hypothese

Die Forschungsfrage dieser wissenschaftlichen Arbeit lautet:

Welche Bedingungen müssen erfüllt sein, damit Nutzer*Innen österreichische WLAN-Provider gegenüber dem Mobilfunkstandard 5G vorziehen?

Aus der obengenannten Forschungsfrage kann die nachfolgende Hypothese abgeleitet werden:

Die Betrachtungen der Sicherheitsaspekte unterscheiden sich für die Nutzer*Innen, sowie das kostenlose Service als auch Datenvolumen zu sparen sind die größten Faktoren für die Nutzung eines österreichischen WLAN-Hotspots.

In Kapitel 4.4 sind die oben genannten Begrifflichkeiten in messbare Indikatoren umgewandelt, anhand dieser wird die Operationalisierung durchgeführt.

4.2 Vorgangsweise

Laut Hug u.a. (, 2015, S. 22–26) bedeutet empirisch forschen, wissenschaftliche Erfahrungen zu gewinnen und dabei die Forschungsfragen lösungsorientiert mit wissenschaftlichen Techniken und Methoden zu bearbeiten. Um die anfallende Forschung zu bearbeiten, wird ein bestimmter Prozess durchlaufen. Ein Problem wird in einem Forschungsgebiet erkannt, die in eine Forschungsfrage und in eine Hypothese verfasst wird. Der Forschungsprozess beinhaltet die Planung, Durchführung, Analyse, Interpretation, Diskussion und Präsentation der Erkenntnisse (Ebster & Stalzer, 2013, S. 142-143).

Bei empirischen Forschungsmethoden wird zwischen zwei Verfahren unterschieden, quantitativ und qualitativ. In einem quantitativen Verfahren werden die empirischen Sachverhalte als Zahlen dargestellt und mit statistischen Methoden verarbeitet. Als

Messinstrumente kommen standardisierte Befragungen oder die quantitative Inhaltsanalysen zur Geltung. In einem qualitativen Verfahren steht die persönliche Anschauung des Menschen im Vordergrund und es werden die subjektiven Lebenswelten erkundet. (Hug u. a., 2015, S. 87–89)

Um die Forschungsfrage dieser wissenschaftlichen Arbeit beantworten zu können, soll die Kombination einer qualitativen und quantitativen Forschung herangezogen werden. Man spricht hier von einer Mixed-Methods-Forschung. Kuckartz (, 2014, S. 33) beschreibt die Definition dieser Forschungsmethode wie folgt:

„Unter Mixed-Methods wird die Kombination und Integration von qualitativen und quantitativen Methoden im Rahmen des gleichen Forschungsprojekts verstanden. Es handelt sich also um eine Forschung, in der die Forschenden im Rahmen von ein- oder mehrphasig angelegten Designs sowohl qualitative als auch quantitative Daten sammeln. Die Integration beider Methodenstränge, d.h. von Daten, Ergebnissen und Schlussfolgerungen, erfolgt je nach Design in der Schlussphase des Forschungsprojektes oder bereits in früheren Projektphasen.“

Es existieren fünf verschiedene Designtypen in einer Mixed-Methods-Forschung, und zwar die Triangulation, Komplementarität, Entwicklung, Initiation und Expansion (Greene u. a., 1989, S. 127). Als Designtyp wurde die Komplementarität ausgewählt, da diese auf Elaboration, Illustration und auf ein besseres Verständnis durch die Resultate einer zweiten Studie zielen. Forschungsergebnisse der angewandten Methode werden hierdurch vervollständigt, ergänzt und erweitert interpretiert. (Kuckartz, 2014, S. 58)

Die erste Phase der Planung von empirischen Forschungen ist zuerst die Formulierung der Forschungsfrage und dessen Bezug auf die Theorie. Zweitens trennen sich die Wege zur Beantwortung der Forschungsfrage in eine qualitative und quantitative Teilstudie bei einem parallelen Design des Mixed-Methods. Diese Teilstudien sind parallel zueinander angeordnet und werden gleichzeitig durchgeführt. Beide Studien verlaufen unabhängig voneinander, die jegliche Standards der quantitativen und qualitativen Forschung entsprechen. Nach den durchgeführten Abläufen werden die Ergebnisse der Studien an der Endphase aufeinander bezogen (,vgl. Abbildung 21). Für die Erstellung eines integrativen Berichts wird der Begriff Meta-Inferenzen benutzt, da diese die Ergebnisse auf eine Metaebene darstellen. Der Mixed-Methods-Ansatz ist nicht nur eine additive Zusammentragung von unterschiedlichen Methoden, sondern es lassen sich Erkenntnisse aus der qualitativen und quantitativen Forschung gewinnen. Aristoteles-Spruch, das

Ganze mehr als die Summe seiner Teile ist in diesem Fall zutreffend. (Kuckartz, 2014, S. 73–75)

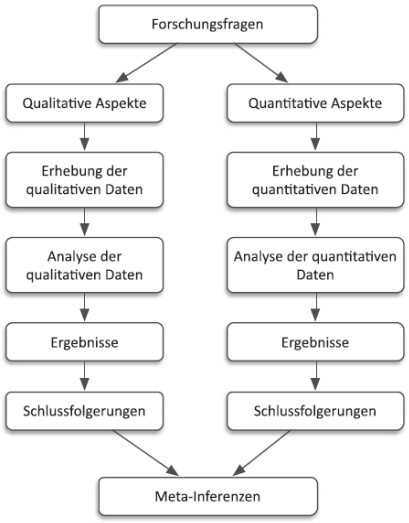

Abbildung 21 - Ablaufschema eines parallelen Design (Kuckartz, 2014, S. 74)

Bei der qualitativen Forschung bilden die Säulen des qualitativen Denkens nach Mayring (, 2016, S. 24–37) eine wichtige Rolle für diese Entscheidung. Qualitatives Denken betont die Ganzheitlichkeit des Menschen, die Entwicklung als auch deren Beruf des Menschen soll miteinbezogen werden. Es behandelt nicht die isolierte Betrachtung einzelner Aspekte, da neue Aspekte während der Untersuchung hervorkommen können. Die Offenheit ist beim qualitativen Denken gefordert, da hierdurch neue Relevanzen zum Forschungsthema sich herauskristallisieren können. Damit von einem gemeinsamen Verständnis auszugehen ist, werden Begriffe vorher abgeklärt und durch die Kommunikation die Unverständlichkeiten beseitigt. (Mayring, 2016, S. 24–37)

Mündliche Befragungen existieren als qualitative Forschungsmethode, welche auch als Interview benannt werden. Ein Interview zwischen Forschenden mit einer zu erforschenden Person dient der wissenschaftlichen Erhebung von Daten. Diese sind systematisch und handeln von einem bestimmten Forschungsthema, samt seiner Forschungsfrage. (Hug u. a., 2015, S. 100)

Die Befragten des Interviews sind Personen mit Expertisen zu einem bestimmten Thema. Es soll deren Einstellung, Betrachtungsweise und Interpretationen im Interview erforscht und widerspiegeln (Gläser & Laudel, 2010, S. 40). Bei der Auswahl von Personen mit Expertisen ist zu achten, dass diese Kompetenzen und Wissen im Themengebiet aufweisen können (Baur & Blasius, 2019, S. 680).

Um Interviews durchzuführen können, gilt es deren Standardisierung festzulegen. Es wird zwischen vollstandardisierte, halbstandardisierte und nichtstandardisierte Interviews unterschieden. In dieser wissenschaftlichen Arbeit wird ein nichtstandardisiertes Interview verwendet. Der Fragewortlaut und deren Reihenfolge wird von der interviewenden Person vorgegeben, jedoch nicht die Antwortmöglichkeiten. (Gläser & Laudel, 2010, S. 41)

Das leitfadengestützte Expert*Inneninterview generiert spezifische Informationen über ein zu untersuchendes Phänomen, die normalerweise nicht zu erhalten wären. Dazu ist ein Leitfadeninterview ein analytischer Zugang innerhalb eines methodenpluralistischen Ansatzes geeignet, also wie bereits oben beschrieben, die Kombination der qualitativen und quantitativen Methoden. (Kaiser, 2014, S. 30–31)

Leitfadengestützte Interviews können zu Lerneffekten führen, da jedes Interview zu neuen Informationen und somit zu angereicherten Hintergrundwissen für das nächste Interview generiert (Gläser & Laudel, 2010, S. 194). Den generierten Mehrwert von leitfadengestützten Interviews beschreiben Baur und Blasius (, 2019, S. 669) als:

„Qualitative, leitfadengestützte Interviews sind eine sehr verbreitete, ausdifferenzierte und methodisch vergleichsweise gut ausgearbeitete Methode, qualitative Daten zu erzeugen. Leitfadeninterviews gestalten die Führung im Interview über einen vorbereiteten Leitfaden, Experteninterviews sind definiert über die spezielle Auswahl und den Status der Befragten“.

Im zweiten Forschungsstrang, des quantitativen Ansatzes werden mit Hilfe spezifischen Hilfs- und Instrumententheorien die methodischen Entscheidungen verknüpft. Diese beeinflussen den Theoriegehalt und die Interpretierbarkeit der Daten. Im Sinne der Präsentationsqualität der Studie, müssen die Gütekriterien detailliert offengelegt und von der Wissenschaftsgemeinschaft für inhaltlich gerechtfertigt gehalten werden. Um eine Hypothese anhand von Daten zu prüfen, muss im Zuge eines geordneten und dokumentierten empirischen Forschungsprozess zuerst die Daten gewonnen werden. Damit etwas sinnvolles über die infrage stehende Hypothese mitgeteilt werden kann. (Döring & Bortz, 2016, S. 52)

Für die Durchführung der quantitativen Forschung, existieren eine große Anzahl an verschiedensten Stichproben. Jedoch spielen drei Typen der nicht-probabilistischen Stichproben eine wichtige Rolle, und zwar sind es die Gelegenheitsstichproben, die Quotenstichprobe und die Stichprobenbeziehung mittels spezieller Verfahren. Die

Gelegenheitsstichprobe ist einer der häufigsten Stichprobentypen in der quantitativen Sozialforschung. Definitionsmäßig sind diese mit dem geringsten Aufwand verbunden, da Personen in die Studie einbezogen werden, bei welchen gerade eine günstige Gelegenheit besteht. Im Internet veröffentlichte Online-Umfragen oder in der Vorlesung an einer Universität verteilte Umfragen sind schnell erledigt. Die Aussagekraft quantitativer Forschungen von Gelegenheitsstichproben ist sehr begrenzt und hätten bei einer reinen Auswahl ohne eine zweite Forschungsmethode eine niedrige Repräsentativität. (Döring & Bortz, 2016, S. 306)

Ein schriftlicher Online-Fragebogen ist mittlerweile die wichtigste vollstrukturiere Befragungstechnik in der Sozialforschung und in akademischen Grundlagenforschungen. Eine große Effizienz des Verfahrens, tritt dadurch in Vorschein. Für eine Online-Umfrage ist ein Befragungsserver im Web notwendig. Auf diesen Umfrageserver ist ein Teilnehmer-Management, eine geordnete Präsentation des Fragebogens und die Dokumentation der Antworten möglich. Nach der Befragung stehen die gewählten Antworten der zu befragenden Personen als digitale Datensätze zur Verfügung. Um die Benutzerfreundlichkeit zu garantieren, muss der Online-Fragebogen auf das Medium abgestimmt sein. Im Grunde genommen muss das Lesen am Bildschirm optimiert sein. Für die Orientierung der Befragten soll ein Fortschrittsbalken dargestellt sein und die Befragung soll nicht länger als 10 bis 15 Minuten dauern. (Döring & Bortz, 2016, S. 414–415)

4.3 Methoden

4.3.1 Qualitative Forschungsmethode

Für die Forschungsarbeit wurden als Forschungsmethoden ein leitfadengestütztes Expert*Innen-Interview und eine Online-Umfrage als Erhebungsverfahren ausgewählt. Bevor die Interviews mit den Expert*Innen durchgeführt werden konnten, musste im Vorfeld ein Interviewleitfaden erstellt werden. Dieser Interviewleitfaden soll, die im Zuge der durchgeführten Interviews erhobenen Daten vereinheitlichen, strukturieren und eine Vergleichbarkeit ermöglichen. Nach einer intensiven Auseinandersetzung mit einschlägiger Fachliteratur und nach ersten Vorgesprächen mit potentiellen Expert*Innen, wurde der dem Anhang A beigefügte Interviewleitfaden formuliert.

Der Interviewleitfaden muss den Personen mit der Expertise das freie Erzählen ermöglichen, da diese die notwendige Berufserfahrung mitbringen. Den Expert*Innen

bietet dies die Möglichkeit, ihre Eindrücke abseits eines definierten Bewertungsschemas wiedergeben zu können.

Eine kurze Themeneinweisung und Abklärung erfolgen noch bevor die erste Frage gestellt wird. Hiermit soll ein einheitliches Verständnis zum Forschungsthema gewährleistet werden. Die nachfolgenden Kriterien für die Auswahl der geeigneten Expert*Innen sind:

- Langjährige Erfahrungen in den Technologien Mobilfunk und/oder WLAN
- Personen die bei WLAN-Providern oder Mobilfunkbetreibenden tätig sind
- Personen die bei Herstellenden von WLAN-Komponenten tätig sind

Die aufgezeichneten Interviews, sollen zur Gänze transkribiert werden. Mittels der Transkription wird die gesprochene Sprache in eine Schriftsprache verschriftlicht. Dadurch wird die nachfolgende Auswertung vereinfacht. Allgemeine akzeptierte Transkriptionsregeln von Interviewprotokollen existieren nicht. Teilnehmende des Interviews werden anonymisiert und mit eindeutigen Codes definiert. Dem Autor sollen die Codes die Zuordnung ermöglichen, mit wem die Interviews durchgeführt wurden. (Gläser & Laudel, 2010, S. 193–194)

In dieser Arbeit wird die Volltranskription als Protokollierungstechnik gewählt, d.h. eine vollständige Verschriftlichung aller Audio- bzw. Videoaufzeichnungen (Döring & Bortz, 2016, S. 583). Die Abschrift der einzelnen Interviews mit den Expert*Innen erfolgt in einem separaten Word-Dokument.

Im ersten Absatz dieses Kapitels wurde bereits erwähnt, wie wichtig es sei die Daten einheitlich und vergleichbar zu erheben. Um dies auch im Rahmen der vorliegenden wissenschaftlichen Arbeit gewährleisten zu können, soll bei der Durchführung und Auswertung der Expert*Innen Interviews die qualitative Inhaltsanalyse nach Mayring zur Anwendung kommen. Die qualitative Inhaltsanalyse nach Mayring findet gerade bei der Auswertung von Fragebögen bzw. Interviews häufig Anwendung, da sie mittels einer systematischen Vorgehensweise und festgelegter Kriterien (Regeln) eine geordnete und strukturierte Bearbeitung/Analyse von Inhalten (Materialien) garantiert. Für ein strukturiertes Vorgehen bei der Inhaltsanalyse definierte Mayring ein „allgemeines inhaltsanalytisches Ablaufmodell“, dass die nachfolgenden Tätigkeiten ablauftechnisch gliedert (Mayring, 2015, S. 50–60):

1. Festlegung des Materials
2. Analyse der Entstehungssituation
3. Formale Charakterisierung des Materials
4. Festlegung der Analyserichtung
5. Theoretische Differenzierung der Fragestellung
6. Bestimmung der Analysetechnik
7. Definition der Analyseeinheiten
8. Durchführung der Materialanalyse

Mayring (, 2016, S. 114) beschreibt die Auswertung der transkribierten Interviews der qualitativen Inhaltsanalysen als eine Methode, mit der Texte inhaltlich analysiert werden. Das Ziel der qualitativen Inhaltsanalyse gilt es die Texte theorie- und regelgeleitet zu verstehen und zu interpretieren. Es wird zwischen den drei Grundformen der Analyse, nämlich Zusammenfassung, Explikation und Strukturierung unterschieden. Bei der gewählten Analysetechnik die Zusammenfassung, wird das Material auf die bedeutenden Inhalte reduziert. Das gewonnene Material im Zuge der Interviews, stellt noch immer ein Abbild des Grundmaterials dar (Mayring, 2015, S. 65–69). Die Zusammenfassung von Mayring folgt dabei einen definierten Ablaufmodell, welches nachfolgend erläutert wird (Mayring, 2015, S. 70–72):

1. **Paraphrasierung:** Anhand der Paraphrasierung sollen jene Textteile, welche nicht inhaltstragend sind, aus dem erstellten Transskript entfernt werden. sollen Auf ein höheres Sprachniveau sollen alle Textstellen, die eine inhaltliche Bedeutung haben, gehoben werden.
2. **Generalisierung auf das Abstraktionsniveau:** Die vorabgewonnenen Paraphrasen bei der Generalisierung des Textes, werden auf eine definierte Abstraktionsebene gebracht und Satzaussagen generalisiert.
3. **Erste Reduktion:** In der ersten Reduktion werden alle bedeutungsgleichen Paraphrasen eliminiert und nur jene weiterverendet, die für das Material von Bedeutung sind.
4. **Zweite Reduktion:** Alle paraphrasierten Stellen werden in der zweiten Reduktion mit einem ähnlichen Inhalt zusammengefasst und bei Bedarf neu formuliert. Durch die beiden Reduktionen können unter anderem Kategorien für die Analyse erstellt werden.

4.3.2 Quantitative Forschungsmethode

Im zweiten Teil der Forschungsmethode kommt ein vollstrukturierter Onlinefragebogen zum Einsatz. Zu Beginn wird ein Grobkonzept entworfen, der anschließend verfeinert wird. Nach Fertigstellung des konstruierten Fragebogens wird dieser einem Vortest unterzogen. Bei Bedarf wird nach Vollzug des Vortests in der Revision überarbeitet und danach den Probanden und Probandinnen zur Verfügung gestellt. Das Grobkonzept ist ein aufwendiger Prozess der den wissenschaftlichen Gütekriterien der Objektivität, der Reliabilität und der Validität unterliegt. Standardisierte Fragebögen bestehen aus sechs Elemente (Döring & Bortz, 2016, S. 405–406):

- Fragebogentitel
- Fragebogeninstruktion
- Inhaltliche Frageblöcke
- Statistische Angaben
- Fragebogen-Feedback
- Verabschiedung

Nachdem das Grobkonzept des Fragebogens erstellt wurde, muss daraus das resultierende Feinkonzept nachfolgende Aspekte betrachten (Döring & Bortz, 2016, S. 407–409):

- **Art der Items und Antwortformate:** Leicht verständliche und schnell zu beantwortende Items müssen im Fragebogen enthalten sein.
- **Reihenfolge der Items:** Ziel ist es thematische Fragen in Blöcke zusammenzufassen und eine logische Schrittweise zu erstellen.
- **Filterführung im Fragebogen:** Existieren einzelne Items oder Blöcke, die nicht von allen zu befragenden Personen zu beantworten sind, dann werden Filterführungen eingesetzt.
- **Layout des Fragebogens:** Es ist auf ein ansprechendes Layout zu achten, damit die Antwortverzerrungen vermieden werden.
- **Fragebögen für unterschiedliche Distributionswege:** Bei der Verwendung von vollstandardisierten Fragebögen, ist auf den Aufbau, die Länge und das Layout bei verschiedenen Endgeräten zu achten.

- **Fragebögen für interkulturelle Studien:** Damit ein Fragebogen in interkulturellen Studien verstanden wird, muss dieser von Muttersprachlern begutachtet werden.

Die Antwortformate von Fragebögen sind in verschiedene Varianten unterteilt. Am häufigsten kommen die unipolare und bipolare Ratingskalen in Betracht. Unipolare Ratingskalen bilden die Intensität eines Merkmals ab. Diese Merkmale besitzen keine negativen Werte bzw. keinen Gegenpol. Bei bipolaren Ratingskalen sind gegensätzliche Merkmal am Ende des Skalenende zu sehen. (Döring & Bortz, 2016, S. 245)

Der Online-Fragebogen beinhaltet eine 6-stufige unipolare Likert-Skala. Die Ratingskala bildet die Intensität des Merkmals graduell ab. Im Anhang B ist der Online-Fragebogen angehängt.

Aufgrund der Kombination von einer qualitativen und quantitativen Forschungsmethode, gilt es sicherzustellen, dass die Mixed-Methods-Studie eine hohe wissenschaftliche Qualität aufweist. Die qualitativen und die quantitativen Gütekriterien der Sozialforschung sind daher integraler Bestandteil der Forschungsmethode (Döring & Bortz, 2016, S. 114). Hug und Poscheschnik (, 2015, S. 93) beschreiben, dass sich eine gute wissenschaftliche Forschung an Gütekriterien zu halten hat. Mittels dieser kann die Qualität der wissenschaftlichen Studie beurteilt und die Mindestanforderungen eingehalten werden. Da sich ein Teil dieser wissenschaftlichen Arbeit mit der qualitativen Erhebung beschäftigt, sind die nachfolgenden sechs Gütekriterien qualitativer Forschung nach Mayring formuliert (Mayring, 2016, S. 144–148):

- Verfahrensdokumentation
- Argumentative Interpretationsabsicherung
- Regelgeleitetheit
- Nähe zum Gegenstand
- Kommunikative Validierung
- Triangulation

Laut Baur und Blasius (Baur & Blasius, 2019, S. 490–496) sind die quantitative Gütekriterien in drei Hauptkriterien unterteilt:

- Objektivität
- Reliabilität
- Validität

Aus der oben gestellten Forschungsfrage (,vgl. Kapitel 4.1) ergeben sich nachfolgende Hypothesen, welche die Sicherheitsaspekte verifizieren:

- **Hypothese 1:** Männer und Frauen unterscheiden sich in der angegebenen Bedeutung von Sicherheit.
    - Besitzen Frauen ein stärkeres Sicherheitsbewusstsein gegenüber dem anderen Geschlecht den Männern? Die aufgestellte Hypothese soll darüber Klarheit schaffen und zeigen, dass es einen Unterschied gibt. Die Überprüfung der Hypothese findet mittels eines T-Test statt.
- **Hypothese 2:** Je älter eine Person, desto höher die Bedeutung von Sicherheit.
    - Ältere Generationen besitzen ein höheres Sicherheitsbewusstsein als die jüngeren Generationen. Ist eine Person jünger, so ist die Sicherheit weniger wichtig. Um die Hypothese bestätigen zu können, wird eine Korrelationsanalyse durchgeführt.
- **Hypothese 3:** Personen mit unterschiedlichem Bildungsabschluss unterscheiden sich in der angegebenen Bedeutung von Sicherheit.
    - Haben Personen einen höheren oder einen niedrigeren Bildungsabschluss, so unterscheidet sich das Sicherheitsempfinden bzw. die Bedeutung der Sicherheit. Das Ergebnis der Varianzanalyse soll die Hypothese bestätigen.

4.4 Operationalisierung

Um die aufgestellte Hypothese zu beantworten, gilt es messbare Begrifflichkeiten anhand Indikatoren zu messen (,vgl. Kapitel 4.1). Den Ausgangspunkt der Operationalisierung bilden die Begriffe. Die Begriffe werden durch Dimensionen ergänzt, die sich wiederum aus Indikatoren ableiten. Die nachfolgenden Indikatoren bilden die Basis für die Befragung der Expert*Innen bzw. daraus ableitend für die Online-Umfrage (, vgl. Tabelle 5).

Begriff	Dimension	Indikator
Effizienz	Infrastruktur	• Flexibilität und Skalierbarkeit • Kosten
	Modulationsverfahren	• Datendurchsatz • Frequenz
	Umgebung	• Dichte
	Energie	• Batterie
Sicherheit	Gefahren	• Angriffsvektoren • Protokolle & Verschlüsselungen

Tabelle 5 – Operationalisierung

4.5 Durchführen der Erhebung

Wie bereits in Kapitel 4.3 beschrieben, wurde anhand von leitfadengestützten Expert*Innen Interviews und einer Online-Umfrage die Erhebung durchgeführt. Die Akquirierung der Expert*Innen erfolgten teilweise durch telefonische bzw. schriftliche Anfragen und durch das vorhandene berufliche Netzwerk des Autors. Auswahl und Akquirierung der Expert*Innen sind nachfolgend dargestellt.

4.5.1 Auswahlkriterien der Expert*Innen

Um geeignete Expert*Innen zu eruieren, galten die nachfolgenden Auswahlkriterien:

- **Unterschiedliche Organisationen:** Um unterschiedliche Sichtweisen und Praxiserfahrungen zu erfahren, wurden Expert*Innen aus unterschiedlichen Organisationen und Branchen befragt. Die befragten Personen sind in internationalen und in nationalen Unternehmen tätig.
- **Berufserfahrung und Position:** Ausschlaggebend bei der Auswahl der Expert*Innen ist das ein fachspezifisches Wissen vorhanden sein muss. Eine langjährige Erfahrung beim Betreiben von WLAN-Hotpsots oder/und bei Mobilfunkbetreibende und deren Know-How war ein Kriterium. Personen welche auch bei internationalen Herstellenden für Netzwerkprodukte tätig sind und entsprechendes Wissen vorweisen können, sind als Expert*Innen eingestuft.

4.5.2 Akquirierung der Expert*Innen

Das Akquirieren der Expert*Innen wurde auf verschiedenen Kommunikationskanälen durchgeführt, die nachfolgende Aufzählung stellt diese dar:

- **Vorhandenes Netzwerk:** Im Vorfeld wurden die persönlichen Kontakte des Autors nach den zuvor definierten Auswahlkriterien (‚vgl. Kapitel 4.5.1) schriftlich bzw. telefonisch kontaktiert. Im Zuge der Konversation wurde auf das geplante Forschungsvorhaben eingegangen und ob eine Teilnahme bei der Befragung in Frage kommen würde.
- **Ausgeweitetes Netzwerk:** Das vorhandene Netzwerk hat den Kontakt zu weiteren Expert*Innen hergestellt. Persönliche Kontaktdaten wurde ausgetauscht und Termine für die Befragung mit den geeigneten Expert*Innen vereinbart.
- **Soziales Netzwerk:** In sozialen Netzwerken wie „XING“ oder „Linkedin“ wurde mit Hilfe von Schlüsselbegriffen nach Expert*Innen gesucht. Bei einem Treffer wurden diese über die Plattform schriftlich kontaktiert.

Nach erfolgreicher Zusage mit den Expert*Innen wurde der Termin, der Ort und die Art des Interviews festgelegt. Aufgrund der Verwendung von Microsoft Teams als Aufnahmemedium, konnte das Interview ohne eine fixe Örtlichkeit durchgeführt werden. Der Vorteil von Microsoft Teams liegt an der Speicherung der Audiokommunikation und der automatischen Transkription der gesprochenen Sprache. Am Beginn des Interviews wurde der Hinweis auf die Aufnahme, der Transkription und auf die Anonymität der Expert*Innen verwiesen. Zu Beginn des Interviews wurden das Forschungsthema, die Forschungsfrage und das zu untersuchende Ziel vorgestellt. Um ein gemeinsames Verständnis zu generieren, wurden noch die Begrifflichkeiten besprochen. Während des Interviews wurden Notizen gemacht, die in einem späteren Verlauf des Interviews als Grundlage für weitere Fragen dienten. Nach Abschluss der Interviews wurden die Aufnahmen analysiert und wesentliche Inhalte paraphrasiert.

4.5.3 Fragebogenkonstruktion und Datenerhebung

Der erstellte Online-Fragebogen, (, vgl. Anhang B) enthält in seiner endgültigen Fassung für den quantitativen Forschungsweg sieben Fragen. Dieser unterteilt sich in den nachfolgenden vier verschiedenen Rubriken:

- **EI:** Einleitende Frage
- **EF:** Effizienz
- **SI:** Sicherheit
- **SD:** Soziodemografisch

Die Rubriken Effizienz (EF) und Sicherheit (SI) werden im Zuge der Online-Befragung anhand der Likert-Skalen zwischen „1 = *trifft gar nicht zu*“ bis „6 = *trifft völlig zu*“ beantwortet. Die Likert-Skalen 1 bis 3 werden als negativ und die Likert-Skalen 4 bis 6 als positiv gewertet. In der Rubrik Effizienz (EF) werden die persönlichen Gründe einer Nutzung eines österreichischen WLAN-Hotspots in Hinblick auf die vier Dimensionen der Effizienz abgefragt. Des Weiteren wird in der Rubrik Sicherheit (SI) die fünfte Dimension Sicherheit nach persönlichen Einschätzungen der Sicherheit bei einer Nutzung von österreichischen WLAN-Hotspots abgefragt. Bei den Rubriken Einleitende Frage (EI) und Soziodemografisch (SD) werden die gestellten Fragen, mit Hilfe von einfach Auswahlfragen beantwortet. Im soziodemografischen Aspekt werden die Daten der Respondenten wie Alter, Geschlecht, formale Bildung und Mobilfunkvertrag erhoben. Das Ausfüllen des Online-Fragebogens nimmt in der Regel drei bis fünf Minuten in Anspruch.

Der Erhebungszeitraum war vom 16.03.2022 bis einschließlich 28.03.2022 unter dem Link https://www.soscisurvey.de/wlanvs5g/ abrufbar. In dieser Zeit konnte die Onlineumfrage geöffnet und die Befragungen der teilnehmenden Personen durchgeführt werden. Der Online-Fragebogen wurde unteranderem am Campus der FernFH zur Verfügung gestellt. Zusätzlich wurden weitere teilnehmende Personen mittels digitalen Kommunikationskanälen (wie beispielsweise E-Mail, WhatsApp) kontaktiert und der Online-Fragebogen an diese versendet, mit der Bitte um Weiterleitung der Online-Umfrage. Hierbei handelt es sich um die sogenannte Schneeballtechnik und basiert auf die Gelegenheitsstichprobe (, vgl. Kapitel 4.2). Bei den Willkürlichen Stichproben kann es dazu führen, dass nur ein spezifisches Netzwerk untersucht wird und es zu einer systematischen Verzerrung gelangt (Baur & Blasius, 2019, S. 490–496).

Für die Online-Umfrage kam der SoSci Survey zum Einsatz. Die Server befinden sich in Deutschland und bieten einen hohen Datenschutz (DSGVO-konform) für die teilnehmenden Personen an.

4.5.4 Datenauswertung und statistische Verfahren

Die erhobenen Daten der Online-Umfrage wurden nach Bereinigung der Datensätze, diese in die Statistik Software IBM SPSS eingespielt. Anschließend wurden diese mit diesem Tool quantitativ ausgewertet. Ergebnisse der quantitativen Datenauswertung wurden mittels deskriptiver Statistik visuell (als Kuchen-, Balken- und Histogramm) und nummerisch (als Median und Mittelwert) dargestellt. Darüber hinaus wurde auch die Inferenzstatistik angewandt, die eine schließende Statistik mittels t-Test eine Ausprägung der gewonnen Daten zwischen Variablen in der Population die Hypothesen prüft (Döring & Bortz, 2016, S. 52).

5 Ergebnisse und Schlussfolgerungen

In diesem Kapitel werden die Ergebnisse anhand der Aussagen der Expert*Innen auf die jeweiligen Dimensionen und die der durchgeführten Online-Umfrage zusammengefasst bzw. grafisch aufbereitet. Im Zuge der Inhaltsanalyse werden Textpassagen vereinheitlich, um im darauffolgenden Schritt diese interpretieren zu können.

5.1 Ergebnisse Expert*Innen Interview

Die Ergebnisse und die Darstellungen der qualitativen Forschung werden in den nachfolgenden Kapiteln (,vgl. 5.1.1 und 5.1.5) illustriert.

5.1.1 Infrastruktur

Bezüglich der Infrastruktur lässt sich sagen, dass die Anbindungen sei es durch einer der beiden Drahtlostechnologien 5G oder WLAN, oder einer drahtgebundenen Lösung immer auf die Wünsche der Kundschaft und die Möglichkeiten vor Ort ankommt. Diese Ansicht teilen sich alle fünf Expert*Innen. Es bestehen jedoch Unterschiede in Bezug auf die Implementierung und die Installation der Infrastruktur bei der Kundschaft. Unteranderem betonen die Expert*Innen die technologischen Verbesserungen und die Potentiale der Kostenersparnisse. Expert*In 1 regelt die Skalierbarkeit und die Flexibilität durch das eingesetzte Personal, da eine flache Hierarchie im Unternehmen und ein kleines Team rascher auf die Anforderungen reagieren können. Die eingesetzten Produkte sind Linux basierend und werden bei Verbesserungen der Software oder bei entdeckten Sicherheitslücken schnell eingespielt. Expert*In 3 hebt die Architektur der Unternehmen vor, in einem Controller losen Infrastruktur können die Lösungen höher skalieren, Kosten sparen und sind sehr flexibel in ihrem Einsatzgebiet. Expert*In 2 und Expert*In 3 sehen hier auch in den kommenden 6 GHz Frequenzband bei Wifi6 ein großes Potential, da diese wie das 5 GHz Frequenzband eine sehr ähnliche Reichweite haben und noch unbenutzt sind. Expert*In 4 sieht es vor, dass die Standorte vorzugsweise mit einer drahtgebundenen Technologie angebunden werden. Es spricht aber auch nichts gegen eine 5G Verbindung. Hervorgehoben wurde die kritische Latenzzeit bei der Kundschaft und die Verbesserung gegenüber der vierten Mobilfunkgeneration. Expert*In 5 kann mittels dem Network Slicing und dem SDN auf die spezifischen Anforderungen der Kundschaft reagieren. Auch zeitkritische Dienste wie beispielweise das autonome Fahren können aufgrund der hoch automatisierten Infrastruktur problemlos abgearbeitet

werden. Ein wesentlicher Nachteil ist aber die Erneuerungen der kompletten Mobilfunkinfrastrukturen alle fünf Jahre.

Die nachfolgende Abbildung 22 fasst die Aussagen der Expert*Innen zur Dimension Infrastruktur zusammen.

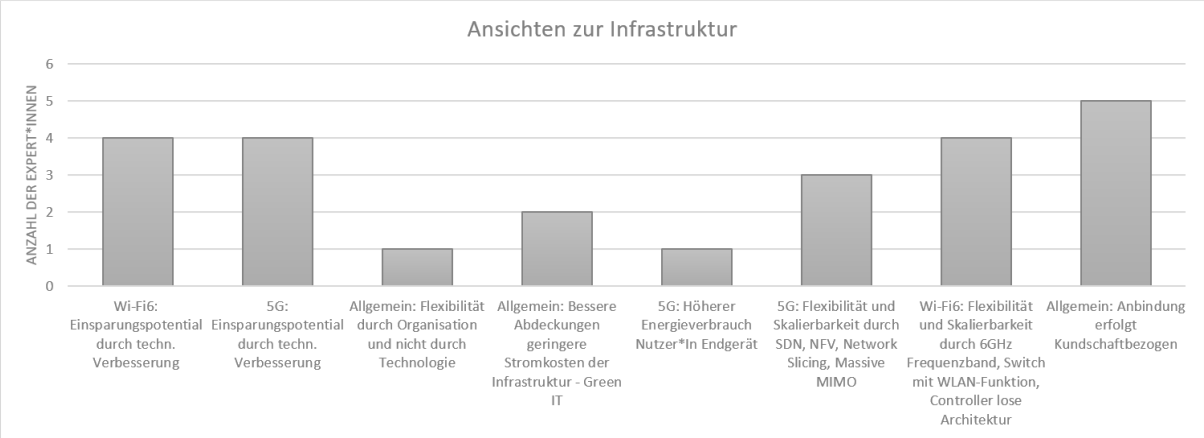

Abbildung 22 - Ansichten zur Infrastruktur

5.1.2 Modulationsverfahren

Drei der fünf Expert*Innen heben das neue Modulationsverfahren OFDMA im Wi-Fi6 Standard hervor. Expert*In 3 ergänzt OFDMA mit 256 Unterkanälen, welche eine Durchsatzsteigerung in unterschiedlichen Zeitfenstern und ein paralleles Senden der Daten ermöglichen („viel effizienter als beim Vorgänger AC“, Anm. Expert*In 3). Expert*In 1 bestätigt ebenfalls, dass die neuen Modulationsverfahren eine Verbesserung im WLAN-Segment darstellen, jedoch die Vorteile aufgrund der fehlerhaften Konfigurationen von den Netzwerkbetreibenden verloren gehen. Die Endgeräte werden von der Kundschaft selbst aufgestellt und konfiguriert, aber nur in seltenen Fällen erfolgt dies von einem Fachpersonal („fast nicht vorhandenen Fall von Expert*Innen in Betrieb genommen“, Anm. Expert*In 1). Um beim Mobilfunkstandard eine effizientere Abdeckung zu erzielen, werden mehrere kleinere Funkzellen laut Expert*In 2, 3, 4, 5 benötigt. Expert*In 5 hebt die Mobilfunkzellen mit den 100-fachen Antennen gegenüber WLAN-Antennen hervor, die ein ähnliches Verfahren zum WLAN besitzen („die Sorgen dafür, dass der Datendurchsatz erheblich höher ist“, Anm. Expert*In 5). Höhere Bandbreiten werden mittels höherer Frequenzen erzielt, welche abhängig von Widerständen (beispielsweise Mauern und Bäume im urbanen Gebieten) in der Sichtverbindung zwischen einem Mobilfunkmasten und den Endgeräten der Nutzer*Innen sind.

Problematisch kann dies beim autonomen Fahren sein, wo geringe Latenzen notwendig sind, laut Expert*In 3 und 5. Übertragungen in niedrigeren Frequenzbereichen sind resistenter gegenüber Störungen als Übertragungen in höheren Frequenzbereichen. Expert*In 2 merkt beim Thema Effizienz die Downlink und Uplink MU-MIMO Technologie an, dass hier eine bessere Nutzung der Funkkapazität ermöglicht wird.

Die nachfolgende Abbildung 23 fasst die Aussagen der Expert*Innen zur Dimension Modulationsverfahren zusammen.

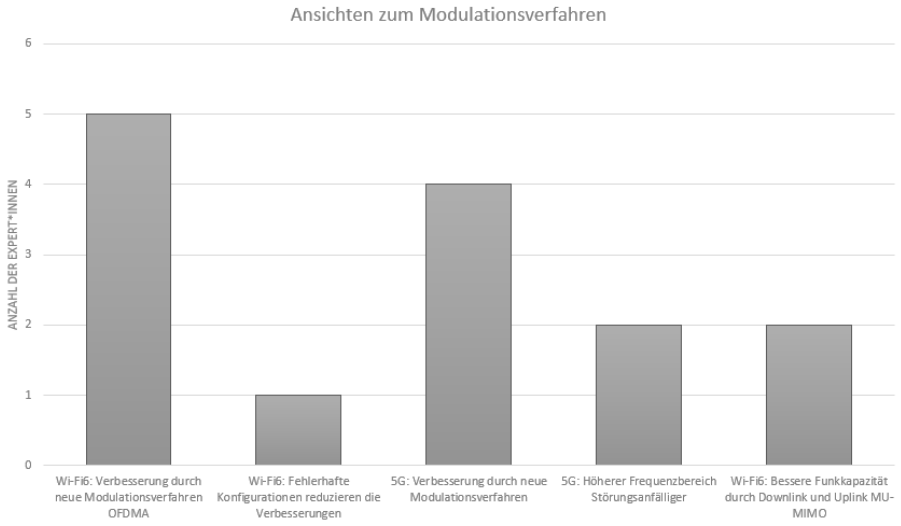

Abbildung 23 - Ansichten zum Modulationsverfahren

5.1.3 Umgebung

Von den befragten Expert*Innen sind sich alle einig, dass im neuen Wi-Fi6 Standard die Probleme in dichten Umgebungen reduziert werden. Bedenken hat Expert*In 1, da eine fehlerhafte Konfiguration eines WLAN-Router die Funkkanäle weiterhin beeinträchtigen werden. Drei von fünf Expert*Innen betonen die neue Funktionalität des BSS Colorings im Wi-Fi6 Standard hervor, wodurch es zu keiner Datenkollision kommt. Expert*In 3 erwähnt den 8-fachen Faktor der Kanalwiederverwendung im Wi-Fi6, in dem es zur effizienteren Kanalnutzung und Spektrum kommt. Im Mobilfunkstandard 5G sind sich vier von fünf Expert*Innen einig, dass es aufgrund der Funkmastdichte im urbanen Gebiet eine verbesserte Netzabdeckung gewährt wird. Zusätzlich wird auf die Problematik mit dem höheren Frequenzspektrum hingewiesen. Höhere Datenübertragungen sind anfälliger auf Frequenzstörungen. Expert*In 3 spricht dabei von einer niedrigeren QAM, da dieser resistenter als die 256QAM im Mobilfunkstandard 5G ist. Im ländlichen Bereich wird die Versorgung nicht wie im urbanen Bereich sein, weil die Infrastrukturkosten

höher sind und es zu geringeren Störungen im 5G-Mobilfunkstandard kommt, laut Expert*In 4. Ein wichtiger Aspekt wird noch von Expert*In 5 ergänzt, es können lizenzierte Netze erworben werden, welche für die eigene Übertragungen verwendet werden.

Die nachfolgende Abbildung 24 fasst die Aussagen der Expert*Innen zur Dimension Modulationsverfahren zusammen.

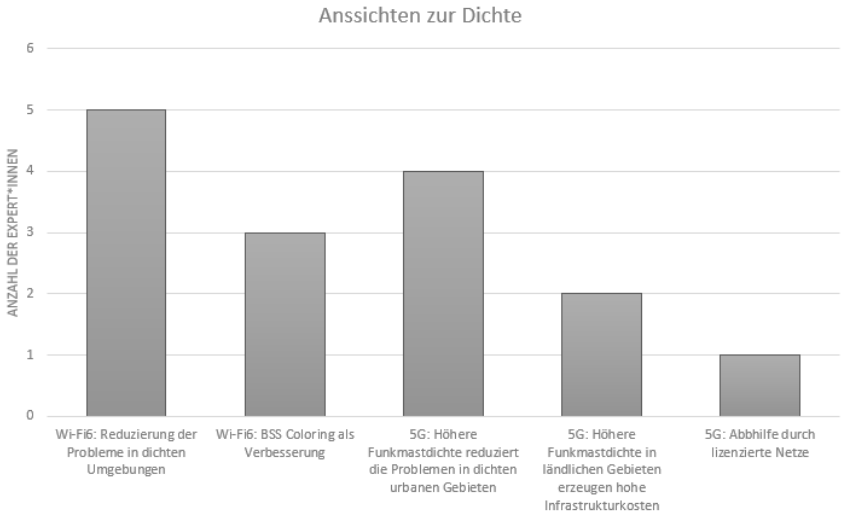

Abbildung 24 - Ansichten zur Dichte

5.1.4 Energie

In Bezug auf die Batterieeffizienz der Endgeräte der Nutzer*Innen, sehen drei von fünf Expert*Innen im WLAN die Funktionalität Target Wake Time (TWT), als eine Verbesserung der energieschonenden Nutzung von Batterien. Eine Kommunikation zwischen einem WLAN-Accesspoint und einem WLAN-Empfangsgerät besteht nur, wenn Netzwerkpakete übermittelt werden müssen („Sleep Mode, keine Antworten nur wenn Traffic herrscht“, Anm. Expert*In 2). Dieser Ansicht ist auch Expert*In 5 der die Verbesserung der WLAN-Chips von den Herstellenden betont und nachfolgende Zusammenfassung ergänzt: Im kommenden 6GHz-Band im WiFi-6 Standard sind weniger Störungen vorhanden, wodurch ein besseres Signal Level existiert und es zu einem geringeren Stromverbrauch bei den Endgeräten kommt. Vergleicht man die Aussagen in Bezug auf den Mobilfunkstandard 5G, sehen vier von fünf Expert*Innen eine Verbesserung der Energieeffizienz. Expert*In 3 merkt die Peak to Avarage Rate an,

dessen Performance im Gegensatz zum Mobilfunkstandard 4G verbessert hat. Ein Problem sieht Expert*In 5 bei den verfügbaren Frequenzen im Mobilfunkstandard 5G. Höhere Bandbreiten benötigen mehr Frequenzen, wodurch der Stromverbrauch der integrierten Chips in Smartphones steigt. Ein Umschalten von den Frequenzen beispielweise zwischen 4G und 5G ist der Grund dafür. Zusammengefasst kann gesagt werden, dass die physikalischen Grenzen der Kapazitäten immer weiterentwickelt werden und bessere Akkulaufzeiten entstehen.

Die nachfolgende Abbildung 25 fasst die Aussagen der Expert*Innen zur Dimension Modulationsverfahren zusammen.

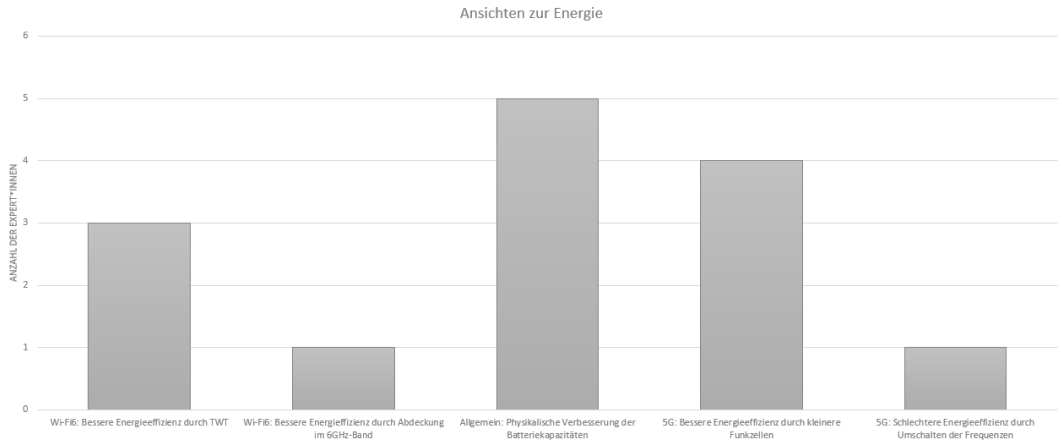

Abbildung 25 - Ansichten zur Energie

5.1.5 Gefahren

Die Gefahren bzw. die Angriffsvektoren in den beiden Drahtlostechnologien Wi-Fi6 und 5G sind weiterhin bestehend. In einem Use Cases wie beispielsweise das autonome Fahren, kommen neue Bedrohungen zum Vorschein, da nun Edge Computing zum Einsatz kommen. Laut allen Expert*Innen besteht die größte Gefahr bei österreichischen WLAN-Providern, dass Hacker*Innen den Datenverkehr mitlesen können, sogenannte Man-in-the-Middle Attacken. Im Jahr 2015 war dieses Angriffsszenario stark verbreitet, da der Datenverkehr nicht verschlüsselt wurde und ein Mitlesen der Daten für kriminelle Personen einfach war, fügte Expert*In 1 hinzu. Abhilfe soll das neue Protokoll Enhanced Open schaffen. Vier von fünf Expert*Innen sehen hier den Vorteil gegenüber komplett offenen WLAN-Hotspots, dass der 4-Wege-Handshake verschlüsselt ist. Ähnlich sieht es Expert*In 3, bei dem eine VPN Verbindung ein zusätzliche Sicherheitsfunktion aktiviert. Expert*In 5 verweist auf die täglichen Angriffe auf die Infrastruktur, sogenannte DDoS-

Attacken („man hört jede Woche von Angriffen auf die Infrastruktur“, Anm. Expert*In 5). Eine Vielzahl von Angriffen sei es physischer Natur oder auch durch Sicherheitslecks in Betriebssystemen, weil diese nicht auf aktuelle Sicherheitsupdates gepatcht wurden. Eine Übernahme durch Hacker*Innen oder eine Zerstörung der Mobilfunkmasten bzw. WLAN-Router, wodurch die Verfügbarkeit nicht garantiert wird, sehen Expert*In 2 und 3 als eine zusätzliche Gefahr. Expert*In 1 negiert diesen Punkt und hebt die Nutzer*Innen selbst als schwächstes Glied hervor. Den Nutzer*Innen fehlt es an Bewusstsein, wodurch eine Effizienz und Sicherheit der Drahtlostechnologie Wi-Fi6 und 5G nicht gegeben ist. Für Expert*In 3,4 und 5 ist das Verschlüsselungsprotokoll 5G-AKA beim Roaming zwischen den Mobilfunkmasten eine wesentliche Verbesserung dem Vorgänger gegenüber. Der definierte Schlüssel kann nicht zurückgerechnet werden und erhöht damit die Sicherheit. Expert*In 2 und 5 definieren im 5G Mobilfunkstandard, dass die Smartphones eher anfälliger sind, da Viren und Schadsoftwares auf dem Endgerät durch die Nutzer*Innen eingeschleust werden. Vier von Fünf Expert*Innen sehen keine negativen Auswirkungen von der Verwendung von WLAN-Hotspots der Nutzer*Innen, da es ein kostenloses Service ist und eine Art der Gewohnheit herrscht.

Die nachfolgende Abbildung 26 fasst die Aussagen der Expert*Innen zur Dimension Modulationsverfahren zusammen.

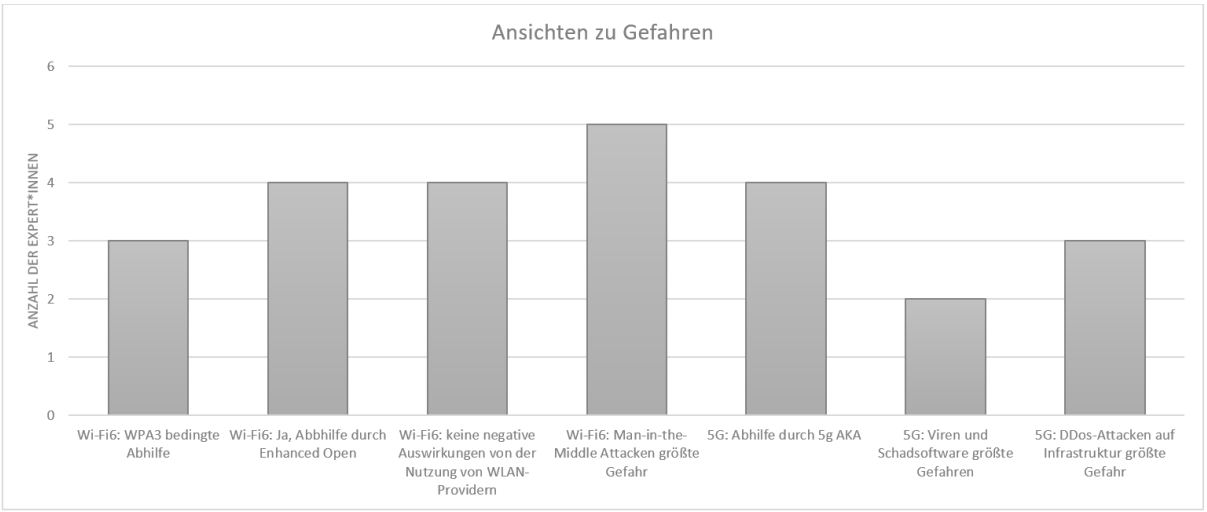

Abbildung 26 - Ansichten zu Gefahren

5.2 Ergebnisse Online-Umfrage

In diesem Kapitel werden die Ergebnisse der Online-Umfrage deskriptiv beschrieben (, vgl. Kapitel 5.2.1 und 5.2.2), sowie die aufgestellten Hypothesen für die quantitative Messung beantwortet (, vgl. Kapitel 5.2.4).

5.2.1 Auswertung der Stichprobe nach soziodemografischen Merkmalen

Das Interview wurde 113-mal angeklickt und geöffnet, jedoch wurden nur 99 Datensätze als gültige Fälle deklariert. Die Rücklaufquote der Online-Umfrage liegt bei 87,61%. Von den 99 Datensätzen haben 90,9% (n=90) einen österreichischen WLAN-Hotspot schon genutzt. Als Auswahlkriterium zählt nur ein komplett ausgefüllter Online-Fragebogen (bis Seite 5) als vollwertig. Von den 99 Datensätzen sind 30,3% (n=30) weibliche, 68,7% (n=68) männliche und 1% (n=1) diverse Personen (, vgl. Abbildung 27). Es ist zu erkennen, dass fast zwei Drittel der Befragten Personen Männer waren.

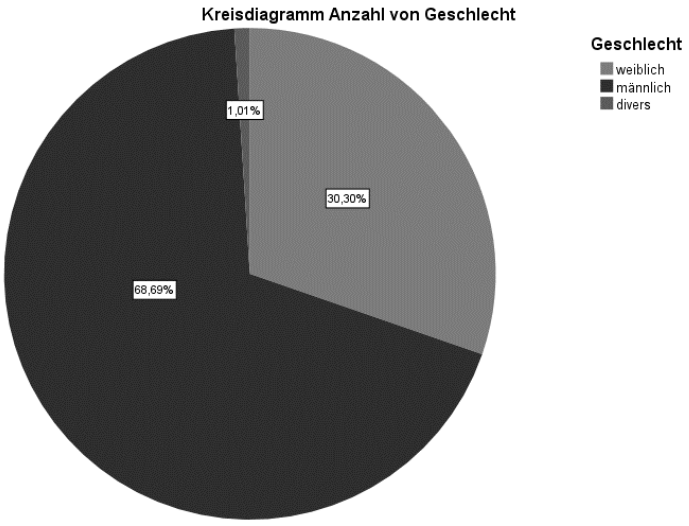

Abbildung 27 – Ergebnis der prozentuellen Geschlechterzusammensetzung

Von den teilnehmenden Personen bildete die Gruppe der 30 bis 34 Jahren von 21,2% (n=21) die größte Teilnahme an der Online-Umfrage. Dichtgefolgt von den beiden Gruppen der 25 bis 29 Jahren von 20,2% (n=20) und der 35 bis 39 Jahren von 20,20% (n=20). Die viertgrößte Gruppe bilden die 40 bis 44-Jährigen von 13,1% (n=13). Der Mittelwert der Altersgruppe liegt bei 5,6 und deutet daraufhin, dass die durchschnittliche teilnehmende Person der Online-Umfrage zwischen 30 und 39 Jahre alt und männlich war (, vgl. Abbildung 28). Eine Person der Altersgruppe 65 Jahre oder älter, gab das Geschlecht divers an und lag bei 1% (n=1).

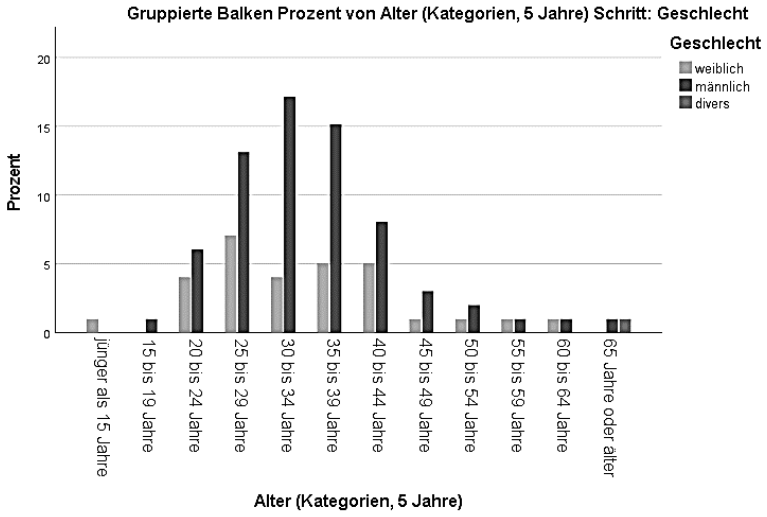

Abbildung 28 – Ergebnis der prozentuellen Altersverteilung nach Geschlechtern

Bei der Auswertung der teilnehmenden Personen betreffend deren Mobilfunkverträgen, teilen sich Magenta (n=26) und Drei (n=26) mit je 26,26% den ersten Platz. Auf den dritten Platz folgt der Mobilfunkvertrag von A1 (n=19) mit 19,19%. Diese drei Mobilfunkverträge der teilnehmenden Personen bilden mehr als die Hälfte ab, in Summe 71,71% (n=71). Den Rest der Kategorie Mobilfunkverträge bilden HoT mit 10,10% (n=10), sonstige Anbieter mit 7,07% (n=7), Bob mit 6,06% (n=6) und als letzter Yesss mit 5,05% (n=5) (, vgl. Abbildung 29).

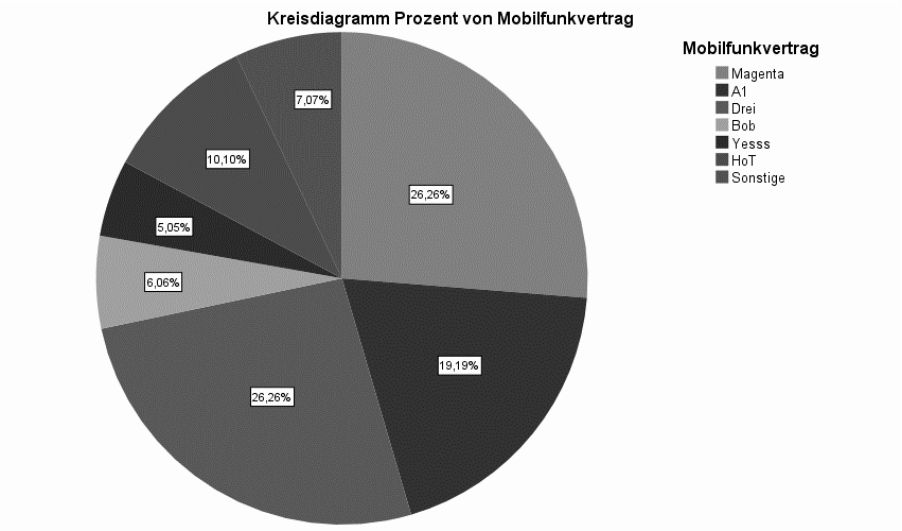

Abbildung 29 – Ergebnis der prozentuellen Verteilung nach Mobilfunkverträge

Bezüglich der formalen Bildung stehen sich zwei gleichgroße Gruppen gegenüber, und zwar Personen mit einem Abschluss einer Universität/FH/Akademien zu 36,36% (n=36) und einer abgeschlossenen Matura zu 36,36% (n=36). 22,22% (n=22) haben eine Lehre bzw. eine mittlere Schule abgeschlossen und nur 5,05% (n=5) besitzen einen Pflichtschulabschluss.

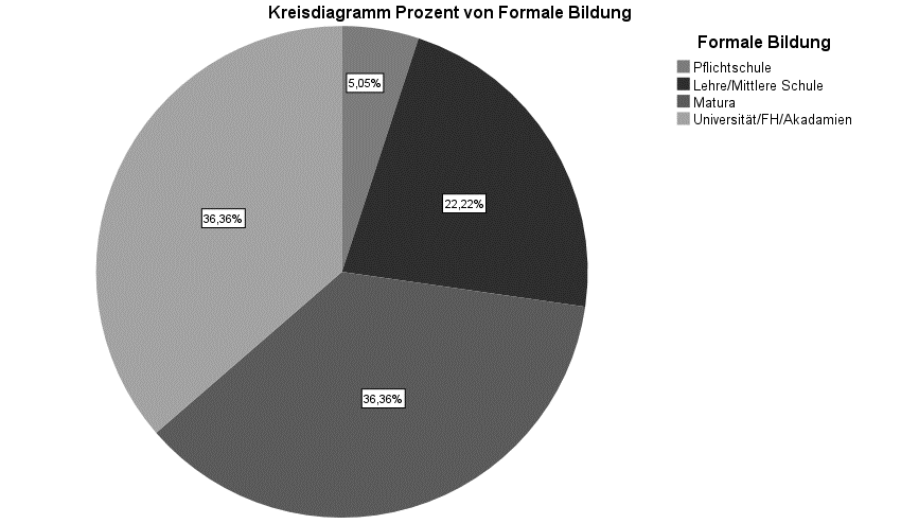

Abbildung 30 - Ergebnis der prozentuellen Verteilung nach der formalen Bildung

5.2.2 Auswertung der Effizienz anhand deskriptiver Statistik

In der Tabelle 6 werden die Fragen bzgl. der Rubrik Effizienz (EF) deskriptiv ausgewertet und grafisch mittels Histogramme visualisiert. Die Frage *„ich verwende österreichischen WLAN-Provider, weil“* stellen die Beweggründe einer Nutzung eines österreichischen WLAN-Provider dar. Um eine Aussage treffen zu können, wird der Mittelwert, der Median, die Standardabweichung und das Quartil (Perzentil) der einzelnen Item-Fragen berechnet.

Statistiken

		Es geht um Effizienz WLAN gegenüber 5G: ich mir Datenvolumen beim eigenen Mobilfunkvertrag sparen möchte	Es geht um Effizienz WLAN gegenüber 5G: ich dadurch schnelleres Internet habe	Es geht um Effizienz WLAN gegenüber 5G: meine aufgerufenen Webseiten und Applikationen schneller laden	Es geht um Effizienz WLAN gegenüber 5G: das angebotene Service kostenlos ist	Es geht um Effizienz WLAN gegenüber 5G: mein Mobilfunkempfang im Indoorbereich schlechter ist	Es geht um Effizienz WLAN gegenüber 5G: mein Mobilfunkempfang im Outdoorbereich schlechter ist	Es geht um Effizienz WLAN gegenüber 5G: mein Mobilfunkanbieter keine gute nationale Abdeckung hat	Es geht um Effizienz WLAN gegenüber 5G: der Akku meines Endgeräts länger hält
N	Gültig	99	99	99	99	99	99	99	99
	Fehlend	0	0	0	0	0	0	0	0
Mittelwert		4,09	3,39	3,46	4,68	3,90	2,90	2,62	2,59
Median		5,00	3,00	4,00	5,00	4,00	3,00	3,00	2,00
Std.-Abweichung		1,980	1,778	1,837	1,621	1,735	1,515	1,455	1,702
Perzentile	25	2,00	2,00	2,00	4,00	3,00	2,00	1,00	1,00
	50	5,00	3,00	4,00	5,00	4,00	3,00	3,00	2,00
	75	6,00	5,00	5,00	6,00	6,00	4,00	4,00	4,00

Tabelle 6 - Auswertung der Häufigkeit Effizienz

Die nachfolgenden Abbildungen stellen die einzelnen Item-Fragen der Online-Umfrage in deren Beantwortung detaillierter dar.

Abbildung 31: Bei der Auswertung der Frage: *„Ich verwende österreichischen WLAN-Provider, weil ich mir Datenvolumen beim eigenen Mobilfunkvertrag sparen möchte“* liegt der Mittelwert bei 4,09 (SD = 1,980) und der Median bei 5.

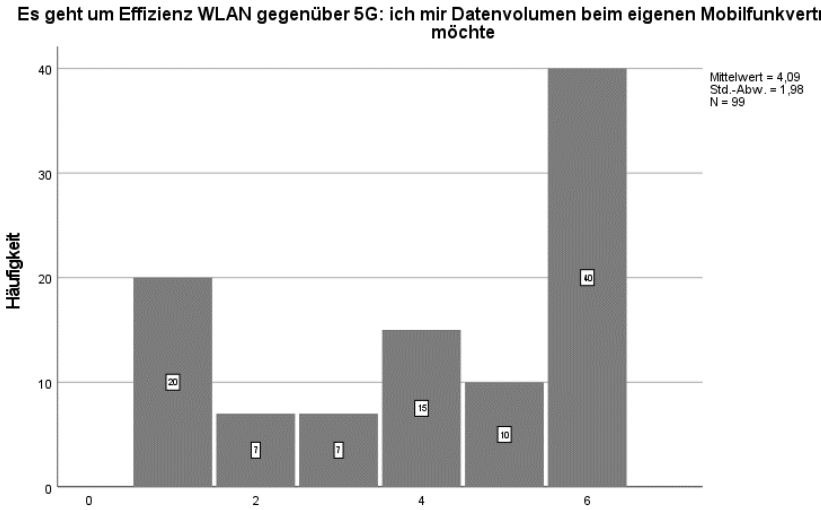

Abbildung 31 - Ergebnis der Frage „ich mir Datenvolumen beim eigenen Mobilfunkvertrag sparen möchte"

Abbildung 32: Bei der Auswertung der Frage: *„Ich verwende österreichischen WLAN-Provider, weil ich dadurch schnelleres Internet habe“* liegt der Mittelwert bei 3,39 (SD = 1,778) und der Median bei 3.

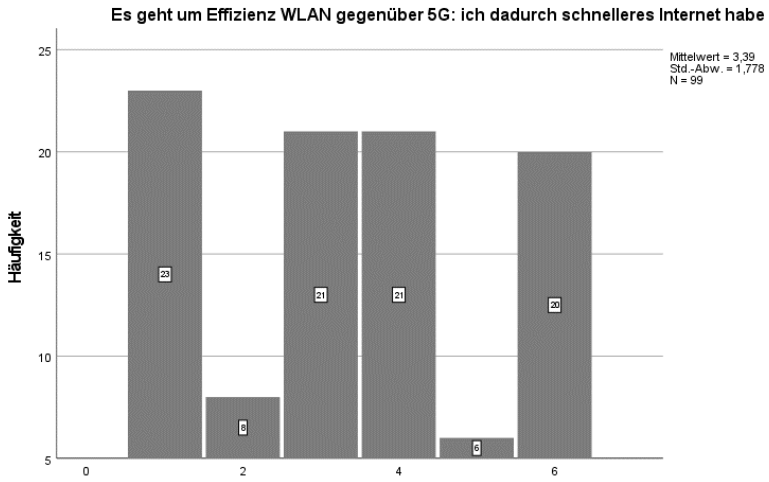

Abbildung 32 - Ergebnis der Frage „ich dadurch schnelleres Internet habe“

Abbildung 33: Bei der Auswertung der Frage*: „Ich verwende österreichischen WLAN-Provider, weil meine aufgerufenen Webseiten und Applikationen schneller laden“* liegt der Mittelwert bei 3,46 (SD = 1,837) und der Median bei 4.

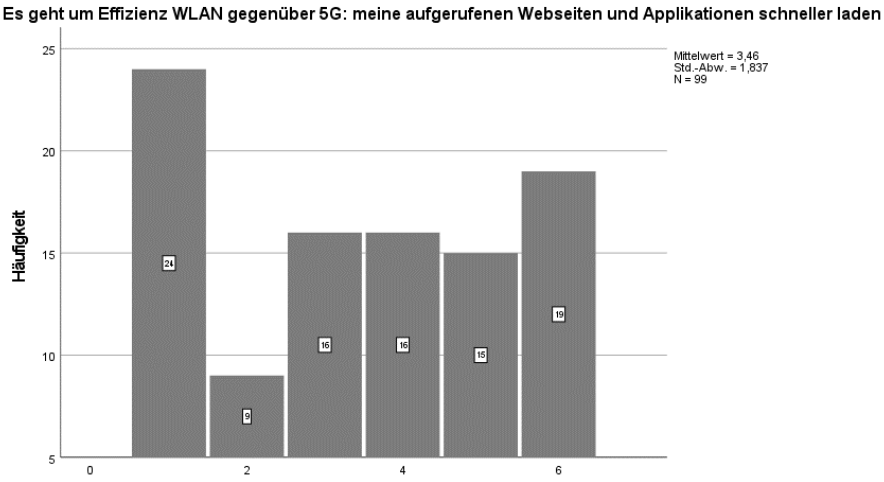

Abbildung 33 - Ergebnis der Frage „meine aufgerufenen Webseiten und Applikationen schneller laden“

Abbildung 34: Bei der Auswertung der Frage*: „Ich verwende österreichischen WLAN-Provider, weil das angebotene Service kostenlos ist“* liegt der Mittelwert bei 4,68 (SD = 1,621) und der Median bei 5.

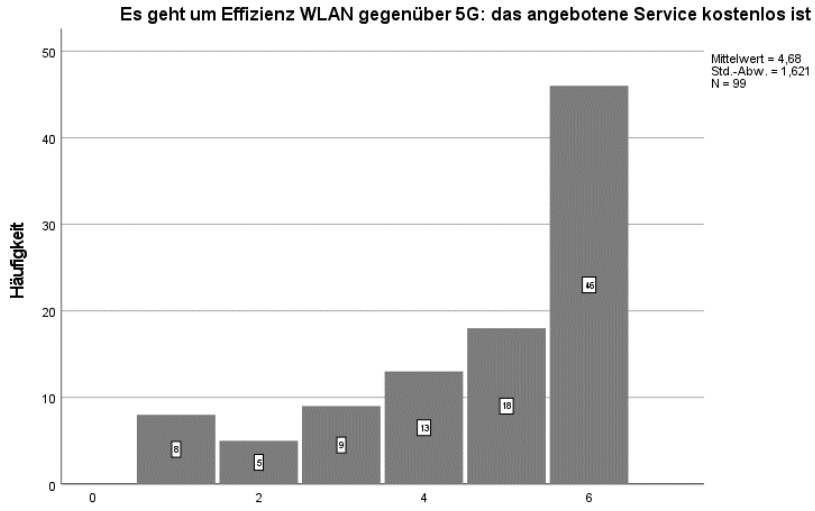

Abbildung 34 - Ergebnis der Frage „das angebotene Service kostenlos ist"

Abbildung 35: Bei der Auswertung der Frage*: „Ich verwende österreichischen WLAN-Provider, weil mein Mobilfunkempfang im Indoorbereich schlechter ist“* liegt der Mittelwert bei 3,90 (SD = 1,735) und der Median bei 4.

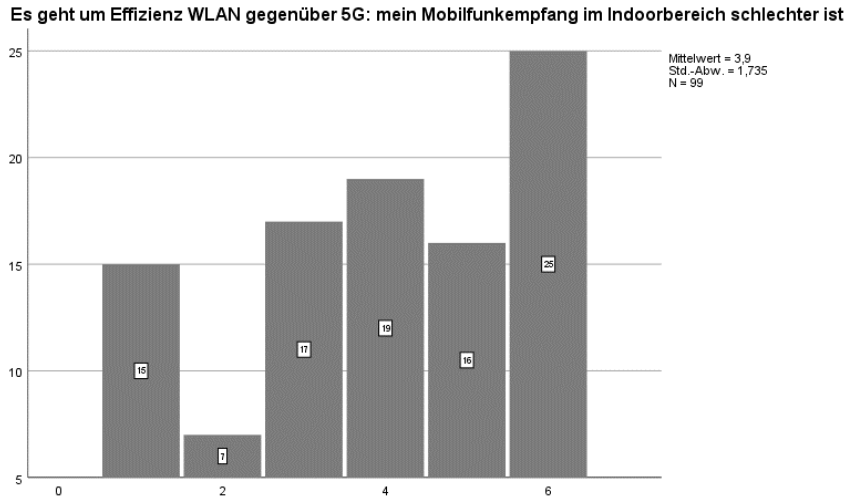

Abbildung 35 - Ergebnis der Frage „mein Mobilfunkempfang im Indoorbereich schlechter ist"

Abbildung 36: Bei der Auswertung der Frage*: „Ich verwende österreichischen WLAN-Provider, weil mein Mobilfunkempfang im Outdoorbereich schlechter ist“* liegt der Mittelwert bei 2,90 (SD = 1,515) und der Median bei 3.

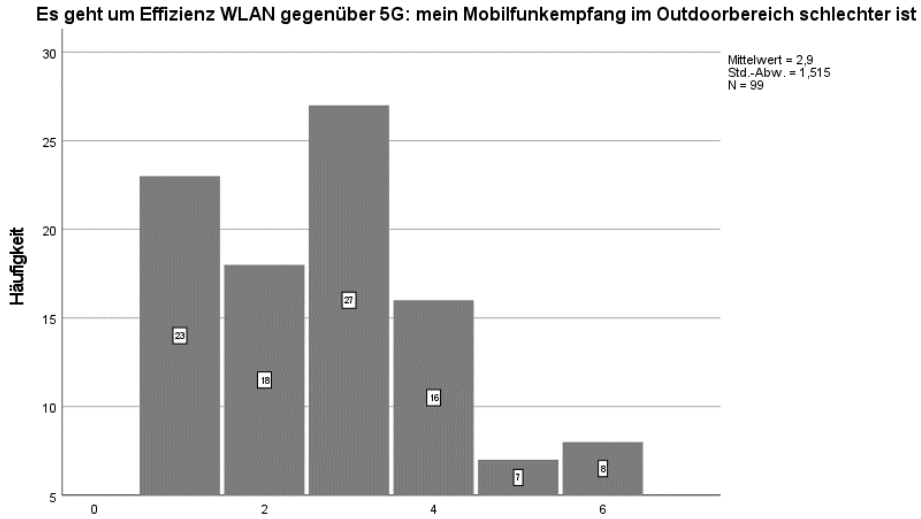

Abbildung 36 - Ergebnis der Frage „mein Mobilfunkempfang im Outdoorbereich schlechter ist"

Abbildung 37: Bei der Auswertung der Frage*: „Ich verwende österreichischen WLAN-Provider, weil mein Mobilfunkanbieter keine gute nationale Abdeckung hat“* liegt der Mittelwert bei 2,62 (SD = 1,455) und der Median bei 3.

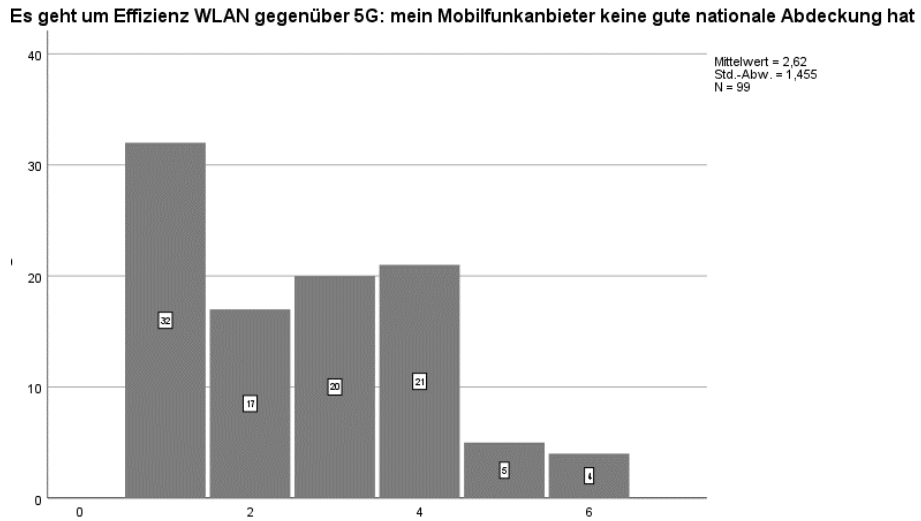

Abbildung 37 - Ergebnis der Frage „mein Mobilfunkanbieter keine gute nationale Abdeckung hat“

Abbildung 38: Bei der Auswertung der Frage*: „Ich verwende österreichischen WLAN-Provider, weil der Akku meines Endgeräts länger hält“* l liegt der Mittelwert bei 2,59 (SD = 1,702) und der Median bei 2.

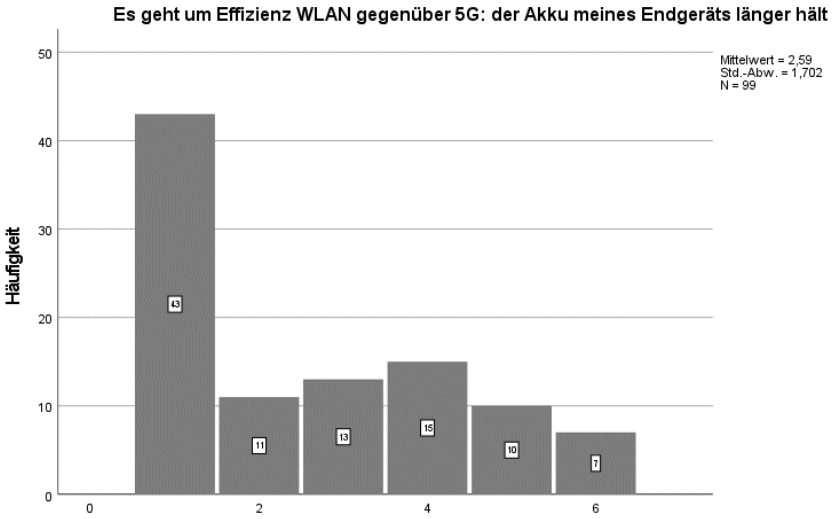

Abbildung 38 - Ergebnis der Frage „der Akku meines Endgeräts länger hält“

5.2.3 Auswertung der Sicherheit anhand deskriptiver Statistik

Mittels der deskriptiven Statistik sind die Fragen aus der Rubrik Sicherheit (SI) „*Die Nutzung von österreichischen WLAN-Hotspots sind sicher, weil*“ ausgewertet und grafisch dargestellt (, vgl. Tabelle 7). Der Mittelwert, der Median, die Standardabweichung und das Quartil (Perzentil) der einzelnen Item-Fragen wurden berechnet.

Statistiken

		Es geht um Sicherheit WLAN gegenüber 5G: ich nur verschlüsselte Webseiten aufrufe	Es geht um Sicherheit WLAN gegenüber 5G: ich einen VPN-Dienst für die Verschlüsselung nutze	Es geht um Sicherheit WLAN gegenüber 5G: ich keine persönlichen Login-Daten auf Webseiten eingebe	Es geht um Sicherheit WLAN gegenüber 5G: der WLAN-Provider aktuelle Sicherheitsprotokolle verwendet	Es geht um Sicherheit WLAN gegenüber 5G: der WLAN-Provider seine Hardware und Software vor Dritten schützt	Es geht um Sicherheit WLAN gegenüber 5G: Hacker*Innen die Kommunikation nicht mitlesen können	Es geht um Sicherheit WLAN gegenüber 5G: mein Endegeräte die aktuellsten Updates besitzen
N	Gültig	99	99	99	99	99	99	99
	Fehlend	0	0	0	0	0	0	0
Mittelwert		3,14	2,97	3,64	3,43	3,46	2,80	4,33
Median		3,00	3,00	4,00	4,00	4,00	3,00	5,00
Std.-Abweichung		1,629	1,821	1,854	1,486	1,668	1,512	1,666
Perzentile	25	2,00	1,00	2,00	2,00	2,00	1,00	3,00
	50	3,00	3,00	4,00	4,00	4,00	3,00	5,00
	75	4,00	4,00	5,00	4,00	5,00	4,00	6,00

Tabelle 7 - Auswertung der Häufigkeit Sicherheit

5.2.4 Auswertung der aufgestellten Hypothesen

Um die aufgestellten Hypothesen verifizieren zu können, wurde die interne Konsistenz der Sicherheitsskala aufgestellt (, vgl. Tabelle 8). Cronbach's Alpha = .722, zeigt eine ausreichende interne Konsistenz an, die Fragen korrelieren ausreichend miteinander. Zusätzlich wurde die Berechnung des Mittelwertscores für die Sicherheit durchgeführt (, vgl. Tabelle 9).

Reliabilitätsstatistiken

Cronbachs Alpha	Anzahl der Items
,722	7

Tabelle 8 - Ergebnis interne Konsistenz

Skala-Statistiken

Mittelwert	Varianz	Std.-Abweichung	Anzahl der Items
23,78	51,032	7,144	7

Tabelle 9 - Ergebnis Mittelwertscore Sicherheit

Hypothese 1 - Männer und Frauen unterscheiden sich in der angegebenen Bedeutung von Sicherheit

Die nachfolgenden Histogramme (, vgl. Abbildung 39 und Abbildung 40) zeigen keine essenzielle Abweichung von der Normalverteilung dar.

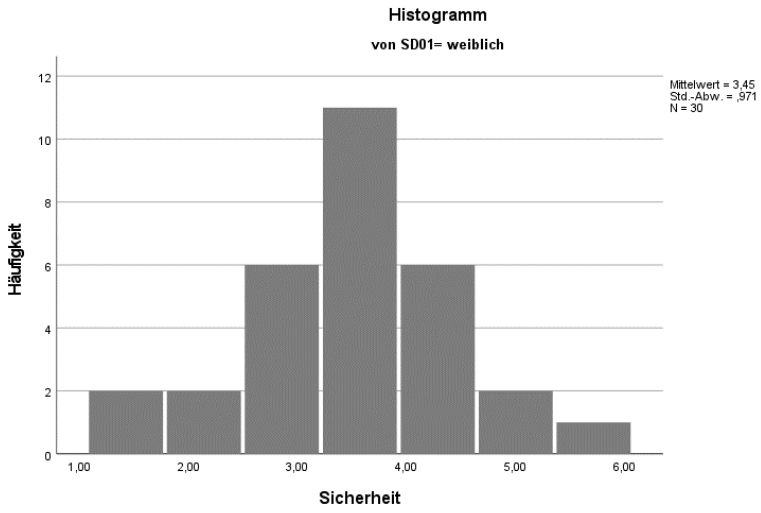

Abbildung 39 - Ergebnis des weiblichen Geschlechts

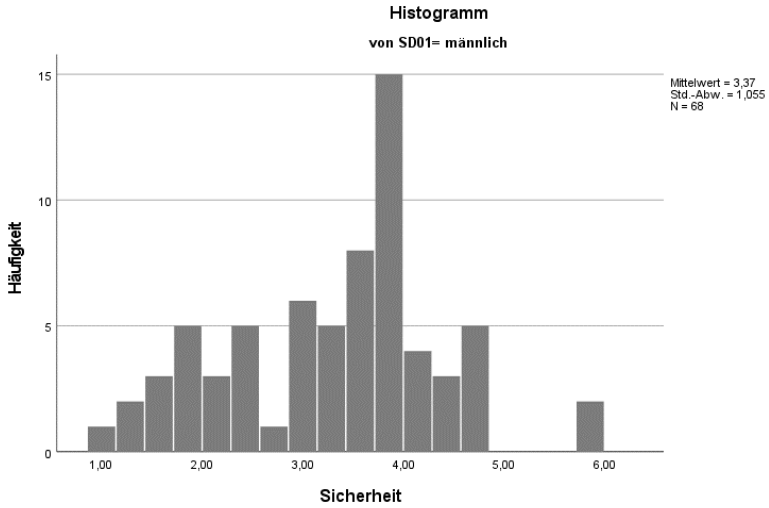

Abbildung 40 - Ergebnis des männlichen Geschlechts

Der Shapiro-Wilk Test ist für beide Gruppen nicht signifikant (, vgl. Tabelle 10).:

$$\text{Frauen - } W(30) = 0.96,\ p = .332 \tag{1.1}$$

$$\text{Männer, } W(68) = 0.97,\ p = .133 \tag{1.2}$$

Tests auf Normalverteilung[b]

		Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Geschlecht	Statistik	df	Signifikanz	Statistik	df	Signifikanz
Sicherheit	weiblich	,154	30	,067	,961	30	,332
	männlich	,120	68	,017	,972	68	,133

a. Signifikanzkorrektur nach Lilliefors

b. Sicherheit ist bei Geschlecht = divers konstant und wird in alle erstellten Boxplots aufgenommen. Es wurde übergangen.

Tabelle 10 - Ergebnis der Normalverteilung

Der Levene-Test zeigt keinen signifikanten Unterschied der Varianz zwischen den Gruppen, $F(1, 96) = 0.78$, $p = .380$. (, vgl. Tabelle 11).

Test bei unabhängigen Stichproben

		Levene-Test der Varianzgleichheit		t-Test für die Mittelwertgleichheit							
						Signifikanz				95% Konfidenzintervall der Differenz	
		F	Sig.	T	df	Einseitiges p	Zweiseitiges p	Mittlere Differenz	Differenz für Standardfehler	Unterer Wert	Oberer Wert
Sicherheit	Varianzen sind gleich	,776	,380	,366	96	,358	,715	,08263	,22580	-,36558	,53085
	Varianzen sind nicht gleich			,378	60,005	,353	,707	,08263	,21863	-,35469	,51995

Tabelle 11 - Ergebnis Levene-Test

Das Ergebnis des t-Test zeigt, dass es keinen signifikanten Unterschied in der Bedeutung von Sicherheit zwischen Männern und Frauen gibt (, vgl. Tabelle 12):

$$M(\text{Frauen}) = 3.45 +/- 0.97,\ M(\text{Männer}) = 3.37 +/- 1.05 \quad (1.3)$$

$$t(96) = 0.37,\ p = .715,\ \text{Cohen's d} = 0.08 \quad (1.4)$$

Effektgrößen bei unabhängigen Stichproben

		Standardisierer[a]	Punktschätzung	95% Konfidenzintervall	
				Unterer Wert	Oberer Wert
Sicherheit	Cohen's d	1,03022	,080	-,350	,510
	Hedges' Korrektur	1,03836	,080	-,347	,506
	Glass' Delta	1,05477	,078	-,352	,508

a. Der bei der Schätzung der Effektgrößen verwendete Nenner.
Cohen's d verwendet die zusammengefasste Standardabweichung.
Hedges' Korrektur verwendet die zusammengefasste Standardabweichung und einen Korrekturfaktor.
Glass' Delta verwendet die Standardabweichung einer Stichprobe von der Kontrollgruppe.

Tabelle 12 - Ergebnis t-Test

Hypothese 2 – Je älter eine Person, desto höher die Bedeutung von Sicherheit

Das Ergebnis der Korrelationsanalyse nach Spearmen zeigt, dass kein signifikanter Zusammenhang zwischen dem Alter und der Bedeutung von Sicherheit existiert (, vgl. Tabelle 13). Der berichtete p-Wert ist zweiseitig, da der Korrelationskoeffizient in die der Hypothese entgegengesetzte Richtung geht.

$$R(97) = -.075,\ p = .459 \quad (1.5)$$

Korrelationen

			Sicherheit	Alter (Kategorien, 5 Jahre)
Spearman-Rho	Sicherheit	Korrelationskoeffizient	1,000	-,075
		Sig. (2-seitig)	.	,459
		N	99	99
	Alter (Kategorien, 5 Jahre)	Korrelationskoeffizient	-,075	1,000
		Sig. (2-seitig)	,459	.
		N	99	99

Tabelle 13 - Ergebnis Spearmen Korrelation

Hypothese 3 – Personen mit unterschiedlichem Bildungsabschluss unterscheiden sich in der angegebenen Bedeutung von Sicherheit

Die nachfolgenden Histogramme (,vgl. Abbildung 41 bis Abbildung 44) zeigen keine essenzielle Abweichung von der Normalverteilung dar.

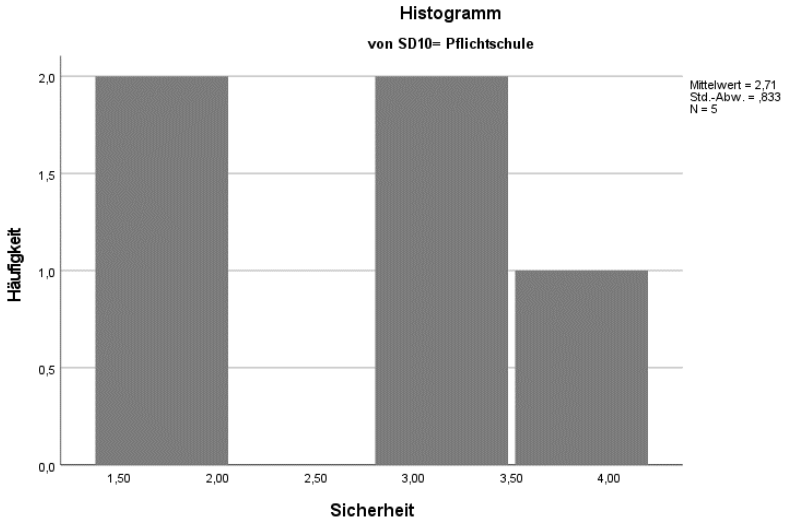

Abbildung 41 - Ergebnis Bedeutung Sicherheit Pflichtschule

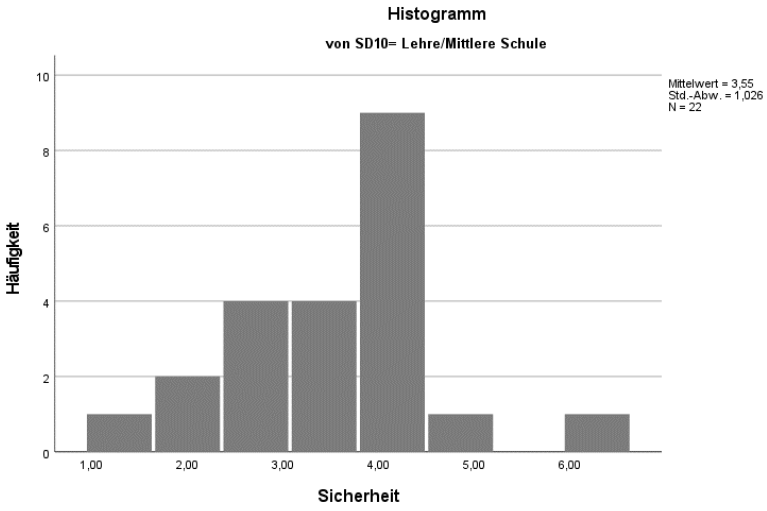

Abbildung 42 - Ergebnis Bedeutung Sicherheit Lehre/Mittelere Schule

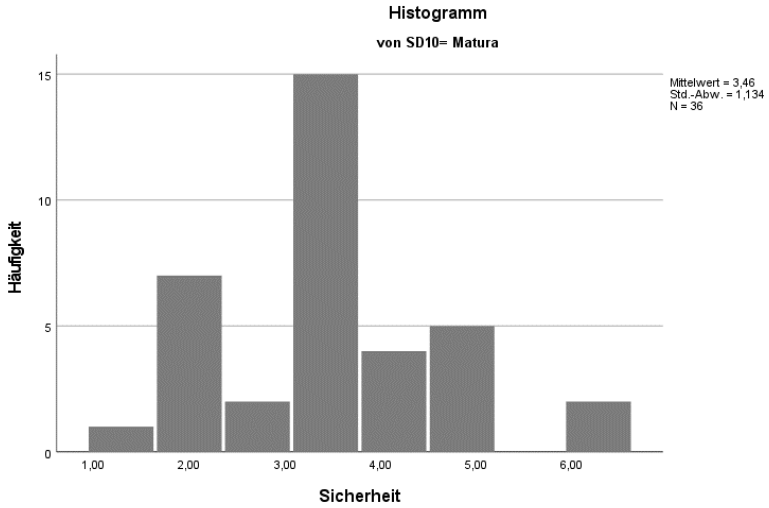

Abbildung 43 - Ergebnis Bedeutung Sicherheit Matura

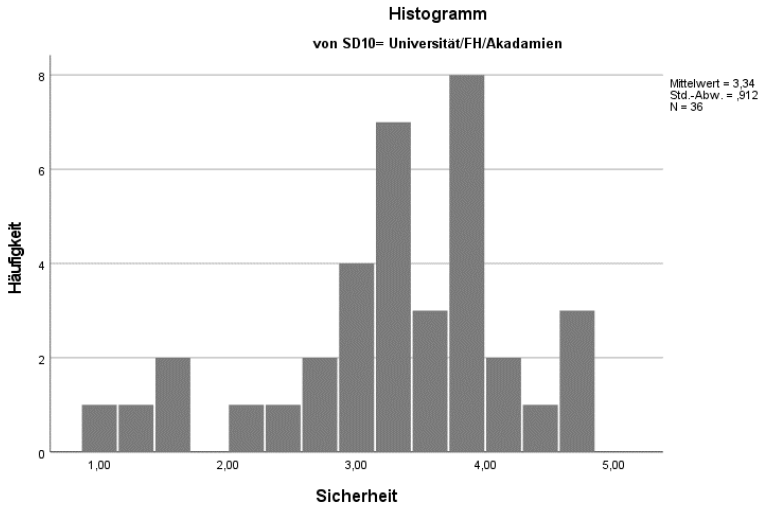

Abbildung 44 - Ergebnis Bedeutung Universität/FH/Akademien

Das Ergebnis der Varianzanalyse zeigt, dass es keinen signifikanten Unterschied in der Bedeutung von Sicherheit für unterschiedliche Bildungsstufen existiert (, vgl. Tabelle 14).

M(Pflichtschule) = 2.71 +/- 0.83, M(Lehre/MittlereSchule) = 3.55 +/- 1.03, M(Matura) = 3.46 +/- 1.13, M(Universität) = 3.34 +/- 0.9 (1.6)

$$F(3, 95) = 1.00,\ p = .398,\ \text{partial eta}^2 = .031 \quad (1.7)$$

Tests der Zwischensubjekteffekte

Abhängige Variable: Sicherheit

Quelle	Typ III Quadratsumme	df	Mittel der Quadrate	F	Sig.	Partielles Eta-Quadrat
Korrigiertes Modell	3,114[a]	3	1,038	,997	,398	,031
Konstanter Term	566,627	1	566,627	544,010	<,001	,851
SD10	3,114	3	1,038	,997	,398	,031
Fehler	98,950	95	1,042			
Gesamt	1244,367	99				
Korrigierte Gesamtvariation	102,063	98				

a. R-Quadrat = ,031 (korrigiertes R-Quadrat = ,000)

Tabelle 14 - Ergebnis der Varianzanalyse

5.3 Diskussion

Die vorliegende wissenschaftliche Arbeit war auf der Suche nach den Bedingungen für die Nutzung eines österreichischen WLAN-Hotspot und deren Sicherheitsaspekt gewidmet. In diesem Kapitel werden die Ergebnisse detaillierter beschrieben und in Zusammenhang gebracht, welche aus der empirischen Datenauswertung hervorgehen und der theoretischen Literaturanalyse beschrieben wurden.

5.3.1 Diskussion der Ergebnisse

Um die Ergebnisse der empirischen Untersuchung zu analysieren und zu interpretieren, werden die Begriffe Effizienz und Sicherheit voneinander getrennt. Ziel ist es, die einzelnen Dimensionen inklusive der daraus gewonnen Erkenntnisse der beiden Forschungsmethoden zu ergänzen und darzustellen.

Der Begriff **Effizienz** ist in fünf Dimensionen unterteilt, bzgl. der Infrastruktur bestätigen alle fünf Expert*Innen, dass die Errichtung von Standorten abhängig von den Möglichkeiten vor Ort ist. Zusätzlich wird auch auf die Wünsche der Kundschaft eingegangen. Technologische Verbesserungen der beiden Drahtlosstandards 5G und Wi-Fi 6 bringen einen Charakter des Potentials für die Kosteneinsparung mit sich. Das neue Frequenzband 6 GHz und die neuen Controller losen Architekturen, besitzen eine hohe Flexibilität und Skalierbarkeit, wodurch auch die Nutzer*Innen profitieren werden. Für eine zusätzliche WLAN-Abdeckung können Switche mit integrierten WLAN-Antennen betrieben werden. Betrachtet man das Ergebnis der quantitativen Forschung und die Frage „I*ch verwende österreichischen WLAN-Provider, weil mein Mobilfunkempfang im Indoor schlechter ist*“, ist zu erkennen, dass viele Nutzer*Innen keine optimale Mobilfunkabdeckung in Gebäuden haben. 5G Mobilfunkanbietende wollen mit SDN, Network Slicing und massive MIMO die Probleme des Mobilfunkstandard 4G verringern

bzw. lösen. Für die Kundschaft können spezifische Anforderungen umgesetzt werden und die Probleme mit schlechten Mobilfunkempfang im Indoorbereich verbessern. Im Outdoorbereich sehen die Expert*Innen keine Probleme bzgl. der Netzabdeckung. Auch die Frage *„Ich verwende österreichischen WLAN-Provider, weil mein Mobilfunkempfang im Outdoor schlechter ist“* bestätigt, dass die Mobilfunkabdeckung in diesem Segment weniger betroffen ist. Die zwei Fragen *„ich verwende österreichischen WLAN-Provider, weil ich mir Datenvolumen beim eigenen Mobilfunkvertrag sparen möchte“* und *„ich verwende österreichischen WLAN-Provider, weil das angebotene Service kostenlos“* zeigen, dass die Nutzer*Innen ein Einsparungspotenzial beim eigenen Mobilfunkanbietenden sehen und es kostenlos ist. Es lässt sich daraus schließen, sollten Nutzer*Innen keine optimale Mobilfunkabdeckung haben, dann werden nach Alternativen gesucht und im Indoorbereich wird ein österreichischer WLAN-Hotspot genutzt.

Die Dimension Modulationsverfahren zeigt, dass das neue Modulationsverfahren OFDMA für Wi-Fi6 effizienter bei der Datenübertragung ist und eine verbesserte Durchsatzsteigerung ermöglicht. Um diesen Effekt nicht zu verlieren, müssen die Komponenten lt. Expert*In 1 ordnungsgemäß konfiguriert werden. Die Auswertung der Frage *„Ich verwende österreichischen WLAN-Provider, weil ich dadurch schnelleres Internet habe“* ergab, dass diese weniger aufgrund der Schnelligkeit genutzt werden. Zukünftige österreichische WLAN-Hotspots könnten diesen Faktor positiv beeinflussen, bei der Integration und Aufbau des neuen Wi-Fi6 Standards. Höhere Bandbreiten verwenden höhere Frequenz, die jedoch von Widerständen bei der Sichtverbindung zwischen Endgerät der Nutzer*Innen und den sendenden Antennen unterbrochen werden. Daher kann es bei kritischen Anwendungsszenarien (‚wie beispielsweise das autonome Fahren) zu gröberen Problemen führen. In Bezug auf die Frage *„Ich verwende österreichischen WLAN-Provider, weil meine aufgerufenen Webseiten und Applikationen schneller laden“,* ergab die Auswertung, dass bei der Nutzung eines österreichischen WLAN-Hotpots Webseiten und Applikationen schneller laden. Die Daten werden schneller geladen, da die Latenzzeiten niedriger sind und unterbrechungsfreie Datenübertragung möglich ist.

In Hinblick auf die Dimension Umgebung, bestätigen alle Expert*Innen weitere Abhilfe in dichten Umgebungen bei der Nutzung von Wi-Fi6. BSS Coloring und die effiziente Kanalnutzung bringen für die Nutzenden weitere Vorteile bei der Drahtlosübertragung. 5G wird im urbanen Gebiet stark ausgebaut, die Probleme mit der Dichte wird durch die Anzahl der Funkmastdichte reduziert. Im ländlichen Gebiet ist eine optimale 5G Mobilfunkabdeckung im urbanen Gebiet kaum möglich, da die Infrastrukturkosten

exponentiell steigen. Generell kann gesagt werden, dass die Mobilfunkabdeckung in Österreich gut ist. Dies wurde auch durch die Auswertung der Frage *„Ich verwende österreichischen WLAN-Provider, weil mein Mobilfunkanbieter keine gute nationale Abdeckung hat“* erhoben. Sind störungsfreie und unabhängige Frequenzen relevant, so können lizenzierte Frequenzen erworben werden.

Ein wesentlicher Aspekt ist die Batterieeffizienz der Endgeräte der Nutzer*Innen. Die Endgeräte kommunizieren durchgehend mit dem WLAN-Accesspoint oder mit dem Mobilfunkmasten. Die nächste Dimension Energie beinhaltet die Verbesserung der energieschonenden Nutzung von Batterien. Eine Abhilfe im WLAN-Segment wird durch Target Wake Time (TWT) erzielt. Das Endgerät und der WLAN-Accesspoint kommunizieren nur wenn es notwendig ist, eine durchgehende Verbindung ist nicht notwendig. Dadurch wird die Batterie geschont und die Batterielaufzeit verlängert. Auch beim Mobilfunkstandard 5G kommt es zur Verbesserung der effizienten Energienutzung. Aktuell wird durch das Umschalten von den höheren zu den niedrigeren Frequenzen aber auch umgekehrt, der erhöhte Stromverbrauch im Chip hervorgerufen. Ergänzt durch die Frage *„Ich verwende österreichischen WLAN-Provider, weil der Akku meines Endgeräts länger hält“* ist zu erkennen, dass dies ein weniger wichtiger Faktor für die Nutzung eines österreichischen WLAN-Hotspots ist. Allgemein ist festzuhalten, dass die physikalischen Verbesserungen die Batteriekapazitäten steigern und dadurch eine längere Batterielaufzeit erzielt wird.

Bezugnehmenden auf den Begriff **Sicherheit** und den potentiellen Gefahren bei der Nutzung österreichischer WLAN-Hotspots wurden die aufgestellten Hypothesen aus Kapitel 4.3.2 widerlegt. Es existieren keine Unterschiede innerhalb der Stichprobe, sei es das Geschlecht, das Alter oder der Bildungsabschluss. Dies deutet daraufhin, innerhalb der Stichprobe das Sicherheitsbewusstsein ident ist.

Die größte Gefahr bei der Nutzung eines österreichischen WLAN-Hotspots besteht bei einer Man-in-the-Middle Attacke, laut den Expert*Innen. Heutzutage ist das Mitlesen der Kommunikation durch den Einsatz neuer Protokolle oder Verschlüsselungen erschwert. In der Vergangenheit war das Mitlesen für Hacker*Innen einfacher, da es nur unverschlüsselte Webseiten gab. Nutzer*Innen verwenden teilweise einen VPN-Zugang, rufen nur verschlüsselte Webseiten auf und geben keine persönlichen Login-Daten ein (, vgl. Tabelle 7). Zusätzlich bieten die neuen Protokolle einen verbesserten Schutz gegenüber kriminellen Personen, sei es im Mobilfunk oder WLAN an. Die Nutzer*Innen werden von Enhanced Open bei offenen WLAN-Hotspots profitieren. Zukünftig werden

vor allem in offenen öffentlichen Hotspots die Nutzer*Innen profitieren. Im Rahmen der quantitativen Forschung wurde die Frage *„Die Nutzung von österreichischen WLAN-Hotspots sind sicher, weil der WLAN-Provider aktuelle Sicherheitsprotokolle verwendet“* mit einem Mittelwert von 3,43 (SD = 1,486) und Median von 4 angegeben. Das neue Verschlüsselungsprotokoll WPA3 wird auch einen großen Teil beitragen, sobald alle Endgeräte dies unterstützen. Äußerst positiv ist anzumerken, dass die Endgeräte der Nutzer*Innen am aktuellsten Stand sind. Vieren und Schadsoftwares können nur einen begrenzten Schaden bei den Nutzer*Innen hervorrufen. Die Frage *„Die Nutzung von österreichischen WLAN-Hotspots sind sicher, mein Endgerät die aktuellsten Updates besitzen“*, wurde mit einem Mittelwert von 4,33 (SD = 1,666) und Median von 5 ausgewertet und bildet die höchste Bewertung bei der Online-Umfrage. Beim Mobilfunk 5G, sehen drei von fünf Expert*Innen die größte potentielle Gefahr auf die Infrastruktur von DDoS-Attacken ausgehend. Die drei Säulen der CIA-Triade (, vgl. Kapitel 2.4) sind dadurch in Gefahr. Des Weiteren wird der physische Schutz oder die feindliche Übernahme durch Sicherheitslecks der eingesetzten Hardware als weitere Angriffsvektoren der Mobilfunkanbietenden genannt. Beim Roaming zwischen den Mobilfunkmasten bringt das neue 5G-AKA Verschlüsselungsprotokoll eine wesentliche Verbesserung.

Resümierend kann gesagt werden, dass einige Faktoren die Nutzung eines österreichischen WLAN-Hotspots begünstigen. Drei wesentliche Faktoren sind die kostenlose Nutzung, Datenvolumen zu sparen und dass die Mobilfunkabdeckung in Indoorbereichen nicht zufriedenstellend ist. Die nachfolgende Tabelle 15 soll die Rangreihe nach dem berechneten Mittelwert für die Rubrik Effizienz absteigend darstellen:

Itemfragen	Mittelwert	Standardabweichung	Median
das angebotene Service kostenlos ist	**4,68**	**1,621**	**5**
ich mir Datenvolumen beim eigenen Mobilfunkvertrag sparen möchte	4,09	1,980	5
mein Mobilfunkempfang im Indoorbereich schlechter ist	**3,90**	**1,735**	**4**
meine aufgerufenen Webseiten und Applikationen schneller laden	3,46	1,837	4
ich dadurch schnelleres Internet habe	**3,39**	**1,778**	**3**
mein Mobilfunkempfang im Outdoorbereich schlechter ist	2,90	1,515	3
mein Mobilfunkanbieter keine gute nationale Abdeckung hat	**2,62**	**1,455**	**3**
der Akku meines Endgeräts länger hält	2,59	1,702	2

Tabelle 15 - Rangliste Effizienz

Das Sicherheitsbewusstsein unterscheidet sich bei den Nutzer*Innen in der Stichprobe nicht. Diese sind für die Sensibilisierung im Sicherheitsaspekt selbstverantwortlich und werden in Zukunft durch technologische Verbesserungen und Sicherheitsmechanismen stetig profitieren. Bestehende Angriffsvektoren wie das Mitlesen der Datenkommunikation bildet die größte Gefahr bei einer Nutzung der österreichischen WLAN-Providern für die Nutzer*Innen. Endgeräte der Nutzer*Innen sind auf dem neuersten Sicherheitsstand und schließen Sicherheitslücken für Ransomware, Viren und anderen Schadsoftwaren.

5.3.2 Diskussion der ausgewählten Methode

Diese Masterarbeit wurde mithilfe einer Mixed-Methods-Forschung durchgeführt. Zwei unabhängig voneinander durchgeführte Forschungsstränge, bieten eine gute Möglichkeit das Spektrum zu erweitern bzw. zu ergänzen. Beide Ergebnisse der Forschungsmethoden fließen am Ende in eine Zusammenfassung und bilden eine Ebene. Für die Mixed-Methods-Forschung wurde ein paralleles Design ausgewählt, ein Vertiefungsdesign (sequenzieller Ablauf) wurde bewusst nicht gewählt (Kuckartz, 2014, S. 116). Das Wissen wurde anhand der Literaturrecherche aus der Theorie aufgebaut. Aufgrund der Covid19-Pandemie wurden die Interviews mit den Expert*Innen über MS Teams abgehalten. Auch in einem digitalen Zeitalter, ist eine Interaktion unter vier Augen für die persönliche Wahrnehmung (Gestik, Mimik, usw.) äußerst relevant. Hintergrundgeräusche können die Kommunikation über digitale Medien stören. Die Online-Umfrage ist für eine quantitativen Erhebung sehr hilfreich. Zu beachten ist wie die Fragen gestellt werden, ob diese nach der Erhebung anschließend ausgewertet können und wie die Auswertung mittels statistischer Vorgehensweise durchgeführt werden kann. Die Kombination der qualitativen und quantitativen Forschungsmethode zeigte sich als sehr vorteilhaft für die Beantwortung der Forschungsfrage.

6 Conclusio

6.1 Fazit

Ziel der vorliegenden wissenschaftlichen Arbeit war es, die Bedingungen für die Nutzung eines österreichischen WLAN-Hotspots gegenüber dem Mobilfunkstandard 5G zu identifizieren. Ein wesentlicher Bestandteil der Evaluierung war es auch den Sicherheitsaspekt der Nutzer*Innen zu erforschen. Da es sich bei diesem Thema um ein sehr aktuelles und breites Feld handelt, wurde nur der technologische Aspekt der Drahtlostechnologien Wi-Fi6 und 5G betrachtet.

Aus diesem Grund erfolgten Expert*Innen Interviews mit Personen, die ein spezielles Fachwissen auf dem Gebiet der Drahtlostechnologien besitzen. Die Interviews ergaben, dass die technologischen Verbesserungen positive Auswirkungen auf die Sicherheit aufgrund neuer Sicherheitsprotokolle und auf die Datenübertragung bzw. Datenmenge für die Nutzer*Innen haben wird. Ergänzend wurde eine Online-Umfrage anhand einer willkürlichen Stichprobe durchgeführt. Resultierend aus der Online-Umfrage ergaben sich die Bedingungen einer Nutzung in einer Rangliste wieder.

Aufgrund der Ergebnisse der durchgeführten Interviews und der statistischen Erhebung der Online-Umfrage, kann die in der vorliegenden Arbeit definierte Forschungsfrage mit folgenden Bedingungen beantwortet werden: Österreichische WLAN-Provider werden genutzt,

- Da es ein kostenloses Service ist,
- Um Datenvolumen beim eigenen Mobilfunkvertrag zu sparen und
- Weil die WLAN-Abdeckung im Indoorbereich besser ist als der Mobilfunkempfang

WLAN kompensiert die Schwächen des Mobilfunkstandards 5G, hauptsächlich im Indoorbereich ist kostenloses WLAN ein Standard geworden. Österreichischen WLAN-Provider haben weiterhin eine Existenzberechtigung, wodurch die Nutzer*Innen nach wie vor profitieren. Jene genannten Faktoren konnten nachweislich zur Nutzung eines österreichischen WLAN-Provider beitragen.

In Bezug auf den Sicherheitsaspekt, konnte die aufgestellte Hypothese anhand der Auswertung der statistischen Ergebnisse nicht bestätigt werden. Die Nutzer*Innen unterscheiden sich unabhängig vom Alter, Geschlecht oder Bildungsstand nicht.

Eine umfassende Auseinandersetzung mit einschlägiger Fachliteratur zeigt, dass Forschung auch mittels dieser stattfinden kann. Von wichtiger Bedeutung waren allerdings auch die Aussagen der Expertinnen und Experten, die ihre Erfahrungen aus der Praxis reflektieren konnten.

6.2 Ausblick

Weiterführende Forschungen können die Ergebnisse dieser vorliegenden wissenschaftlichen Arbeit nutzen, um weitere Bestrebungen im Hinblick auf die Implementierung des Verschlüsselungsprotokoll Enhanced Open darzustellen. Aufgrund dieses Protokolls kann die Akzeptanz der Nutzenden vor und nach der Implementierung gemessen werden. Womöglich kann ein WLAN-Provider hierdurch noch mehr profitieren und seine Legimitation bestätigen. Neue Frequenzspektren wie beispielsweise in Wi-Fi 6E, ermöglichen höhere Datenübertragungen. Praxisbezogene Erforschungen könnten sich mit den resistenten Störsignalen und den Line-of-Sight (LoS) im Indoor- und Outdoorbereich beschäftigen.

7 Literaturverzeichnis

3GPP TS. „System Architecture for the 5G System“, 1. Dezember 2021. https://www.etsi.org/deliver/etsi_ts/123500_123599/123501/15.03.00_60/ts_123501v150300p.pdf.

3GPP. „Feasibility Study on New Services and Markets Technology Enablers“. Release 14, 30. September 2016. https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=2897.

A-SIT Zentrum für sichere Informationstechnologie – Austria. „Sicherer Umgang mit WLAN-Hotspot“, 20. August 2021. https://www.onlinesicherheit.gv.at/Services/Technologie-Trends/WLAN-Hotspots/Sicherer-Umgang-mit-WLAN-Hotspots.html.

Aguilera, Pablo. *A Hyperconnected World: 802.11ax and the next Generation WiFi*, 2018.

Asfinag Maut Service GmbH. „Gratis Surfen auf Autobahn Rastplätzen“, 25. Juli 2021. https://www.asfinag.at/stat/wifi/pdfs/MSG_Service_GratisWLAN.pdf.

Baur, Nina, und Jörg Blasius, Hrsg. Handbuch Methoden der empirischen Sozialforschung. 2., Vollständig überarbeitete und Erweiterte Auflage. Handbuch. Wiesbaden: Springer VS, 2019.

Bundesamt für Sicherheit in der Informationstechnik. „IT-Grundschutz-Bausteine NET.2.1: WLAN-Betrieb“, Februar 2021. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium_Einzel_PDFs_2021/09_NET_Netze_und_Kommunikation/NET_2_1_WLAN_Betrieb_Edition_2021.pdf;jsessionid=616FBE7FB686AE7C9F3FB8B5961AE0F9.internet081?__blob=publicationFile&v=2.

Cisco Systems. „Cisco Annual Internet Report (2018–2023) White Paper“, 16. Oktober 2021. https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html.

D. Harkins, Ed. und Aruba Networks. „Dragonfly Key Exchange“. Internet Research Task Force (IRTF), 2015. https://datatracker.ietf.org/doc/html/rfc7664.

D. Harkins, Ed., HP Enterprise, und Google. „Opportunistic Wireless Encryption“. Internet Engineering Task Force (IETF), 2017. https://datatracker.ietf.org/doc/html/rfc8110.

Dahlman, Erik, Stefan Parkvall, und Johan Sköld. *5G NR: The next Generation Wireless Access Technology*. Second edition. London San Diego, CA Cambridge, MA Oxford: Elsevier, Academic Press, 2021.

David Coleman. *Wi-Fi 6 for Dummies, Extreme Networks Special Edition*. New York: John Wiley & Sons, Inc., 2021.

David Coleman und Lawrence C. Miller. *Wi-Fi 6 for Dummies, Restech & Aerohive Special Edition*. New York: John Wiley & Sons, Inc., 2018.

DBpedia. „Mobilfunknetzbetreiber“, 15. November 2021. https://dbpedia.org/page/Mobile_network_operator.

Der Rat der Europäischen Union. RICHTLINIE 2008/114/EG DES RATES, Pub. L. No. 2008/114/EG (2008). https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32008L0114&from=HR.

Dieter Burgartz und Ralf Röhring. *Information Security Management, Praxishandbuch für Aufbau, Zertifizierung und Betrieb, Loseblattsammlung*. 41. Aufl. Köln: TÜV Verlag, 2014.

Döring, Nicola, und Jürgen Bortz. *Forschungsmethoden und Evaluation in den Sozial- und Humanwissenschaften*. Springer-Lehrbuch. Berlin, Heidelberg: Springer Berlin Heidelberg, 2016. https://doi.org/10.1007/978-3-642-41089-5.

Ebster, Claus, und Lieselotte Stalzer. *Wissenschaftliches Arbeiten für Wirtschafts- und Sozialwissenschaftler*. 5., Überarbeitete und Erweiterte Auflage. UTB Wirtschaftswissenschaften, Sozialwissenschaften 2471. Wien: facultas, 2017.

Edgeworth, Brad, Jason Gooley, David Hucaby, und Ramiro Garza Rios. *Ccnp and ccie enterprise core encor 300-401 official cert guide*. 1. Aufl. Hoboken: Cisco Press, 2019.

ETSI GR. „Network Functions Virtualisation (NFV); Use Cases“, Mai 2017. https://docbox.etsi.org/isg/nfv/open/Publications_pdf/Specs-Reports/NFV%20001v1.2.1%20-%20GR%20-%20NFV%20Use%20Cases%20revision.pdf.

ETSI TS. „5G; System Architecture for the 5G System“. Release 15, September 2018. https://www.etsi.org/deliver/etsi_ts/123500_123599/123501/15.03.00_60/ts_123501v150300p.pdf.

Europäische Kommission. „Digitaler Binnenmarkt: EU-Verhandlungsführer einigen sich auf WiFi4EU-Initiative“, 1. Oktober 2021. https://ec.europa.eu/commission/presscorner/detail/de/IP_17_1470.

Diekmann, Andreas. *Empirische Sozialforschung: Grundlagen, Methoden, Anwendungen*. 14. Auflage, Originalausgabe. Reinbeck bei Hamburg: rowohlts enzyklopädie im Rowohlt Taschenbuch Verlag, 2021.

Gier, Marcus. *WLAN und Hotspot-Know-how*. 1. Aufl. Köln: Unika-Fachverl, 2006.

Edgeworth, Brad, Jason Gooley, David Hucaby, und Ramiro Garza Rios. *Ccnp and ccie enterprise core encor 300-401 official cert guide*. 1. Aufl. Hoboken: Cisco Press, 2019.

Greene, Jennifer C., Valerie J. Caracelli, und Wendy F. Graham. „Toward a Conceptual Framework for Mixed-Method Evaluation Designs“. *Educational Evaluation and Policy Analysis* 11, Nr. 3 (September 1989): 255–74. https://doi.org/10.3102/01623737011003255.

Henry, Jerome, Barton, Robert, und Hucaby, David. *CCNP Enterprise Wireless Design and Implementation - ENWLSD 300-425 and ENWLSI 300-430 Official Cert Guide Designing & Implementing Cisco Enterprise Wireless Networks*, 2020. http://www.vlebooks.com/vleweb/product/openreader?id=none&isbn=9780136600909.

Hug, Theo, Gerald Poscheschnik, und Bernd Lederer. Empirisch forschen: die Planung und Umsetzung von Projekten im Studium. 2., Überarb. Aufl. UTB Schlüsselkompetenzen 3357. Konstanz München: UVK-Verl.-Ges, 2015.

Kaiser, Robert. *Qualitative Experteninterviews: Konzeptionelle Grundlagen und praktische Durchführung*. Springer, 2014. https://doi.org/10.1007/978-3-658-02479-6.

Khorov, Evgeny, Anton Kiryanov, Andrey Lyakhov, und Giuseppe Bianchi. „A Tutorial on IEEE 802.11ax High Efficiency WLANs“. *IEEE Communications Surveys & Tutorials* 21, Nr. 1 (2019): 197–216. https://doi.org/10.1109/COMST.2018.2871099.

Kotler, Philip, und Friedhelm Bliemel. *Marketing-Management. Hauptbd.* 10., Überarb. und Aktualisierte Aufl. Stuttgart: Schaeffer-Poeschel, 2001.

Kuckartz, Udo. Mixed Methods: Methodologie, Forschungsdesigns und Analyseverfahren. Mixed Methods. Wiesbaden: Springer VS, 2014.

Kukushkin, Alexander. Introduction to mobile network engineering: GSM, 3G-WCDMA, LTE and the road to 5G. Hoboken, NJ: John Wiley & Sons, 2018.

Liyanage, Madhusanka, Ijaz Ahmad, Ahmed Bux Abro, Andrei Gurtov, und Mika Ylianttila, Hrsg. Comprehensive guide to 5G security. Hoboken, NJ: John Wiley & Sons, 2018.

Mathy Vanhoef und Frank Piessens. „Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2“, 2017. https://papers.mathyvanhoef.com/ccs2017.pdf.

Mayring, Philipp. Einführung in die qualitative Sozialforschung: eine Anleitung zu qualitativem Denken. 6., Überarbeitete Auflage. Pädagogik. Weinheim Basel: Beltz, 2016.

———. Einführung in die qualititative Sozialforschung: eine Anleitung zu qualitativem Denken. 5. Aufl. Beltz Studium. Weinheim Basel: Beltz, 2008.

———. Qualitative Inhaltsanalyse: Grundlagen und Techniken. 10., neu Ausgestattete Aufl., Dr. nach Typoskr. Beltz Pädagogik. Weinheim Basel: Beltz, 2008.

———. Qualitative Inhaltsanalyse: Grundlagen und Techniken. 12., Überarb. Aufl. Weinheim Basel: Beltz, 2015.

ÖBB. „WLAN im Zug“, 25. Juli 2021. https://www.oebb.at/de/reiseplanung-services/im-zug/wlan-im-zug.

Oran Sharon und Yaron Alpert. „Scheduling strategies and throughput optimization for the Uplink for IEEE 802.11ax and IEEE 802.11ac based networks“, 27. März 2018. https://arxiv.org/abs/1803.10657v1.

Osseiran, Afif, Hrsg. *5G mobile and wireless communications technology*. United Kingdom : New York: Cambridge University Press, 2016.

Penttinen, Jyrki T. J., Hrsg. *The telecommunications handbook: engineering guidelines for fixed, mobile, and satellite systems*. Chichester, West Sussex, United Kingdom: Wiley, 2015.

Prasad, Ramjee. *5G: 2020 and Beyond*. River Publisher Series in Communications. Aalborg: River Publishers, 2014.

Rachid El Hattachi, Javan Erfanian, und Brian Daly. „NGMN 5G White Paper“. Next Generation Mobile Networks, 17. Februar 2015. https://www.ngmn.org/wp-content/uploads/NGMN_5G_White_Paper_V1_0.pdf.

Rech, Jörg. *Wireless LANs: 802.11-WLAN-Technologie und praktische Umsetzung im Detail ; 802.11a/h, 802.11b, 802.11g, 802.11i, 802.11n, 802.11d, 802.11e, 802.11f, 802.11s, 802.11ac, 802.11ad*. 4., Aktualisierte und erw. Aufl. Hannover: Heise, 2012.

Roger Piqueras Jover und Vuk Marojevic. „Security and Protocol Exploit Analysis of the 5G Specifications“. Institute of Electrical and Electronics Engineers, 17. Januar 2019. https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8641117.

Sauter, Martin. *Grundkurs Mobile Kommunikationssysteme: LTE-Advanced, UMTS, HSPA, GSM, GPRS, Wireless LAN und Bluetooth*. 6., Überarb. Aufl. Wiesbaden: Springer Fachmedien Wiesbaden, 2015.

Schäfers, Tim Philipp, und Rico Walde. *WLAN Hacking: Schwachstellen aufspüren, Angriffsmethoden kennen und das eigene Funknetz vor Hackern schützen: WLAN-Grundlagen und Verschlüsselungsmethoden erklärt: der Umgang mit den beliebtesten Angriffsprogrammen: Gegenmaßnahmen in Heim- und Firmennetzwerken implementieren*. Haar bei München: Franzis Verlag GmbH, 2018.

Statista. „Number of smartphone users from 2016 to 2021“, 22. September 2021. https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/.

Trick, Ulrich. *5G: Eine Einführung in die Mobilfunknetze der 5. Generation*. 1. Aufl. Boston: DE GRUYTER OLDENBOURG, 2020.

Valdar, A. R. *Understanding telecommunications networks*. 2nd edition. IET telecommunications series 71. London, United Kingdom: The Institution of Engineering and Technology, 2017.

Wi-Fi Alliance. „Wi-Fi CERTIFIED WPA3™ Technology Overview“, Januar 2021. https://www.wi-fi.org/download.php?file=/sites/default/files/private/Wi-Fi_CERTIFIED_WPA3_Technology_Overview_202101.pdf.

———. „WPA3™ Specification“, 14. Dezember 2020. https://www.wi-fi.org/download.php?file=/sites/default/files/private/WPA3_Specification_v3.0.pdf.

Zhu, Shao Ying, Sandra, Scott-Hayward, Ludovic, Jacquin, und Richard, Hill. Guide to security in SDN and NFV. New York, NY: Springer Berlin Heidelberg, 2017.

8 Abbildungsverzeichnis

9 Tabellenverzeichnis

10 Abkürzungsverzeichnis

1G	Erste Generation des Mobilfunks
2G	Zweite Generation des Mobilfunks
3G	Dritte Generation des Mobilfunks
3GPP	Third-Generation Partnership Project
4G	Vierte Generation des Mobilfunks
5G	Fünfte Generation des Mobilfunks
5G-AKA	Authentication and Key Management
AMPS	Advanced Mobile Phone System
AN	Access Network
API	Appplication Programming Interface
APT	Advance Persistent Threats
ARPF	Authentication Credential Repository and Processing Function
ASFINAG	Autobahnen- und Schnellstraßen-Finanzierungs-Aktiengesellschaft
BS	Base Station
BSC	Base Station Controller
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSS	Basic Service Set
CN	Core Network
CP	Control Plane
CRC	Cyclic Redundancy Check
CriC	Critical Communications
CSMA/CA	Carrier sense with multiple access collision avoidance
DDos	Distributed Denial of Service
E2E	End-to-End
EAP	Extensible Authentication Protocol
EAP-AKA	Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement
EDGE	Enhanced Data Rates for GSM Evolution
eMBB	Enhanced Mobile Broadband
eV2X	Enhancement of Vehicle-to-Everything
FDMA	Frequency Division Multiplexing

FR1	Frequency Range 1
FR2	Frequency Range 2
GRPS	General Packet Radio Service
GSM	Global System for Mobile Communications
GUTI	Globally Unique Temporary Identity
IaaS	Infrastructure-as-a-Service
ICT	Information and Communication Technology
IEEE	Institute of Electrical and Electronics Engineers
IMSI	International Mobile Subscriber Identity
IoT	Internet of Things
IRTF	Internet Research Task Force
ISDN	Integrated Services Digital Network
ITU	International Telecommunication Union
MIMO	Multiple Input and Multiple Output
mMTC	Massive Machine-Type Communication
MIoT	Massive Internet of Things
mMTC	Massive Machine-Type Communication
mmWave	Millimeterwellenkommunikaton
MNO	Mobile Network Operator
MSC	Mobile Switching Centre
MU-MIMO	Multi User MIMO
MVNO	Mobile Virtual Network Operator
NaaS	Network-as-a-Service
NFV	Network Function Virtualisation
NTT	Nippon Telephone and Telegraph
ÖBB	Österreichische Bundesbahnen
OFDM	Orthogonal Frequency Division Multiplexing
OFDMA	Orthogonal Frequency Division Multiple Access
OSI	Open Systems Interconnection
PMK	Pairwise Master Key
PSK	Preshared Key
PSTN	Public Switched Telephone Network

PTK	Pairwise Transient Key
QAM	Quadrature Amplitude Modulation
RFC	Request for Comments
RTR	Rundfunk und Regulierungs-GmbH
SBA	Service Based Architecture
SDN	Software Defined Networking
SEAF	Security Anchor Function
SNIR	Signal to Noise and Interference Ratio
TACS	Total Access Communication System
TKK	Telekom-Control-Kommission
TLS	Transport Layer Security
TWT	Target Wake Time
uMTC	Ultra-reliable Machine-Type Communication
UMTS	Universal Mobile Telecommunications System
UP	User Plane
W-CDMA	Wideband-Code Division Multiple-Access
Wi-Fi	Wireless Fidelity
WLAN	Wireless Local Area Network
WPA3	Wi-Fi Protected Access 3
WRC	World Radiocommunication Conference
xMBB	Extreme Mobile Broadband

Anhang A

Interviewleitfaden

Einleitung	
Begrüßung und Vorstellung des Interviewers	
Vorstellung des Forschungsprojekts	Forschungsprojekt: 5G Mobilfunkstandard und deren Auswirkung auf österreichische WLAN-Provider Forschungsfrage: Welche Bedingungen müssen erfüllt sein, damit Nutzer*Innen österreichische WLAN-Provider gegenüber dem Mobilfunkstandard 5G vorziehen? Ziel: Akzeptanz der Nutzer*Innen bei österreichischen WLAN-Provider
Einverständniserklärung	Hinweis auf die Aufzeichnung des Interviews und auf die Anonymität der Befragung
Durchführung des Interviews anhand des Fragenkatalogs	
Abschluss	Resümee und Verabschiedung

Fragenkatalog	
Nr.	**Frage**
1	Bitte erzählen Sie mir etwas über Ihren beruflichen Werdegang, seit wann Sie im aktuellen Unternehmen tätig und was Ihre Tätigkeiten bzw. Aufgabenfelder sind.
2	Eine WLAN- und Mobilfunkinfrastruktur von den Betreibenden muss verschiedene Anforderungen erfüllen. Wie kann die Flexibilität und die Skalierbarkeit in Ihrem Unternehmen auf die Anforderungen reagieren?
3	Glauben Sie, dass die technologischen Verbesserungen der beiden Drahtlosstandards die Kosten der Infrastruktur einsparen können?

4	Die neuen Modulationsverfahren der Drahtlostechnologien ermöglichen einen höheren Datendurchsatz. Wie schätzen Sie die Modulationsverfahren ein im Hinblick auf die Effizienz?
5	Gehen Sie davon aus, dass hohe Dichten in der Umgebung samt deren Problemen, durch die technologischen Verbesserungen reduziert werden?
6	Welche Erwartungen haben Sie bei den akkubetriebenen Endgeräten der Nutzer*Innen, deren Energie effizienter genutzt wird?
7	Es existieren eine Vielzahl an unterschiedlichen Gefahren bei Wi-Fi6 und 5G. Welche Angriffsvektoren haben das größte Potential und stellen die Sicherheit der Nutzer*Innen dadurch in Gefahr?
8	Inwieweit können die Protokolle und die Verschlüsselungen bei Wi-Fi6 und 5G die Gefahren reduzieren? Glauben Sie aus Ihrer Erfahrung, dass es eine Auswirkung auf die Verwendung von WLAN-Hotspots der Nutzer*Innen hat?
9	Wie würden Sie die jeweiligen technologische Verbesserungen der jeweiligen Standards beurteilen in Bezug auf Effizienz und Sicherheit? Inwieweit werden die Nutzer*Innen dadurch profitieren?
10	Möchten Sie abschließend noch etwas zum Thema Effizienz und Sicherheit in Bezug auf WI-FI6 und 5G erzählen oder sonstige Aspekte ergänzen?

Begriff	Dimension	Indikator
Effizienz	Infrastruktur	• Flexibilität und Skalierbarkeit • Kosten
	Modulationsverfahren	• Datendurchsatz • Frequenz
	Umgebung	• Dichte
	Energie	• Akku
Sicherheit	Gefahren	• Angriffsvektoren • Protokolle & Verschlüsselungen

Transkript Expert*In 1

00:00:12 Sprecher 1
Hallo!

00:00:12 Sprecher 2
Ja, jetzt habe ich eine englische Stimme gehört die mir erklärt hat, dass jetzt dieses Gespräch aufgezeichnet und auch transkribiert wird.

00:00:21 Sprecher 1

Sehr gut, alles klar.

00:00:23 Sprecher 1

Dann würden wir starten. Bitte erzählen Sie mir etwas über Ihren beruflichen Werdegang. Seit wann Sie im aktuellen Unternehmen tätig und was ihre Tätigkeiten beziehungsweise Aufgabenfelder sind.

00:00:41 Sprecher 2

Das heißt, ich soll jetzt kurz über meinem gesamten beruflichen Lebensweg erzählen?

00:00:48 Sprecher 1

Ja, den Gesamten. Eher vielleicht teilweise IT-lastig oder Wlan-lastig.

00:00:52 Sprecher 2

Okay, das war bei mir immer IT-lastig.

00:00:54 Sprecher 2

Ich fange an. AHS, Matura.

00:00:59 Sprecher 2

Erster Job in einem Unternehmen, dass sich mit Datenkommunikation beschäftigt hat. Konkret waren das damals Standleitung Modems und Dial-Up Modems mit unglaublichen Geschwindigkeiten von 300 Bit pro Sekunde. Später dann halt, 1200 Bit pro Sekunde, 2400 Bit pro Sekunde, 9600 und am Ende waren es die berühmten, weiß ich gar nicht mehr, ich glaube nur 28 k war das Maximum über die Telefonleitung bei Dial-Up Modems.

00:01:31 Sprecher 2

Genau damals eben, dieses Unternehmen war General Distributor für die amerikanische Firma US Robotics, einer der damals weltgrößten Modemproduzenten.

00:01:43 Sprecher 2

Und mein Aufgabenbereich damals war Pre Sales, natürlich jetzt nicht nur im Bereich von Datenkommunikation über Telefonleitungen, sondern hauptsächlich auch x25. Das war statiks P, man kann sagen, dass das eine Art Vorläufer des Internets war, auch ein paketorientiertes Netzwerk, dass ausschließlich im professionellen Umfeld verwendet wurde. Später dann bei einer anderen Firma, Produktmanager für Datenkommunikations Produkte, dann Ausbildung gemacht Marketing, Export Management.

00:02:16 Sprecher 2

Nächste Stufe war dann Ericsson Mobile Phones, wo ich dann das Produkt Marketing Manager aktiv war für Mobile Data, also wiederum Datenkommunikation. Dann gab es noch Steckschnurlostelefone und am Ende auch die Mobiltelefone. Das war vor über 20 Jahren, also zu einer Zeit, als Nokia und Ericsson den Markt beherrscht haben.

00:02:37 Sprecher 2

Anschließend dann nach einem kurzen Ausflug in die Welt des Festnetzes da ging es dann darum, kleine ISDN Nebenstellenanlagen für den österreichischen Markt fit zu machen und einen indirekten Vertrieb aufzubauen.

00:02:50 Sprecher 2

Ging es dann in das erste Unternehmen, an denen ich beteiligt war. Das war ein Unternehmen, das sich auf die Herstellung und den Vertrieb von Mobiltelefonen spezialisiert hat allerdings, dann auch eben anderer Produkte gemacht hat, wie zum Beispiel MP3 Player.

00:03:07 Sprecher 2

Und auch zumindest war, dass der Plan wurde nie umgesetzt. Die allerersten WLAN Produkte. In dieser Zeit dieses Unternehmens, das war vom 2000 – 2004, musste ich sehr, sehr oft nach Fernost reisen. Konkret war ich wirklich oft in Taiwan und das war genau die Zeit, als die allerersten WLAN Produkte auf den Markt gekommen sind, also sprich da sprechen wir von 802 Punkt 11 B, wie Berta. Der allererste WLAN Standard, der ja

glaub ich, wenn ich mich richtig erinnere. Brutto heiße 11 Megabit unter theoretisch geschafft hat.

00:03:47 Sprecher 2

Ja 2005 kam dann die Selbstständigkeit mit einer neuen Firma und diese Firma gibt es jetzt schon seit 17 Jahren und, , Hauptmotivation, der für die Gründung dieser Firma war, ist die Unkultur zu beenden für Internetzugang über WLAN im Kaffeehaus Geld zu verlagern. Sprich die damaligen Anbieter haben vom Nutzer Geld verlangt für die WLAN Nutzung. Derartige Geschäftsmodelle haben natürlich nie funktioniert.

00:04:16 Sprecher 2

Meine Idee war eben das Geschäftsmodell wie gsagt umzudrehen, sprich der Benutzer bezahlt nichts, aber der Standort, an dem das Ganze installiert ist, der bezahlt für diesen Service und das funktioniert bis heute so. Unter anderem auch durch die Arbeit von Freeware sind diese Bezahl-Hotspots oder bezahlen WLAN-Hotspots, dann immer mehr zurückgedrängt worden und irgendwann einmal auf wurde das aufgegeben.

00:04:44 Sprecher 2

Also ich glaube, es gibt in Österreich, keinen einzigen mehr, aber vielleicht täusche ich mich ja, aber ich kenne zumindest keine mehr oder niemanden, der so etwas macht. Auch in den Hotels nicht.

00:04:53 Sprecher 2

Ja, und damit kann ich eben behaupten, dass ich seit mehr als 20 Jahren mich mit dem WLAN Thema beschäftigen, weil das eben bei dieser früheren Firma schon Teil der Fall war und dem dann natürlich seit der Selbständigkeit der Gründung 2005 auch. Als solches habe ich eben die ganzen Entwicklungen mitgemacht eben die E, die Evolution 800 211 B dann G, so weiter und sofort bis zu AX. Was man halt heute haben.

00:05:22 Sprecher 2

Ja, von dem her glaube ich habe ich jetzt nochmal ein kurzes, einen kurzen Überblick gegeben. Was mach ich jetzt im Unternehmen? Bei kleinen Unternehmen ist es so, dass man wie immer Mädchen für alles ist. Die ersten 7 Jahre war ich ja überhaupt One Man Show und habe alles selbst gemacht. Das heißt, das ging eben vom Vertrieb bis hin über

die Entwicklung der Produkte, Software, technisch Wartung, Montage, Installation, Buchhaltung, Büroreinigung, einfach alles.

00:05:52 Sprecher 2

Ja, und diese Vielseitigkeit hat mir immer großen Spaß gemacht und war auch ein Grund, warum ich dem Unternehmen damals kein extremes Wachstum verordnet habe, sondern, mich dafür entschieden habe es sehr langsam und dafür stetig, ah, stetiges Wachstum anzustreben und, ah, das funktioniert bis heute so, dass jetzt heißt wir wachsen nach wie vor aber sehr, sehr langsam und damit sehr gesund.

00:06:20 Sprecher 1

Danke, vielen Dank. Gut, dann würden wir gleich auf die nächste Frage stürzen ja, ahm, es geht um Punkte Flexibilität ja, also ein WLAN und ein Mobilfunkinfrastrukturbetreibender, wie sie es auch sind als WLAN Provider. Muss sich auch verschiedener Anforderungen agieren und muss auch diese erfüllen. Ja, wie können Sie oder wie kann die Flexibilität und ihre Skalierbarkeit in ihrem Unternehmen auf die Anforderungen reagieren?

00:06:52 Sprecher 2

Ahm, dadurch, dass wir ein sehr kleines Unternehmen sind, sind wir entsprechend schnell und der zweite Punkt ist dadurch, dass wir keine Produkte von der Stange verwenden, sondern Hardware auf der Linux zum Einsatz kommt. Sind wir viel schneller als alle anderen, weil wir für viele Verbesserungen, sofern das jetzt nicht neue Funkstandards sind, ahm, neue Software herstellen und die daneben Remote einspielen können bei unseren Kunden.

00:07:21 Sprecher 2

Und dadurch sicherstellen können, dass eben zum Beispiel bei Sicherheitslücken im Linux Kernel oder im WLAN Bereich rasch reagiert werden kann.

00:07:32 Sprecher 2

Ahm, wir haben natürlich jetzt nicht aufgrund unserer Kleinheit die Möglichkeit, jetzt hunderte Standorte von heute auf morgen Hardwaretechnisch zu modifizieren. Das funktioniert so natürlich nicht, trotzdem behaupte ich aber, dass wir eines der flexibelsten Unternehmen hier in Österreich was das betrifft sind.

00:07:51 Sprecher 1

Das heißt wenn das jetzt gleich mit der 5G Welt, ja der Mobilfunk, das Network function virtualisation? Das kann dadurch abgefedert werden, weil sie ja dann die Spezifikation auf den jeweiligen Kunden ablegen können oder halt jetzt auch die Erweiterungen, das kann man quasi jetzt gleichstellen.

00:08:08 Sprecher 2

Ja, ich weiß jetzt nicht, ob ich die, ob ich jetzt die die Frage da ist ganz richtig verstehe.

00:08:15 Sprecher 2

Prinzipiell ist es so, dass wir die, dass wir natürlich erstens, immer an den Kunden angepasst, unsere Installationen aufbauen, das ist keine Installation, gleicht der Anderen.

00:08:27 Sprecher 2

Und basierend auf dem, was natürlich bei uns nicht nur dokumentiert, sondern technisch auch hinterlegt ist, können wir natürlich eine derartige Installation immer sehr rasch und unkompliziert verändern.

00:08:40 Sprecher 1

Na das ist genau die, die Frage wurde richtig verstanden.

00:08:48 Sprecher 2

Ja ok, gut.

00:08:50 Sprecher 1

Dann die nächste Frage glauben Sie, dass die technologischen Verbesserungen der beiden Drahtlosstandards die Kosten der Infrastruktur einsparen können?

00:08:57 Sprecher 2

Nein, das glaube ich nicht, weil im Wesentlichen, ahm, wenn eine. Wenn ein neuer Standard kommt, der eben notwendig wird, dann bedeutet das ja letztendlich immer, dass man Hardware tauschen muss.

00:09:12 Sprecher 2

Die Hardware muss gekauft werden, die Hardware muss installiert werden und ah, von dem her ist jetzt die technologische Verbesserung. Damit kann ich auch nichts einsparen. Gerade im WLAN Bereich bedeuten ja die immer besseren Geschwindigkeiten in Wirklichkeit immer das ich.

00:09:31 Sprecher 2

Das nur dann funktioniert, wenn ich möglichst keine Hindernisse habe zwischen einem Access Point und einem Client. Sprich sobald ich jetzt Alltagssituationen habe wie eben Hotels, wo ich jetzt zum Beispiel nicht in jedem Zimmer einen Access Point verbauen möchte.

00:09:49 Sprecher 2

Werden viele Vorteile, die neue Standards bringen, marginalisiert, weil die dort einfach nicht greifen in so einer Umgebung. Alleine schon, wenn ich jetzt die Frequenzen betrachte, zum Beispiel 2,4 oder 5 ghz oder dort in Zukunft noch 6 g Hz, das ist ja alles schön, aber nicht in einem.

00:10:10 Sprecher 2

An einem Ort, wo ich eben Hindernisse habe, wo ich Mauern habe, weil ich müsste ja dann viel Dichter bauen, um ebenfalls eine flächendeckende gute Versorgung zu errichten. Im Bereich von 5 oder 6 Ghz also ich bräuchte mehr Hardware als mit nur 2,4 Ghz alleine aufgrund der geringeren Reichweite.

00:10:29 Sprecher 1

Aber das ist genau das, was auch bei 5G eigentlich ist, ja, das desto höher die Frequenz ist, desto.

00:10:34 Sprecher 2

Genau desto schlechter die Durchdringung und desto mehr Sender sind notwendig.

00:10:38 Sprecher 1

Okay.

00:10:39 Sprecher 1

Ach, sehr gut ja.

00:10:42 Sprecher 1

Ahm, gut dann die neuen Modulationsverfahren der Drahtlostechnologien ermöglichen, einen höheren Datendurchsatz. Wie schätzen Sie die Modulationsverfahren im Hinblick auf die Effizienz ein?

00:10:54 Sprecher 2

Prinzipiell, ist ganz klar, dass diese neuen Verfahren einen Vorteil bringen. Das Problem ist nur, dass WLAN heute in einer Art und Weise angewendet wird.

00:11:09 Sprecher 2

, die diese Vorteile zunichtemachen. Was meine ich damit? WLAN Geräte werden ja heute nur im fast nicht vorhandenen Fall von einem Experten in Betrieb genommen, sondern WLAN ist heute in den Modems der Netzbetreiber inkludiert und die werden halt verschickt. Auch selbst aufgestellt von den Kunden oder von WLAN technisch nicht affinen Telekom-Technikern aufgestellt. Und diese Geräte, die da aufgestellt werden. Meiner Meinung nach komplett falsch konfiguriert, die sind absolut Ressourcen verschwendend konfiguriert. Das bedeutet eben, dass zum Beispiel für einen Internetanschluss, der jetzt nicht ultimativ schnell ist.

00:12:01 Sprecher 2

Die volle Breite eines Kanals zum Beispiel verbraucht wird, anstatt dass man die Kanalbreite entsprechend schmäler macht, wo man auch immer ganz locker die Geschwindigkeit jetzt dieser Internetanschluss bietet, drüber kriegt.

00:12:12 Sprecher 2

Sind diese Geräte leider so eingestellt, dass sie eben eigentlich das Maximum an verfügbaren Funkressourcen verbrauchen. Und damit habe ich dann die Situation, wenn wir uns jetzt ein Wohnhaus vorstellen mit vielen Wohnungen, dass es dort WLAN-technisch dann eigentlich schon sehr schlecht aussieht, weil jedes Gerät das sind der Wohnung steht.

00:12:34 Sprecher 2

Eine viel höhere Breite des Kanals verbraucht, als es technisch eigentlich notwendig wäre und damit die Möglichkeit eben auszuweichen.

00:12:43 Sprecher 2

Nicht mehr vorhanden ist und damit wird das eigentlich kannibalisiert. Es nützt nichts, wenn ich immer ausgefeiltere Verfahren verwende, die für theoretisch mehr Durchsatz sorgen, wenn dann eben Geräte ausgeliefert werden, wo sich eigentlich niemand irgendwas dabei denkt.

00:12:59 Sprecher 2

Hauptsache, es funktioniert irgendwie, und an den Nachbarn der daneben sitzt, denkt niemand, und am Ende haben dann alle eine schlechtere und niedrigere WLAN Übertragungsraten, als es eigentlich notwendig wäre.

00:13:13 Sprecher 1

Wie sieht es dann beim BSS Coloring aus? Weil dieser Art Feature, der genau quasi hinhört? Wenn jetzt ein anderer Accesspoint spricht, das dann auch antwortet.

00:13:26 Sprecher 2

Wenn wir. Ich habe ja nur ein sehr begrenzte. Eine begrenzte Breite eines Kanals zur Verfügung oder eines Frequenzbandes zur Verfügung. Und wenn ich eben jetzt, wenn jetzt einer der es vollmacht oder 2 vollmachen, dann kann der Dritte mit denen reden.

00:13:48 Sprecher 2

Es wird ja deswegen nicht mehr frei, zumindest nach dem Verständnis, das ich jetzt habe. Ich lasse mich aber sehr gerne aufklären, wenn das ein, wenn die Technologie wirklich dafür sorgt, dass jetzt bei einem anderen Gerät irgendwas freigemacht wird.

00:14:01 Sprecher 1

Okay, gut dann.

00:14:06 Sprecher 1

Gehen Sie davon aus, dass hohe Dichten in der Umgebung samt deren Problemen durch die Technologie, technologische Verbesserung reduziert werden, also ist es im Prinzip vielleicht eine Frage, die auf die vorige anknüpft.

00:14:21 Sprecher 2

Ja, das überschneidet sich jetzt eben auch schon mit dem, was ich vorhin erzählt habe.

00:14:28 Sprecher 2

Prinzipiell natürlich ja, technologische Verbesserungen sind immer ein Vorteil, aber die hohen Dichten, sehe ich eben genau aus den Gründen, die ich vorhin gesagt habe sie ich sehe nicht, dass du jetzt besser werden, weil ich ganz sicher bin, dass eben dann die ersten Netzbetreiber ihre Geräte ausliefern. Mit dem aller neuesten Standard, dass sie dann genau wieder so schlecht konfiguriert sein werden wie bisher.

00:14:57

Wir sind.

00:14:58 Sprecher 1

Also eher der Fokus, dass der User, wenn der User also besser gesagt.

00:15:04 Sprecher 1

Zusammengefasst, wenn der User alles richtig konfigurieren würde, dann wären wahrscheinlich die ganzen Features und die jetzt nachkommen sicher sinnvoll. Aber dadurch, dass die User eher.

00:15:12 Sprecher 2

Ja, das macht ja keiner das macht ja keiner. Das machen nur wir Experten, aber jetzt der normale Konsument, der einfach irgendein Internet WLAN braucht, der hat ja schon überhaupt ein Problem zu unterscheiden. Das ja die Begriffe Internet und WLAN, das das da beginnt, das ja schon die Leute verstehen gar nicht den Unterschied.

00:15:28 Sprecher 1

OK.

00:15:32 Sprecher 1

Verstehe ja. Gut, dann welche Erwartungen haben Sie bei den akkubetriebenen Endgeräten oder Smartphones Laptops? Der Nutzer, ah, deren Energie effizienter genutzt werden soll oder genutzt wird.

00:15:46 Sprecher 2

Ja, das ist ja jetzt pure Physik. Gerade eben jetzt.

00:15:52 Sprecher 2

Wenn habe ich eben kleinere Funkzellen, speziell jetzt im Mobilfunkbereich brauche ich weniger Energie und zudem zu den Funkzellen durchzudringen, von dem er wird, also die wird weniger Energie verbraucht. Wenn ich da eben auch an meine berufliche Vergangenheit zurückdenke, an die ersten GSM Mobiltelefone, die ja wirklich im 900 Megahertz Band. Da schlag mich jetzt nicht.

00:16:17 Sprecher 2

Zumindest ein Band glaube ich, war es nur mit einem Watt Leistung gefahren sind, wenn also da die nächste Mobilfunk Station Kilometer entfernt war.

00:16:27 Sprecher 2

Und wir vergleichen das mit der Situation heute, dann haben wir das ja in dieser Art nicht mehr, weil eben es vielmehr Mobilfunk, Sendestationen gibt im Netz. Und damit nicht mehr so weit gefunkt werden muss, wie das eben früher der Fall war.

00:16:46 Sprecher 1

Alles klar. Gut dann dann schenk mir rüber auch zu sicherheitsrelevanten Themen, ja. Es existiere ja eine Vielzahl an unterschiedlichen Gefahren beim Wi-Fi 6 und 5G Standard. Ah, welche Angriffsvektoren haben das größte Potenzial und stellen die Sicherheit der Nutzer dadurch in Gefahr?

00:17:05 Sprecher 2

Das ist jetzt für mich eine sehr schwierige Frage, weil ich jetzt nicht als Hacker unterwegs bin und damit.

00:17:12 Sprecher 2

Wahrscheinlich von einigen konkreten Angriffsmöglichkeiten, die es gibt, dazu wenig Wissen habe. Prinzipiell, denke ich, dass es sehr wohl eine, naja Gefahr gibt und das ist einfach die, wenn wir jetzt zum Beispiel sagen, wir haben jetzt WPA 3 als aktuellen WLAN Verschlüsselungsstandard, dann ist das zwar prinzipiell natürlich super.

00:17:34 Sprecher 2

Allerdings sind in den Haushalten viele Geräte, die das nicht unterstützen, die das nicht können. Allein wenn du jetzt angebliche Smart Home Geräte zum Beispiel denken. Die eben auch mit dem WLAN verbunden werden müssen oder sollen und die das nicht beherrschen und andere Endgeräte, die ein Problem haben, wenn ein Access Point eben sowohl wie WPA 3 also WPA 2 fährt, dann haben dann checken die das dann, dann können sich diese Endgeräte überhaupt nicht mehr verbinde, was dazu führt, dass man WPA 3 wieder abschalten muss.

00:18:09 Sprecher 2

Sprich die hohe Verbreitung von WPA 2 ist, sicherlich problematisch und das wird sehr, sehr lange dauern, bis irgendwann einmal es soweit sein wird, bis eigentlich WPA 3 der allgemeine Standard sein wird, der am meisten verwendet werden wird. Und solange dass der Fall ist, habe ich natürlich ein Sicherheitsthema.

00:18:29 Sprecher 2

Wobei meine ganz persönliche Einstellung ist, wenn etwas wirklich sicher sein soll, dann ist jede Art von Funk, immer das falsche Mittel.

00:18:38 Sprecher 1

Ja, die nachfolgende Fragen implizieren sich eher auf die Frage mit Protokollen, Verschlüsselung. Das heißt aber eben auch man kann sagen im öffentlichen Bereich, so wie sie jetzt betreiben, ein offenes WLAN ohne Passwort hat, hat seine Gefahr, dass es halt noch im Funkbereich jemand das abfängt und dann quasi mitlesen kann, soweit ich das jetzt.

00:18:59 Sprecher 2

Jaein, da hat sich ja etwas ganz massiv verbessert in den letzten 15 Jahren. Wenn wir an die Anfänge zurückdenken, also Gäste WLAN sind ja nach wie vor hauptsächlich unverschlüsselt und das war vor zehn, fünfzehn Jahren ein wirkliches Thema, weil ja der

gesamte Internetverkehr damals noch unverschlüsselt abgelaufen ist. Insofern hat sich jetzt durch diese Veränderung, dass es eigentlich heute keinen unverschlüsselten Internetverkehr mehr gibt eine deutliche Verbesserung ergeben, weil es eben heute nicht mehr so einfach ist.

00:19:38 Sprecher 2

Verkehr Datenverkehr mit, also mitsniffen kann ich Ihnen natürlich schon, aber den dann auch auszuwerten, weil eben nichts mehr unverschlüsselt übertragen wird.

00:19:48 Sprecher 2

Heute ist, wenn ich hier einen entsprechenden Angriff starten möchte, ein wie wesentlich höherer Aufwand notwendig, weil ich einen Wirklichkeit Zertifikate fälschen muss, um den verschlüsselten Verkehr, abfangen und decodieren zu können, um Mitzulesen.

00:20:05 Sprecher 2

Sprich so wie früher, dass ich irgendeinen Freakkid hinsetzt und einfach irgendwelche lustigen Sachen macht, wie Bilder austauschen auf geladenen Websites und so, das ist ja heute alles nicht mehr möglich. Insofern hat sich durch einen Technologieschub, die Situation verbessert, aber das war in diesem Fall nicht im Mobilfunk oder WLAN Bereich, sondern eigentlich die Tatsache, dass heute http tot ist und auch eben Email Client nur verschlüsselt arbeiten, alles.

00:20:35 Sprecher 2

Die Ganze, die Datenverkehr selbst wird verschlüsselt und das hat für einen viel höheren Anstieg der Sicherheit gesorgt, als es jetzt tatsächliche Verschlüsselungsmechanismen selbst getan haben.

00:20:53 Sprecher 2

ja.

00:21:06 Sprecher 1

Ok. Sehr ausführlich beantwortet, sehr gut. Dann die technologischen Verbesserungen der jeweiligen Standards Drahtlos, also 5G und Wi-Fi6 in Bezug auf Effizienz und Sicherheit. Werden die Nutzer dadurch profizieren oder eher nicht.

00:21:16 Sprecher 2

Ich glaube nicht. Weil.

00:21:20 Sprecher 2

Auch hier wieder dem Konsumenten wirkliches Bewusstsein dafür fehlt, was zum Beispiel jetzt WPA2 oder WPA3 bedeutet. Das ist die eine Sache.

00:21:33 Sprecher 2

Und was eben die Effizienz betrifft.

00:21:37 Sprecher 2

Ja, haben wir auch schon vorher darüber gesprochen, dass eben die Verbesserungen super sind, wenn ich eben möglichst eine direkte Sichtverbindung habe vom Access Point zu meinem Client hin, aber sobald ihr Hindernis sind, wäre ich den Großteil von irgendwelchen Geschwindigkeitsverbesserungen oder Durchsatzverbesserungen wieder vergessen können.

00:22:01 Sprecher 2

Ja, wobei das eben unterschiedliche Anwendungsszenarien sind, wenn wir jetzt eben das Thema öffentliches WLAN betrachten, dann ist das ja ein ganz anderes Anwendungsszenario. Als wenn ich jetzt zum Beispiel in einem Büro.

00:22:13 Sprecher 2

WLAN aufspanne und da jetzt wirklich Mitarbeiter über dieses verschlüsselte WLAN mit einem File Server zum Beispiel verbunden sind, weil da ist ja wirklich dann der Bedarf nach extrem nach maximal möglicher Bandbreite über diese Funkverbindung vorhanden. Während das in einem klassischen Gäste WLAN da brauch ich ja nicht Hunderte Megabit, sondern da.

00:22:35 Sprecher 2

Ist es ausreichend, wenn der irgendeine zweistellige Zahl, an Megabit jetzt hier stabil zur Verfügung hat und das muss gar nicht einmal so hoch sein.

00:22:45 Sprecher 2

Für die üblichen Anwendungen sei es jetzt eben ein Video streamen oder im Internet surfen oder eine Video Videochat durchführen, braucht man ja bei weitem nicht so viel. Also das heißt, wenn damit 10 Megabit hat die er stabil kriegt, dann ist das bereits eine gute Sache wo er eigentlich fast alle Anwendungen, die man normalerweise in einen Gäste WLAN macht, durchführen kann.

00:23:13 Sprecher 1

Ok, sehr gut. Dann als abschließende Frage möchten Sie abschließend noch etwas zum Thema Effizienz und Sicherheit in Bezug auf Wi-Fi 6 und 5G erzählen oder sonstige Aspekte ergänzen?

00:23:23 Sprecher 2

Naja, es wäre eben sehr schön, wenn die Netzbetreiber, die eben WLAN-fähige Modems in großen Mengen ausliefern, hier die Konfiguration dieser Geräte mit wesentlich mehr Hirn durchführen würden, als sie es bisher machen, damit eben die ja doch noch immer sehr begrenzten Ressourcen Frequenz technisch gesehen jetzt.

00:23:44 Sprecher 2

Nicht so komplett sinnlos verbraten werden.

00:23:49 Sprecher 1

Alles klar. Vielen Dank.

00:23:51 Sprecher 1

Dann beenden wir das Gespräch und ich beende auch hiermit die Aufnahme.

00:23:58 Sprecher 2

Okay.

Transkript Expert*In 2

00:00:12 Sprecher 1

Hallo!

00:00:16 Sprecher 2

Ja, ich bin noch da.

00:00:18 Sprecher 1

Gut, wie ist die?

00:00:18 Sprecher 2

Ich habe nichts gehört, nein.

00:00:20 Sprecher 1

Okay.

00:00:20 Sprecher 2

Aber ich habe die Benachrichtigung bekommen, dass es aufgezeichnet wird. Natürlich bin ich damit einverstanden.

00:00:26 Sprecher 1

Sehr gut, alles klar. Dann starten wir mit der ersten Frage.

00:00:31 Sprecher 1

Bitte erzählen Sie mir etwas über den beruflichen Werdegang, seit wann Sie im aktuellen Unternehmen tätig und was Ihre Tätigkeiten beziehungsweise Aufgabenfelder sind.

00:00:40 Sprecher 2

Ich bin seit 2014 also fast 8 Jahren.

00:00:46 Sprecher 2

Bei der 1 Telekom als Netzwerktechniker angestellt und seit den letzten 6 Jahren spezialisiert auf WLAN. Sowohl für Büro, Infrastrukturen als auch im Outdoorbereich von Parkplätzen.

00:01:06 Sprecher 2

Ja, Parkplätze oder etwas Derartiges.

00:01:11 Sprecher 2

Und sonst?

00:01:12 Sprecher 1

Öffentliche Flächen also.

00:01:15 Sprecher 2

Ja für öffentliche Flächen, danke. Um es genau zu sagen für öffentliche Flächen.

00:01:16 Sprecher 2

Ansonsten im Netzwerkbereich, natürlich auch für Routing und Switching tätig. Zuständig und dementsprechend auch für Störungen und anfällige Fehler.

00:01:33 Sprecher 2

Dass diese quasi doch noch gelöst werden.

00:01:37 Sprecher 2

Ja, das wäre.

00:01:40 Sprecher 1

Alles klar dann starten wir mit der Frage 2.

00:01:45 Sprecher 1

Ein WLAN- und Mobile-Infrastrukturbetreiber muss auf verschiedene Anforderungen agieren, die er erfüllt. Wie kann die Flexibilität und die Skalierbarkeit in ihrem Unternehmen auf die Anforderungen reagieren?

00:01:59 Sprecher 2

Ja, das kommt darauf an, was das Unternehmen mehr bevorzugt.

00:02:03 Sprecher 2

Sprich sollte die Infrastruktur mehr auf WLAN bezogen sein, oder auf Mobilfunk. Also bei mir in dem Fall würde ich gerne auf das WLAN Thema eingehen wollen. Hier ist die Frage wie flexibel ist das Unternehmen bezüglich der Access Points die im WLAN-Bereich verwendet werden.

00:02:25 Sprecher 2

Gibt es die Möglichkeit mehrere aufzubauen, zu installieren oder eher weniger. Da kommt es natürlich da rauf an welche Technologien wir bei den Access Points verwenden würde. Zum Beispiel hätten wir mehr Access Points, dann würden wir halt ganz normal 5 GHz oder 2,4 GHZ Bänder ausstrahlen.

00:02:50 Sprecher 2

Sollte man jetzt weniger Access Points zur Verfügung haben, aufgrund der Fläche. Dann könnte man hier sowohl halt auch mit Wi-Fi6 ausstrahlen.

00:03:03 Sprecher 2

Ja, das war es eigentlich so. So hätte ich das jetzt gesehen.

00:03:15 Sprecher 1

Dann die nächste Frage. Glauben Sie, dass die technologischen Verbesserungen der beiden Drahtlosstandards die Kosten der Infrastruktur einsparen können?

00:03:27 Sprecher 2

Ja, also prinzipiell hätte ich das schon so gesehen.

00:03:43 Sprecher 2

Das ist halt jetzt auch wieder die Frage, wie das Unternehmen das Ganze haben möchte. Man könnte sowohl etwas einsparen, wenn jetzt zum Beispiel das Unternehmen eher auf physische Hardware verzichten möchte, also sprich auf Patchkabeln.

00:04:03 Sprecher 2

Oder andere, zum Beispiel Kupfer oder Lichtwellenleiter. Da könnte man ja wohl jetzt auch auf die WLAN Technologie zugreifen. Denn dieser kabellosen Form, das heißt dann würde man sowohl Ersparnisse in Betracht ziehen können.

00:04:22 Sprecher 2

Aber es kommt halt drauf an, wie das Unternehmen das haben möchte. Ja, wenn jetzt mehr gespart werden soll, dann wäre natürlich WLAN eine Variante.

00:04:33 Sprecher 2

Ja, so sollte ich das beantwortet haben.

00:04:36 Sprecher 1

Ich meine es gibt ja im neuen WLAN-Standard neue Features quasi. Und das heißt, allein dadurch würde ich jetzt ein Thema abdecken, das es jetzt dann auch in Zukunft besser funktioniert.

00:04:55 Sprecher 1

Versteh ich das jetzt richtig. Sollte ein WLAN Accesspoint mehrmals aufgebaut sein, bei einer Fläche wie vorhin erwähnt, dann kann es sein, dass du durch Wi-Fi6, dann weniger Bedarf ist. Oder dass dann die Abdeckung besser ist.

00:05:06 Sprecher 2

Genau, also genau dann könnte man hier sehr wohl auch einsparen, also mit Wi-Fi 6 wäre es natürlich umso besser, weil wir dadurch dann auch wieder weniger Hardware hätten, aber mehr Flächendeckung und vor allem eine gute Effizienz.

00:05:26 Sprecher 2

Ok, gut. Dann frage 4 die neue Modulationsverfahren der Drahtlostechnologien ermöglichen einen höheren Datendurchsatz, wie schätzen Sie die Modulationsverfahren Hinblick auf die Effizienz ein?

00:05:46 Sprecher 2

Zum Beispiel bei Mu-MIMO, hat man eben zum Beispiel das gleichzeitige Uploaden und downloaden.

00:05:58 Sprecher 2

Das wäre halt zum Beispiel jetzt schon eine gute Technologie, die effizient wäre oder sich durchsetzen würde.

00:06:11 Sprecher 2

Dann gibt es eben noch die Modulationsverfahren OFDMA, was natürlich auch weiterentwickelt ist, weil es eben hier zum Beispiel mehr Unterkanäle gibt.

00:06:23 Sprecher 2

Wie vorher erwähnt des Mu-MIMO Verfahren, dass dieses Modulationsverfahren dementsprechend besser ist als das bisherige OFDM.

00:06:39 Sprecher 1

Ja ok.

00:06:51 Sprecher 1

Dann die Frage 5. Wie ist es bei der Dichte? Also gehen Sie davon aus, dass die hohe Dichte in der Umgebung samt ihren Problemen durch die technologischen Verbesserungen reduziert werden?

00:07:06 Sprecher 1

Vielleicht als Beispiel, wenn jetzt hier bei mir in der Wohnung, habe ich einen Nachbarn die auch WLAN haben.

00:07:22 Sprecher 2

Genau, da wäre zum Beispiel im WLAN Bereich im das BSS Coloring eine ziemlich effiziente Technologie.

00:07:33 Sprecher 2

Warum? Weil hier ist es möglich, dass die Access Points im WLAN-Bereich auf den gleichen Kanälen sprechen können. Jedoch halt quasi mit einer Color mehr oder weniger jetzt belegt werden.

00:07:48 Sprecher 2

Das heißt quasi das jetzt, sagen wir einmal die Access Points, die Color rot tragen, auch erst dann wirklich agieren, wenn jetzt ein anderer Access Point fragen würde.

00:08:01 Sprecher 2

Das selbe ist jetzt, wenn du jetzt diverse Access Points die Color blau haben, dass die halt quasi dann auch isoliert und getrennt von den Roten sind. Das heißt hier hätte man eine tolle Möglichkeit eben diese Dichtheit auszutricksen oder auszunutzen.

00:08:21 Sprecher 2

Genau, im Vergleich zu Mobilfunk ist es so, dass der im 5 G immer mehr Zellen quasi benötigt werden eben, dass die Frequenzen auch durchhalten und nicht gestört werden. Und hier haben wir eben halt, dass wir die Dichte so abdecken, dass man je mehr Zellen man hat, desto mehr Dichte hat man dann. Das ist im Gegensatz zum Beispiel beim WLAN wie BSS coloring finde ich dann doch mehr ein Vorteil den Punkt.

00:08:56 Sprecher 1

Ja, dies impliziert wieder, dass wieder mehr Geld für die Infrastruktur ausgeben müsste eigentlich. So hätte ich es jetzt verstanden.

00:08:21 Sprecher 2

Genau. Dann können wir zum Beispiel beim WLAN einsparen wiederum.

00:09:11 Sprecher 1

Wie ist es, also welche Erwartungen haben Sie bei den akkubetriebenen Endggeräten der Nutzerinnen deren Energie dann effizienter genutzt wird.

00:09:23 Sprecher 2

Ja, da ist für mich jetzt die Erwartung in erster Linie jetzt, einmal so ganz allgemein betrachtet. Logischerweise wenn die Endgeräte einen kleineren Akku hätten, was

eventuell in der Zukunft passieren kann und natürlich dadurch aber auch mehr Kapazität haben. Dann wird das natürlich ein toller technologischer Vorteil also Fortschritt.

00:09:48 Sprecher 2

Und was ich aber auch mehr erwarte, zum Beispiel, das es quasi diesen Sleep Mode gibt. Das heißt der Client antworte doch wirklich nur dann, wenn ein Traffic herrscht. Also kann einerseits natürlich sehr viel Energie gespart werden und diese Sleepperiode, wenn es jetzt doch, die kann, dann doch sehr lange sein.

00:10:10 Sprecher 2

Das wird dann natürlich eben extrem viel Energie einsparen also mit der Traffic nur dann herrscht wenn auch wirklich etwas benötigt wird. Da ansonsten der Client im Sleep Mode behandelt und das ist dann keine große Sache mehr.

00:10:26 Sprecher 1

Und das heißt, aktuell ist es so oder, wenn ich es so verstehe, dass das Endgerät eine permanente Verbindung zum WLAN Accesspoint hat.

00:10:33 Sprecher 2

So ist es. Ja, genau.

00:10:35 Sprecher 1

Ok, ok sehr gut.

00:10:38 Sprecher 2

Gut. Es existieren eine Vielzahl an unterschiedlichen Gefahren bei Wi-Fi6 und 5G. Welche Angriffsvektoren, haben das größte Potenzial und stellen die Sicherheit der Nutzer dadurch in Gefahr.

00:10:53 Sprecher 2

Also, da ist immer dann die Frage. Was ist jetzt die Gefahr? Für wen, also für mich als Nutzer in dem Fall.

00:11:05 Sprecher 2

Wäre halt eine riesen Gefahr, wenn ich jetzt mit WLAN verbunden bin, das jetzt zum Beispiel an der Man-in-the-Middle stattfinden könnte. Sprich jemand könnte den Traffic auslesen.

00:11:17 Sprecher 2

Beim 5 G ist es jetzt nicht mehr also nicht ganz so einfach.

00:11:28 Sprecher 2

Also wie gesagt ist ein bisschen schwierig zu beantworten, aber ich.

00:11:33 Sprecher 2

Beim WLAN gibt es ja dann noch andere Möglichkeiten also.

00:11:40 Sprecher 2

Wenn jetzt zum Beispiel jemand das WLAN Passwort hatte. Das wäre ja auch zum Beispiel eine potenzielle Gefahr, dass man, wenn man die jetzt irgendwie rausfiltert. Dann hat man ja genauso Möglichkeiten, auf das Netzwerk zuzugreifen.

00:11:54 Sprecher 2

Oder auf die Nutzerdaten, die er dann quasi unterm Strich gelesen werden können.

00:12:03 Sprecher 2

Es gibt natürlich auch physische Gefahren, jetzt nicht nur bezüglich Datenschutz. Wenn jetzt jemand ein Access Point zerstört oder demoliert, dann ist die Verfügbarkeit vom WLAN nicht gegeben. Dasselbe trifft aber auch zu beim 5G. Das heißt wenn hier zum Beispiel einen Funkmasten dementsprechend mal kaputtgeht oder zerstört wird, dann haben wir hier quasi eher die physische Gefahr.

00:12:32 Sprecher 2

Und die ist natürlich auch immer da, das ist leider so. Dann ist hier die Gefahr, dass die Funktionalität zum Beispiel nicht gegeben ist. Es geht jetzt in dem Fall nicht nur um Sicherheit und Datenschutz, sondern natürlich auch um die Verfügbarkeit.

00:12:50 Sprecher 1

Weil sie vorher Smartphone erwähnt haben, weil sie sich nicht äußern konnten. 5G und Smartphone die Frage?

00:13:03 Sprecher 2

Dann wollte ich eher schon in Richtung Virus und Schadsoftware gehen. Das ist, denke ich, aber ein bisschen zu weit gehen würde jetzt.

00:13:15 Sprecher 1

Ok, per se. Würde ich es jetzt so verstehen, dass 5G Funktechnisch sicherer ist abgesehen von der Hardware wie beim WLAN.

00:13:30 Sprecher 2

Ja, genau also da geht es dann wirklich nur noch darum, was der End User macht oder falsch machen kann. Ansonsten ist 5G vom Betreiber aus sehr sicher.

00:13:40 Sprecher 1

Okay, dann kommen wir auch gleich zur nächsten Frage, die auch gleich daran gekoppelt ist.

00:13:46 Sprecher 1

Inwieweit können die Protokolle und die Verschlüsselung bei Wi-Fi6 und 5G die Gefahren reduzieren? Glauben Sie aus ihrer Erfahrung, dass es eine Auswirkung auf die Verwendung von WLAN Hotspots der Nutzerin hat?

00:13:58 Sprecher 2

Da wären zum Beispiel gute Ansätze, quasi die 802.1x Zertifizierungen, das wäre jetzt in dem Fall schon eine ziemliche sehr gute Verschlüsselungsmethode. Das ist der sichere Methode.

00:14:11 Sprecher 2

Vor allem ein guter Ansatz wäre eben auch, wie WPA3 nur das Problem ist, dass es noch nicht alle Geräte unterstützen.

00:14:20 Sprecher 2

Dann gebe es eben jetzt noch zum Beispiel ein Public WLAN. Ist dieses Enhanced Open, wo quasi ein verschlüsselter Handshake stattfindet? Das heißt, dies ist dann wirklich nur möglich mit einem Fake WLAN Access Point, den Sicherheitsmechanismus zu umgehen und das andere wäre eben, wenn das Endgerät ein Problem hat.

00:14:45 Sprecher 2

Von den Technologien hätte ich jetzt da auf 802.1x gezogen. Das es eine sehr gute Verschlüsselungsmethode wäre und auch auf jeden Fall die Gefahren reduzieren würde.

00:15:05 Sprecher 1

Ja, okay.

00:15:08 Sprecher 1

Wie würden Sie die jeweiligen technologischen Verbesserung der jeweiligen Standards beurteilen in Bezug auf Effizienz und Sicherheit? Inwieweit werden die Nutzer dadurch profitieren?

00:15:20 Sprecher 2

Zum Beispiel, wie vorher schon erwähnt BSS Coloring eine gute Entwicklung und auch natürlich für die Sicherheit effizient.

00:15:41 Sprecher 2

Natürlich werden auch die Nutzer profitieren, weil wie vorher schon erwähnt ist ein isolierter Traffic vorhanden.

00:15:56 Sprecher 2

Unabhängig von der Sicherheit, dass das auch ein Nutzer natürlich ein Gefühl von Sicherheit geben würde, ja.

00:16:12 Sprecher 2

Ansonsten fällt mir jetzt nichts ein. Kleiner Hänger.

00:16:19 Sprecher 1

Kein Problem aber das heiß jetzt, salopp gesagt, ist es so dass diese ganzen technischen Verbesserungen auch automatisch die Effizienz und die Sicherheit steigern oder gibt es da irgendwelche Bedenken? Gibt es eine Verschlechterung oder bewegen wir uns in die Richtung des Guten oder?

00:16:41 Sprecher 2

Also wir bewegen uns da definitiv hin in die Richtung, des Guten. Weil es ist ja auch so, dass die ganzen technologisch. Jetzt habe ich den Faden wieder langsam. Dass die technologischen Verbesserungen sich eigentlich von Tag zu Tag auch weiterentwickeln.

00:16:59 Sprecher 2

Also jetzt ist es dann so, das sollte man wirklich als Sicherheitsproblem stattfinden, also aufgefundenen, dass das dann nicht dementsprechend schnell möglichst ausgebessert wird, also verbessert wird mit Updates oder etwas Derartigen. Also von dem her sind wir da generell auf einen sehr guten Weg, weil die Menschheit will in puncto Technik immer mehr Effizienz und Sicherheit, und das passiert auch ehrlich gesagt von Tag zu Tag, ohne dass man es vielleicht weiß.

00:17:30 Sprecher 2

Aus meiner Sicht eben sind die Standard schon sehr weit entwickelt und das wird sich in Zukunft zum Guten natürlich noch weiterentwickeln, bzw. besser weiterentwickeln.

00:17:40 Sprecher 1

Gut, dann sind wir eigentlich schon fast am Ende angelangt. Möchten sie abschließend noch etwas zum Thema Effizienz und Sicherheit in Bezug auf wieviel ist Wi-Fi6 und 5G oder sonstige Aspekte ergänzen?

00:17:54 Sprecher 2

Ja, in Puncto WLAN bin ich nach wie vor der Meinung, dass es einer der sichersten Technologien ist und auch vor allem effizient.

00:18:08 Sprecher 2

Allein unter dem Strich würde ich aber auch sagen, dass der Nutzer selbst verantwortlich ist. Was jetzt genau er will. Möchte er mehr diese komfortable Zone behalten und sagen ich will jetzt nicht mit meinem WLAN verbinden, denn ich habe ja sowieso 5G. Oder ist

jemand ein Gewohnheitstier mehr oder weniger. Und sagt Ich möchte mich mit WLAN verbinden oder im WLAN immer verbunden sein, weil es ja kostenlose Service ist er genutzt werden kann und genutzt wird.

00:18:38 Sprecher 2

Und auch das ist natürlich eine Gewohnheit, also da ist es dann.

00:18:42 Sprecher 2

Meiner Meinung nach so, dass jeder Nutzer selbst dafür verantwortlich ist, was er mehr bevorzugt. Bezüglich Effizienz oder Sicherheit 5G zum Beispiel ist es sehr schnell, aber auch WLAN kann sehr schnell sein.

00:18:59 Sprecher 2

Je nachdem, wie man es gerne hätte, ja also. Eine eher offene Antwort aber ob sie abzuschließen, würde ich sagen das ist, also wer welche Effizienz und Sicherheit haben möchte, das kommt auf jeden selbst an.

00:19:18 Sprecher 2

Also, in Dem Fall Nutzerbezogen.

00:19:23 Sprecher 1

WLAN hat keine Gefahr gegenüber 5G.

00:19:29 Sprecher 2

Das hätte ich jetzt nicht so gesehen.

00:19:32 Sprecher 1

Ok, alles klar, okay.

00:19:34 Sprecher 1

Gut, dann vielen Dank für das Interview. Hiermit beende ich auch die Aufzeichnung.

00:19:38 Sprecher 2

Ich danke.

Transkript Expert*In 3

00:00:10 Sprecher 1

So ich glaube jetzt befinden wir uns in der Aufnahme.

00:00:14 Sprecher 2

Ja, sehe ich.

00:00:14 Sprecher 1

Ja, Bestätigung.

00:00:18 Sprecher 1

Sehr gut, dann beginnen wir gleich mit der ersten Frage. Bitte erzählen sie mir etwas über Ihren beruflichen Werdegang, seit wann Sie im aktuellen Unternehmen tätig und was ihre Tätigkeit beziehungsweise Aufgabenfeld sind.

00:00:29 Sprecher 2

Ja, sehr gerne. Also mein beruflicher Werdegang hat im ISP Umfeld vor 10 Jahren begonnen, hauptsächlich im Bereich Fixed Network und bin momentan bei einem Netzwerk Hersteller bei Arista Networks tätig und bin dort als System Enginner tätig. Und da sind meine Aufgaben Felder, auch unter anderem, die Presales und Postsales Agenten ich Bereich Wirelessnetworking als Teil unseres Campus Networking Portfolios zu betreuen.

00:01:09 Sprecher 1

Sehr gut dann die Frage 2. Eine WLAN- und Mobilfunkinfrastruktur von den Betreibern muss verschiedenen Anforderungen erfüllen. Wie kann die Flexibilität und die Skalierbarkeit in Unternehmen auf die Anforderungen reagieren?

00:01:26 Sprecher 2

Also grundsätzlich Infrastrukturseitig ist es meiner Meinung nach so,

00:01:33 Sprecher 2

Das es eine natürlich breite Auswahl. Ja, ob ich jetzt Controller gestützte oder Controller lose Infrastruktur im Bereich Wireless Networking haben möchte. Ja die Controller Less Lösungen skalieren natürlich einer Meinung nach definitiv höher.

00:01:55 Sprecher 2

Das heißt, da kann ich mal grundsätzlich sehr, sehr hoch skalieren beziehungsweise bei der Flexibilität aufgrund vor allem bei Wi-Fi 6E sehe ich da natürlich mit dem neuen 6 Ghz Spektrum auch eine höhere Flexibilität und Skalierbarkeit, weil ich weiter ausleuchten kann.

00:02:16 Sprecher 2

Weil ich ein schöneres, unbenutztes Band zur Verfügung habe. U nd natürlich auch im Mobilfunk durch die Virtualisierungsmöglichkeiten SDN und NFV. Kann ich dort auch natürlich sehr, sehr hoch skalieren, indem meine Anwendungen halt am Edge laufen und und je nach Use Case dann quasi auch näher.

00:02:40 Sprecher 2

Ja, an den Anwender kommen. Und dadurch, dass ich halt eben diese unified Computesystem habe, die am Edge laufen, kann ich dort natürlich auch nach Bedarf sei es jetzt Nutzeranzahl, sei es jetzt die Auslastung dementsprechend skalieren. Das kann man natürlich sehr gut als Unternehmen nutzen.

00:03:00 Sprecher 2

Und wie gesagt im Wireless Networking sehe ich es einfach man hat eine eine Vielzahl von Herstellern in verschiedenen Access Points.

00:03:08 Sprecher 2

Sei es Indoor oder Outdoor.

00:03:11 Sprecher 2

Verschiedene Architekturen und da kann man einfach sehr gut leben. Zum Beispiel mit Controller losen Architekturen, wie die wir im Einsatz haben, sehr hoch skalieren und dadurch bin ich natürlich sehr, sehr flexibel.

00:03:27 Sprecher 1

Gut. Glauben Sie, dass die technologischen Verbesserung der beiden Drahtlosstandards, die Kosten der Infrastruktur einsparen können?

00:03:40 Sprecher 2

Definitiv, und das hat verschiedene Gründe. Das sind natürlich einerseits einmal dadurch, dass ich sozusagen höhere bessere Modulationen habe. Kann ich natürlich.

00:03:51 Sprecher 2

Oder andere Modulationen verwende, so kann ich da natürlich dann dementsprechend höhere Abdeckung erzielen.

00:04:01 Sprecher 2

Dadurch kann ich natürlich, Definitiv auch Stromkosten senken. Sei das jetzt auf auf der Betreiberseite, sei das jetzt natürlich dann auf der Endnutzer Seite oder man selbst als Unternehmen. Aber weil man natürlich dann auch im gerade Mobilfunk unter anderem.

00:04:23 Sprecher 2

Dadurch virtualisierungs Funktionen zum Beispiel einfach verschiedene Applikationen, verschiedene Use Cases auf derselben Infrastruktur abbilden kann. Auch die Kombination von beiden Technologie, diese Hotspot Lösungen mit Radio SEC. Ergeben dann natürlich dann Synergien, die man im Endeffekt ganz klar Einsparungen bringen werden.

00:04:53 Sprecher 2

Und einfach durch eben diese bessere Abdeckung, durch einen zum Beispiel mit Wi-Fi 6E wieder dieses 6GHz Spektrum, das momentan halt eben frei ist.

00:05:04 Sprecher 2

Das heißt, da habe ich keine Doppelbelastung mit irgendwelchen Wetter, Radar etc. Kann ich das dann einfach optimaler nutzen und dadurch einfach dann im Endeffekt die Kosten einsparen kann. An verschiedenen Punkten in der Infrastruktur weniger Access Point zum Beispiel, wenn ich besser ausleuchten kann, was natürlich wieder zu geringeren Stromkosten führen.

00:05:32 Sprecher 2

Bis dahin, dass ich mehr User servicieren kann. Zum Beispiel, das ich eben verschiedene Use Cases darauf abbilden kann.

00:05:42 Sprecher 2

Dadurch glaube ich einfach, dass die die technologischen Verbesserungen sei es in der Modulation in verschiedenen, sage wir Optimierungen, da einfach dazu führen.

00:05:55 Sprecher 1

Also wie gesagt, heutzutage ist es ja auch von den Regulation notwendig, das ja alles ECO freundlich wird. Und ich glaube hiermit ist die Frage auch sehr gut beantwortet.

00:06:08 Sprecher 1

Gut, glauben Sie, dass die Technik. Was haben wir hier gehabt. Die neuen Modulationsverfahren der Drahtlostechnologien ermöglichen ja einen höheren Datendurchsatz. Wie schätzen Sie die Modulationsverfahren in einem im Hinblick auf die Effizienz ein?

00:06:26 Sprecher 2

Da möchte ich mit Wi-Fi zum Beispiel beginnen. Ja, also einfach da am Einsatz bei 802.11ax mit OFDMA ergibt einfach eine eine Vielzahl an Unterkanälen, die ich verwenden kann. Das sind 256 im 20 MHz Bereich.

00:06:47 Sprecher 2

Und dadurch kommt es zu einer Durchsatzsteigerung einfach zwischen 10 und 20%.

00:06:53 Sprecher 2

Und das liegt einfach daran, dass ich Ressourceunits habe. Die Unterkanäle werden halt in diese RUS eingeteilt und dadurch, dass ich jetzt nicht mehr so mal seriell nacheinander übertragen muss, sondern einfach ich unterschiedliche Zeitfenster verwenden kann. Ja und dadurch ein paralleles Senden ermögliche.

00:07:18 Sprecher 2

Habe ich, dazu habe ich da natürlich rein aufgrund der der Modulation einen höheren Nutzungsgrad.

00:07:36 Sprecher 2

Ja, dadurch finde ich dass, es sehr sehr viel effizienter ist wie noch bei AC. Und da kommen natürlich dann auch noch ndere Faktoren hinzu. Wo ich einfach ein Multi-User MIMO, Downlink und Uplink machen kann.

00:07:54 Sprecher 2

Wo ich dann eben bis zu 8 mal 8 MIMO eben realisieren kann. Ja, dass ich einfach längere OFDM simples habe, was mir natürlich dann den Overhead reduziert und natürlich auch eben BSS-Coloring.

00:08:12 Sprecher 2

Das dann noch mit mit rein spielt. Ja, ich habe auch noch eine Target Wake Time, die da noch dazukommt und und all diese sagen wir einmal Verfahren.

00:08:26 Sprecher 2

Inklusive eben dieser Modulationsverfahren.

00:08:30 Sprecher 2

Wirkt ein, bringt einfach eine höhere Effizienz. Ja und dasselbe natürlich auch im im Mobilfunk, wenn ich dort jetzt zum Beispiel an die 256 QAM Modulation denke. Die mir einfach eine viel schönere natürlich Auslastung oder Effizienz im Spektralbereich bringt.

00:08:56 Sprecher 2

Habe ich dann in beiden Welten sozusagen Modulationen, die dann dadurch eben die Effizienz steigern und damit auch die Bandbreiten im Endeffekt erhöhen.

00:09:09 Sprecher 1

Okay, war sehr ausfürhlich beantwortet.

00:09:13 Sprecher 1

Dann eine Problematik ist ja auch zum Beispiel, dass ja in hohen Dichten. Oder gehen sie jetzt von davon aus, dass die hohe Dichte in der Umgebung samt deren Problemen durch die technologische Verbesserung reduziert warden? Weil es gibt ja immer wieder das

Problem, dass so wie jetzt in Wohnungen oder so. Bei hohen Dichten Übertragungsprobleme auftauchen.

00:09:38 Sprecher 2

Ja. Also grundsätzlich, wenn ich jetzt anfangen mit dem mit 5G eben durch die bereits erwähnte 256 QAM-Modulation. Habe ich einfach eine bessere spektrale Effizienz- Ja, das heißt ich kann die Frequenzbereiche, die Spektralbereichen effizienter und besser nutzen.

00:10:04 Sprecher 2

Was natürlich nur dann sozusagen funktioniert, wenn ich auch dementsprechend ein Störrfreies Übertragen ermögliche. Das heißt wenn da jetzt sehr viele Stör.

00:10:21 Sprecher 2

Oder sagen wir Objekte oder generell, wenn die Übertragung gestört wird, durch verschiedene Faktoren muss ich natürlich dann auf eine niedrigere QAM runterfallen. Ja, das heißt, wenn ich da jetzt zum Beispiel auch Zellen durchaus sozusagen kleiner gestalte.

00:10:42 Sprecher 2

Dann kann ich da dann natürlich eben mit 256 QAM das Meiste rausholen. Also das heißt, kleine Zellen mit 256 QAM, da bekomme ich dann einfach sozusagen, dass das Meiste raus für was ich investiert habe.

00:11:03 Sprecher 2

Das wird natürlich das Problem auch etwas erleichtern.

00:11:09 Sprecher 2

Ja, im im WLAN-Umfeld mit Wi-Fi6 eben dadurch, dass ich eben zum Beispiel BSS coloring verwenden kann oder verwende. Habe ich da einfach eine Möglichkeit diese Kanal den Wiederverwendungsfaktor wenn ich das so nennen kann, um circa einen Faktor von 8 erhöhen kann. Das bringt natürlich dann sicherlich eine große Abhilfe.

00:11:39 Sprecher 2

Dadurch, dass ich jetzt Multi-MIMO im Uplink und Downlink verwenden kann, und eben diese durch die längeren OFDM Symbols ein weniger Overhead habe.

00:11:53 Sprecher 2

Kann ich dann insgesamt dieses Problem besser handhaben. Da sind diese hohen Dichten weniger problematisch warden. Ja das bedingt natürlich dann auch gerade eben im Residentialumfeld, das heißt ich nenne es im Privat, im Heimsektor. Das dort natürlich auch seitens der Provider das dann halt auch genutzt wird. Ja und dass man halt dort auch sozusagen dieses Spektrum und auch die die Kanäle besser nutzt.

00:12:25 Sprecher 1

Okay, das heißt, sie gehen jetzt davon aus, dass das sicherlich von den bisherigen Revolutionen abghängig ist.

00:12:34 Sprecher 2

Ja, genau genau.

00:12:37 Sprecher 1

Gut, wie sehen Sie dann bei den Endgeräten. Also welche Erwartungen haben Sie bei den akkubetriebenen Endgeräten der Nutzerinnen oder Nutzer deren Energie effizienter genutzt wird?

00:12:52 Sprecher 2

Also fangen wir an mit Wi-Fi6. also mit dem WLAN- Teil.

00:12:59 Sprecher 2

Zum Beispiel durch die Target Wake Time, das ist ja quasi ein Enhancment zum Stromsparen. Ja, das heißt, dass sind definitiv Mechanismen, die mal definitiv helfen werden.

00:13:17 Sprecher 2

Ich gehe auch davon aus, dass wenn ich jetzt zum Beispiel Wi-Fi 6E im 6 GHz Bereich mich bewege. Und da keine so bekannten Störsignale habe, dass ich da natürlich dann noch schöner sozusagen ausleuchten kann, dadurch besseres das Signal Level auch dem Endkunden zur Verfügung stellen kann. Dadurch einfach auch weniger Strom brauche.

00:13:48 Sprecher 2

Wenn ich Ich zum Beispiel weniger roumen muss, hat das natürlich einen Impact.

00:13:54 Sprecher 2

5G Bereich gibt es natürlich definitiv, das sehe ich auch ein Einsparungen ja, das liegt einerseits natürlich an der Modulation.

00:14:04 Sprecher 2

Das heißt, wenn ich jetzt das Spektrum effizienter nutzen kann. Kann ich dadurch einfach, wenn ich eben zum Beispiel auch meine Zellen umgestaltet und die kleiner machen, habe ich einfach einen besseren Noise Performance was auch natürlich wieder die den Akku länger halten lässt.

00:14:20 Sprecher 2

Ja,für den Kunden natürlich auch die Peak to Average Power Ratio. Er hat sich von 5G zu 4G noch einmal wieder deutlich verbessert, weil die einfach sehr sozusagen peaky geworden ist.

00:14:38 Sprecher 2

Das heißt, ich habe immer höhere Spitzen bei der Avarage Power Ratio.

00:14:42 Sprecher 2

Und das führt natürlich dann das zum Beispiel auch die Amplifier in den Endgeräten eben ein kürzeres Batterieleben hervorrufen.

00:14:50 Sprecher 2

Dadurch, dass man einfach da wieder versucht hat, diese diese Peaks zu glätten. Das ist mit 5G soweit einmal gelungen wird das natürlich dann auch wieder eine positive Auswirkung haben auf die Akkulaufzeit der Endgeräte. Also ich sehe in den beiden Welten da definitiv positive Trends.

00:15:19 Sprecher 2

Und ich ich denke natürlich auch im Sinne der Green-IT, die natürlich jetzt immer mehr zum Thema wird. Das da halt positive Bewegungen gibt der auch auch im Bereich der Endgeräte.

00:15:36 Sprecher 1

Ok, gut. Dann es gibt ja auch verschiedene Angriffsvektoren ja, bei Wi-Fi6 6 und 5G. Welche Angriffsvektoren haben das größte Potenzial und stellen die Sicherheit der Nutzerin oder Nutzer, der dadurch in Gefahr, wo sehen Sie das größte Potential dieser Angriffe?

00:16:00 Sprecher 2

Also grundsätzlich, gibt es natürlich immer wieder die Gefahr zum Beispiel, der Man-in-the-Middle Attacks. Natürlich gerade auch durch, ich nenne es jetzt einfach mal offene Hotspots.

00:16:21 Sprecher 2

Also sprich verschiedene, gerade in der Gastronomie gibt es an verschiedenen Örtlichkeiten eben sozusagen diese Hotspots. Teilweise sind die dann auch ohne ohne Preshared Key, das heißt wirklich komplett offen. Da sehe ich zum Beispiel im Wi-Fi6 definitiv eine Verbesserung.

00:16:39 Sprecher 2

Eben mit dem Enhanced Open Verfahren für Hotspots, das dann trotzdem verschlüsselt wird.

00:16:44 Sprecher 2

Natürlich gibt es da noch verschiedene Gefahren, das jetzt irgendwer Rogue Access Points zum Beispiel da mit einbringt und ähnlichen. Das sehe ich nach wie vor noch als Issue, aber natürlich auch die die Einführung von WPA3. Sofern das es halt die Endgeräte supporten, bringt er natürlich eine größere Sicherheit.

00:17:12 Sprecher 2

Gerade auch das jetzt dann zum Beispiel die Preshared Key Authentifizierung so nicht mehr existent ist, sondern eben mit SAE abgelöst wird. Seh ich dann da halt auch wieder eine Verbesserung. Ja und im 5G sind natürlich auch einige Sicherheitsaspekte mit diesen Secure Anchor Funktionen eingeführt worden. Ja so, dass zum Beispiel auch im im Roamingfall im Gast Netzwerk eben da auch mehr Wert auf Security gelegt wird.

00:17:49 Sprecher 2

Muss man das eben mit der Homebase sozusagen, abgleicht und und eben dann noch authentifiziert. Also es gibt nach wie vor denke ich, eine große Gefahrenlastoder oder großes Gefahrenpotential.

00:18:09 Sprecher 2

Gerade auch bei bei 5G natürlich dadurch, dass man noch für verschiedene Use Cases wie das autonome Fahren gerade im Bereich SDN, NFV verschiedene Computeressource halt am Edge hat. Und die sehr verteilt sind, ist das sicherlich auch ein neuer Vektor aufgrund von den neuen Use Cases.

00:18:31 Sprecher 2

Auf den wir da ein Auge werfen muss. Aber grundsätzlich, denke ich dass sagen wir mal so Szenarien wie Access Points Man-in-the-Middle Angriffe nach wie vor halt stattfinden könne. Weil einfach WPA3 zum Beispiel auch noch nicht so in der breite supported ist. Und dann natürlich oftmals ein Fallback zu WPA2 stattfindet.

00:19:03 Sprecher 2

Nach wie vor etwas, was man oftmals unterschätzt, ist dann natürlich die Gefahr direkt physisch das heißt zum Beispiel im Access Netz. Das man halt auch eben da die die Access Points Authentifizier und dass da nicht jeder sozusagen sondern Access Point irgendwo in Betrieb nehmen kann. Und dasselbe gilt natürlich für 5G. Ja, dass man da einerseits natürlich die Mobilfunkanbieter das sowieso die physische Sicherheit gewährleisten, dass da jetzt nicht jemand kommt und sich dann dort sozusagen connected und dann dort mitlesen kann ja.

00:19:39 Sprecher 2

Aber so generell, dass schätze ich sind die Gefahren, die sich natürlich verkleinert haben und teilweise neue Vektoren, die da jetzt aufkommen.

00:19:50 Sprecher 1

Vielleicht dann gleich als Übergang, wie sie schon erwähnt haben Protokolle.

00:19:56 Sprecher 1

Wie weit können die Protokolle und die Verschlüsselung bei Wi-Fi6 und 5G reduzieren? Glauben Sie aus ihrer Erfahrung, dass es seine Auswirkung auf die Verwendung von

WLAN Hotspot hat der Nutzer oder der Nutzer innen, also wie vorher schon erwähnt haben. Gibt es es da irgendwas?

00:20:14 Sprecher 2

Ja, also grundsätzlich, wie schon vorher erwähnt in der vorigen Frage beantwortet. Ja es gibt dort schon eben die Protokolle und Verschlüsselungen jetzt zum Beispiel bei der Wi-Fi6 eben wie schon erwähnt den Enhanced Open oder SAE.Schrägstrich WPA3 die natürlich da Gefahren reduzieren können.

00:20:39 Sprecher 2

Ob das jetzt eine eine Auswirkung auf die Verwendung von WLAN Hotspot hat, glaube ich persönlich nicht. Da aber die meisten User, glaube ich da eher wenig darauf achten aus meiner Erfahrung. B die Services sind sowieso Free ja, darum glaube ich, dass das jetzt nicht wirklich eine eine Auswirkung hat, da sag ich mal eher der Bedarf der User wird nach wie vor dann eher in WLAN hotspots VPN Verbindungen aufbauen, wie zuvor auch. Aber ich denke grundsätzlich das eben Protokolle wie WPA3, Enhanced Open, SAE, etc. dieese einige Gefahren sozusagen reduzieren können.

00:21:26 Sprecher 1

Gut. Wie würden sie dann die jeweiligen technologischen Verbesserung der Standards beurteilen in Bezug auf Effizienz und Sicherheit, inwieweit werden dann auch die Nutzer dadurch profitieren?

00:21:39 Sprecher 2

Also grundsätzlich. Ich sag einmal so, zu Verbesserungen gibt es in beiden Standards ganz klar eben auch im Bereich Effizienz und Sicherheit. Einerseits natürlich zum Beispiel bei Wi-Fi 6E, das der Einführung von 6 Gigahertz Spektrum.

00:21:58 Sprecher 2

Das ist definitiv sozusagen wirklich etwas Neues. Ja, weil man da eben Zugriff auf ein Spektrum haben, das sozusagen noch ungenutzt ist, also nichts von irgendwelchen anderen Dingen sei es jetzt Wetter Radar oder irgendwelche anderen Applikationen oder noch physischer Natur darein stören. Das heißt ich habe da mal ein cleanes Spektrum, das ich verwenden kann.

00:22:27 Sprecher 2

Das ist natürlich einerseits für den Nutzer ein Vorteil, weil dadurch kann ich einfach bessere Signalstärke darstellen. Dafür. Da hab ich weniger Störungen was natürlich dann eben auch zu einer längeren Lebedauer des Akkus zum Beispiel im Endgerät.

00:22:49 Sprecher 2

So zeigen sich bezieht.

00:22:53 Sprecher 2

Ich hab natürlich auch BSS-Coloring, was insofern natürlich auch eine gute Sache ist, weil ich einfach meine Kanalnutzung sozusagen durch diese BSS Color, um um circa das das Achtfache erhöhen kann. Das wird wirkt sich dann natürlich auch.

00:23:13 Sprecher 2

Insofern aus, dass ich da halt einfach mein meine Kanäle reusen kann und nicht einfach limitiert bin. Und dann eben, wenn ich die zu nahe nehmen, aber sozusagen verwendete, sich dann da irgendwelche Störungen haben und somit eine eine eine sozusagen verminderte Performance.

00:23:34 Sprecher 2

Ja und natürlich das selbe zum Beispiel mit der mit der 256 QAM-Modulation in der 5G Technologie. In Bezug natürlich auf Sicherheit, ja, es ist natürlich in beiden Varianten vor allem in 5G mindestens mit SDN Funktionen ergeben sich natürlich neue Sicherheitsherausforderungen.

00:23:58 Sprecher 2

Aber dennoch wurde die Architektur generell schon auf mehr Sicherheit ausgelegt. Was natürlich auch immer ein Vorteil ist ja, da hat man ja natürlich auch besonders Augenmerk beim sozusagen erstellen des der Standards. Das ist natürlich auch bei Wi-Fi6 und die Nutzungen dann immer dadurch profitieren im Endeffekt längere Akku Laufzeiten.

00:24:24 Sprecher 2

Ich habe einfach höhere Datenraten, stabilere Signale. Ich kann mehr Nutzer gleichzeitig servicieren usw.

00:24:38 Sprecher 1

Gut. Möchten Sie dennoch abschließend zum Thema Effizienz und Sicherheit im Bezug auf Wi-Fi6 oder 5G sonstige Aspekte ergänzen?

00:24:50 Sprecher 2

Also ich denke, dasss beide Technologien ihr Dasein haben. Ja, ich persönlich sehe Wi-Fi6 eher in den Indoor Applikationen ja, weil der typischerweise der Mobilfunk Nachteile hat. Also in Gebäuden, in Wohnungen. Sehe aber 5G zum Beispiel eher in den Outdoor sei es jetzt wirklich große Campus oder große Manufacturing Anlagen, das autonome Fahren oder ähnliche Use Cases.

00:25:20 Sprecher 2

Da ist, das heißt sowohl bei Wi-Fi 6 oder erweiterte IoT Capabilities als auch 5G hat da Use Cases. Und ich denk, dass das weder das eine noch das andere irgendwie besser ist, sondern beide Ihre Use Cases haben und und wir natürlich doch Synergien nutzen sollten.

00:25:41 Sprecher 2

Eben mit diversen Hotspot Lösungen, dass man halt noch die Services, die man vielleicht aus dem 5G Netz hat, als Enterprise oder auch im Wi-Fi verwenden kann. Sozusagen beide Technologien ergänzend nutzen sollte.

00:25:59 Sprecher 1

Vielen Dank, dann alles klar. Dann bedanke ich mich für das Interview und hiermit beende ich auch dann die die Aufnahme.

00:26:08 Sprecher 2

Danke auch.

Transkript Expert*In 4

00:00:08 Sprecher 1

So, hallo.

00:00:10 Sprecher 2

Ja Hallo.

00:00:12 Sprecher 1

Ja, alles klar. Dann starten wir mit der Aufnahme und auch gleich mit der ersten Frage. Bitte erzählen sie mir etwas über ihren beruflichen Werdegang, seit wann sie im aktuellen Unternehmen tätig und ihre Tätigkeiten beziehungsweise Aufgaben fehlen.

00:00:29 Sprecher 2

Ok also ich bin aktuell in 2 Unternehmen tätig. Bei der Firma Freewave seit 8 Jahren als technischer Leiter.

00:00:39 Sprecher 2

Und bei der Firma Artichoke Computing was meine eigene Firma ist, da bin ich Geschäftsführer und CTO, also quasi auch technischer Geschäftsführer.

00:00:51 Sprecher 2

Noch Details zu den Positionen oder?

00:00:56 Sprecher 1

Ja, bitte nur kurz erwähnen, was Sie zum Beispiel bei Freewave machen und was Sie ungefähr machen.

00:01:03 Sprecher 2

Also bei Freewave machen wir WLAN Hotspot für Gastronomie und Hotellerie zum Beispiel. Das heißt die Kunden wenn, WLAN angeboten, also wenn ein Kunde WLAN anbieten will seinen Gästen. Bieten wir ein Komplettpaket und der Kunde zahlt quasi einfach dafür, dass das funktioniert.

00:01:29 Sprecher 2

Somit haben wir immer wieder WLAN, Installationen an verschiedenen Standardgrößen, also von einem einzelnen Router bis hinzu größeren Installationen mit 40 Access Points.

00:01:43 Sprecher 2

Ist alles dabei und immer verschiedene Gegebenheiten auch haben. Bei der Firma Artichoke Computing Wir haben das Unternehmen gegründet, eigentlich als Serverbereich und sind dann durch die Pandemie dazu gekommen. Das wir Covid-Test jetzt angeboten haben. Wir haben da ein Konzept erarbeitet, wo wir in Container nein kleines Labor drinnen haben.

00:02:10 Sprecher 2

Quasi dezentral, wo es benötigt wird, diese Container aufstellen können. Wo natürlich dann jeweils an diesen Standorten auch immer eine Internet Infrastruktur notwendig ist, was im den meisten Fällen über LTE beziehungsweise 5G funktioniert.

00:02:28 Sprecher 2

An unseren fixen Standorten ist es natürlich auch, geht natürlich auch darum, dass wir eine WLAN Versorgung im größeren Stil brauchen, also auch ganz normal mit Access Point über eine fixe Internetleitung. Also es ist eigentlich von allem etwas dabei, ja.

00:02:51 Sprecher 1

Gut. WLAN und mobile Infrastruktur von den Betreibern muss verschiedene Anforderungen erfüllen. Wie kann die Flexibilität und die Skalierbarkeit in ihrem Unternehmen auf die Anforderungen reagieren?

00:03:06 Sprecher 2

Ja, also natürlich, man muss generell einmal schauen was, was die Anforderungen sind ist ist das eben zum Beispiel in meinem Unternehmen ist das ein mobiler Standort oder ist das ein fixer Standort. Je nachdem muss man dann natürlich die passende Technologie auswählen.

00:03:27 Sprecher 2

Wobei zum Beispiel bei unseren mobilen Standorten wir eigentlich sehr gute Erfahrungen auch mit dem 5G Netz haben. Natürlich muss man auch beachten, dass es dementsprechend skaliert.

00:03:41 Sprecher 2

Je nach Anforderung eben sollten, sollte jetzt zum Beispiel ein 5G Netz an einem Standort nicht verfügbar sein, muss man sich nach Alternativen umschauen. Weil wenn es zum Beispiel Latenz sensitiv ist die Anforderung. Was bei uns jetzt nicht der Fall ist, aber dann müsste man natürlich wenn was bei 5G sehr gut geht.

00:04:04 Sprecher 2

Aber z um Beispiel bei älteren Technologien bei LTE deutlich schlechter ist. Also da muss man einfach dementsprechend vor planen und auch schauen, wenn eine Skalierung notwendig ist, dass die jeweilige gewählte Technologie, das du nachwievor erfüllen kann.

00:04:23 Sprecher 2

Reicht das oder noch etwas?

00:04:25 Sprecher 1

Ja, das reicht. Ich schätze einmal.

00:04:26 Sprecher 2

Ich denke dass es so in meiner Firma halt ist. Ja, also je nachdem was die Anforderung ist. Müssen wir da einfach sein, müssen wir flexible sein und nutzen alle Technologien, die zur Verfügung stehen also.

00:04:45 Sprecher 1

Dazu geöhrt vermlutich Routing, Switchin, LWL-Anbindungen, je nachdem was aktuell möglich ist und wo der besten Kostennutzen wahrscheinlich ist.

00:04:57 Sprecher 2

Genau richtig, also genau. Natürlich wenn wenn an unserem fixen Standort haben wir eine eine- Anbindung. Was natürlich da einer 5G Anbindung vorzuziehen ist, wenn es diese Möglichkeit gibt, ja.

00:05:14 Sprecher 2

An anderen Standorten arbeiten wir eben mit mobilen Technologien, was aber sich wirklich jetzt über die Zeit auch herausgestellt hat, dass das je nach Netzauslastung auch

sehr gut funktionieren kann. Aber natürlich muss man schauen, wie Ausfallskritisch usw., diie jeweiligen Standorte sind. Dann muss man natürlich auch mit mit Backuplösungen sich das anschauen oder eben 5G oder ebend das Mobile nur als Backup verwenden und so weiter.

00:05:45 Sprecher 2

Also das ist ist wirklich sehr unterschiedlich und sehr Standort spezifisch.

00:05:52 Sprecher 1

Sehr gut, dann gleich als Übergangsfrag. Glauben Sie, dass die technologischen Verbesserungen der beiden Drahtlosstandards die Kosten der Infrastruktur einsparen können?

00:06:04 Sprecher 2

Ja also, ich denke mal. Je höher die WLAN Technologien die neuen, je höher die Abdeckung durch die neuen WLAN Standards ist, desto mehr kann man natürlich auch an Energiekosten einsparen.

00:06:24 Sprecher 2

Kommt natürlich auch wiederum immer auf die Anwendungsbereiche an, also es gibt Anwendungsbereiche, wo jetzt zum Beispiel eben auch bei Freewave.

00:06:35 Sprecher 2

In den meisten Fällen kein zu hoher Durchsatz notwendig, sondern da geht es eher die Reichweite notwendig ist. Somit können in so einem Anwendungsfall öffentliche Hotspot zum Beispiel eben. Kann man eher schauen, dass man Geräte mit höherer Reichweite verbaut.

00:06:54 Sprecher 2

Weil die Performance hier eher zu vernachlässigen ist, wenn es nur im Internet surfen geht.

00:07:02 Sprecher 2

Natürlich werden wir, wenn es jetzt stark in Richtung Performance geht, dann müsste man wirklich dann sich Dinge anschauen, wie massive MIMO.Wenn man wirklich hohe Performance braucht. Zum Beispiel mit NfV kann man, natürlich auch Ressourcen sparen gewisse Parts virtualisieren kann und hat natürlich auch eine sehr hohe Skalierbarkeit

00:07:32 Sprecher 2

Also das muss man halt immer schauen, ob das was Sinn macht. Bei den bei den jeweiligen Anforderungen.

00:07:41 Sprecher 1

Ja ok.

00:07:44 Sprecher 1

Ich mein, die Drahtlostechnologien haben ja auch neue Modulationsverfahren. Und die neuen Modulationsverfahren der Drahtlostechnologien ermöglichen eine höheren Datendurchsatz. Wie schätzen Sie die Modulationsverfahren ein im Hinblick auf die Effizienz?

00:08:05 Sprecher 2

Im Hinblick auf die Effizienz ja, also ich denke zum Beispiel das mit OFDM. Dass siich jetzt das Update quasi OFDMA, dass ich ein guter Schritt nach vorne gemacht wurde. Dadurch, dass bei OFDM ja immer das Signal quasi nacheinander übertragen musst werden musste beim belegten Kanal.

00:08:31 Sprecher 2

Hat sich das mit OFDMA verbessert mit den Subcarriers.

00:08:37 Sprecher 2

Und somit ist es möglich eben, dass die Daten gleichzeitig zu übertragen.

00:08:44 Sprecher 2

Und somit deutlich höhere Effizienz zu haben. Und natürlich, was auch der Vorteil ist, ist, dass es aber OFDMA einfach resistenter gegen Störungen ist also.

00:08:58 Sprecher 2

Ich denke, dass das eigentlich ein großer Punkt ist, in dem bei diesem neuen Verfahren.

00:09:12 Sprecher 1

Haben Sie irgendwas bei 5G bedenken oder, was ist da Hinblick auf Effizienz Steigerung?

00:09:22 Sprecher 2

Bei 5G. Ja, grundsätzlich natürlich bei 5G ist es im Vergleich zum Vorgänger auch eine deutliche Steigerung, also hat den neuen Modulationsverfahren über 5 G eingesetzt warden natürlich einen Vorteil.

00:09:39 Sprecher 2

Die Frage wiederum in welchem Bereich also das wird halt nur Sinn machen jetzt für den End Nutzer, wenn er wirklich sehr nahe dem Sender ist, dass er wirklich diese Vorteile von 5G im Vergleich zum Vorgänger ausnutzen kann. Je weiter also, das ist dann eher in Städten und usw. interessant. Im ländlichen Bereich ist das wahrscheinlich meiner Einschätzung nach jetzt kein so großer Vorteil.

00:10:09 Sprecher 2

Weil das meistens die sehen das sicher nicht so nah bei einander wie im städtischen Bereich, aber im Gesamten gesehen natürlich ist 5G auch ein guter Schritt nach vorne ja.

00:10:27 Sprecher 1

Ein guter Übergang. Gehen Sie davon aus, dass hohe Dichten in der Umgebung samt deren Probleme durch die technologischen Verbesserung reduziert werden, weil sie ja gerade eben angesprochen haben Städte und das ländliche Gebiet.

00:10:46 Sprecher 2

Ja hohe dichten in der Umgebung.

00:10:52 Sprecher 2

Generell ist es so, dass ich dort zum Beispiel mit dem BSS coloring, die Datenkollision verhindert wird.

00:11:09 Sprecher 2

Moment kurz.

00:11:11 Sprecher 2

Da leutet jemand, ganz kurz. OK.

00:11:24 Sprecher 2

Ja, also da, da fällt mir dazu ein. Neben das BSS Coloring, was die Datenkollision verhindert und somit die Kommunikation wirklich nur zwischen den beteiligten Geräten stattfindet.

00:11:45 Sprecher 2

Somit ,also das das seh ich da also als gute guter Schritt nach vorne und gute Verbesserung.

00:11:55 Sprecher 2

Und ja, der Mehrwert dadurch ist auf jeden Fall auch die höhere Zellendichte, die ausgenutzt werden kann. Würde mir jetzt dazu einfallen.

00:12:10 Sprecher 1

Okay und wie sehen es beim 5 G bzw. Der Dichte?

00:12:22 Sprecher 2

Ja, bei bei 5G. Naja, da ist natürlich von Haus aus eine höhere Dichte notwendig, wie bereits gesagt also.

00:12:32 Sprecher 2

Aber oder wie ist das jetzt gemeint in Bezug auf 5G?

00:12:38 Sprecher 1

Ja, also ob die, ob die hohe Dichte quasi sind und ob da mehr oder weniger Masten installiert werden müssen, damit ich die Dichte da abfangen kann.

00:12:51 Sprecher 2

Ja, natürlich eben alles was ich ja eh vorher quasi schon gesagt habe. Eben bei 5G ist es halt wirklich der Fall, dass deine höhere Dichte einfach notwendig ist. Um dieselbe Versorgung bieten zu können wie mit dem Vorgänger.

00:13:10 Sprecher 2

Und deswegen seh ich das eher im städtischen Bereich als wirklich interessant, dass man im ländlichen Bereich wird nur sicher nie die vollen Bandbreiten überall zusammen bekommen.

00:13:24 Sprecher 2

Ja, und deswegen denke ich muss da sicher auf lange Sicht geschaut werden, was eben oder ob mit anderen Frequenzen arbeitet.

00:13:37 Sprecher 2

Oder ja, also was ist dafür für Möglichkeiten gibt. Natürlich genau im Allgemeinen, aber im Mobilfunkbereich ist es sehr relevante die Frequenzen natürlich.

00:13:50 Sprecher 2

In genauso wie im WLANbereich oder im Mobilfunkbereich natürlich auf große Sicht einfach drauf geschaut werden muss, dass die Versorgungsgebiete dadurch mich dann irgendwie sich verschlechtern wenn mit anderen Frequenzen gesendet wird.

00:14:08 Sprecher 1

Sehr gut. Welche Erwartungen haben Sie dann bei Akku betriebenen Geräten der Nutzer, deren Energie effizienter genutzt wird?

00:14:20 Sprecher 2

Also ich denke mal, dass die bei den neuen Standards auch bei Wi-Fi6 jetzt sicher ein guter Punkt ist. Die Target wake Time.

00:14:32 Sprecher 2

Was sicher für Mobilgeräte sehr positiv sein kann, wenn eben der der Client nur dann antwortet, wenn es notwendig ist und somit einfach unnötiger Datenverkehr vermieden

werden kann, was dann sicher zu höheren Akku, Laufzeiten von den mobilen Geräten führt.

00:14:58 Sprecher 1

Okey. Gut, dann springen wir zur nächsten Frage. Es existieren eine Vielzahl unterschiedlichen Gefahren bei Wi-Fi6 und 5G. Welche Angriffsvektoren haben das größte Potenzial laut ihnen und stellen die Sicherheit der Nutzerin oder Nutzer dadurch in Gefahr?

00:15:16 Sprecher 2

Grundsätzlich ist natürlich einmal speziell jetzt was WLAN angeht, sehr wichtig, dass die Konfiguration der Infrastruktur mal von Haus aus passt.

00:15:28 Sprecher 2

Da könnte schon von Anfang an ein großer Fehler gemacht werden und natürlich, wenn zum Beispiel auch die falsche Verschlüsselung gewählt wird, irgendeine Verschlüsselung, die leichter gehackt werden kann.

00:15:41 Sprecher 2

Ist leider doch immer wieder der Fall, was man sieht das scheinbar wenn es irgendwie nicht beachtet wird, solche grundsätzlichen Dinge, bei der Erstkonfiguration.

00:15:51 Sprecher 2

Natürlich, dann gibt es, was per WLAN immer wieder natürlich auch sein kann eine Man-in-the-Middle Attack. Wäre ein möglicher Angriff

00:16:02 Sprecher 2

Rouge Access Points sind auch immer wieder im Sicherheitsbereich zu nennen. Natürlich per WLAN, ne und dann gibt es natürlich noch die ganz klassischen, zum Beispiel DDos-Attacke ist möglich.

00:16:18 Sprecher 2

Natürlich werden wir jetzt physischen Zugriff hat, ist es sowieso in den meisten Bereichen möglich, da irgendwelche Hackerangriffe zu machen, also physischer die Zugriff ist immer der letzte Punkt. Was ist eigentlich am einfachsten machen in die Richtung.

00:16:36 Sprecher 2

Ja also bei 5G würde ich sagen ist es im Vergleich zum WLAN sag ich sehr ähnliche Angriffsvektoren.

00:16:45 Sprecher 2

Würde ich sehr ähnlich sehen eigentlich, ja.

00:16:58 Sprecher 1

Okay, sehen Sie noch irgendwelche Gefahren? 5G, weil sie sagten ähnlich?

00:17:06 Sprecher 2

Ja, natürlich, ich meine, dass das größte Potential ist, natürlich wie gesagt physischer Zugriff auf dem einen Seite. Was jetzt bei 5G jetzt eher schwierig ist, aber natürlich das Endgerät beziehungsweise der Benutzer ist natürlich dann immer das Größte eigentlich auch eines der größten Potentiale speziell im Mobilfunkbereich.

00:17:31 Sprecher 2

Sicherheitsupdates nicht am richtigen Stand sind, wenn der Benutzer irgendwie leichtgläubig auf irgendwelche Links klickt oder sowas. A lso das ist glaub ich heutzutage immer, dass das größte Potential Potential, dass da irgendein Virus eingeschleust werden kann oder Gegenangriff gestartet werden kann ja.

00:17:54 Sprecher 1

Okay, sehr gut, ja.

00:17:59 Sprecher 1

Genau, inwieweit können die Protokolle und die Verschlüsselung bei und 5G Gefahren reduzieren. Glauben Sie aus Ihrer Erfahrung, das es eine Auswirkung auf die Verwendung von WLAN Hotspot der Nutzer hat?

00:18:15 Sprecher 2

Grundsätzlich sind die, ist der Schritt zur Wi-Fi6 6 jetzt zum Beispiel natürlich eine Verbesserung, weil damit ja quasi auch WPA 3 gekommen ist.

00:18:27 Sprecher 2

Mit dem SAE Protokoll, was im Vergleich zum Preshared-Key was vorher üblich war eine sichere Authentifizierungsmethode ist.

00:18:39 Sprecher 2

Was Unternehmen angeht, die sollten natürlich generell immer auf 802.1x setzen.

00:18:48 Sprecher 2

Natürlich für ein Unternehmen, die Authentifizierung mit einem Zertifikat eigentlich immer die sicherste Lösung ist, wenn es, um wenn es um heikle Daten geht, im Unternehmen.

00:19:01 Sprecher 2

Bei WLAN Hotspots oder offenen WLANs eben.

00:19:06 Sprecher 2

Ist sicher ein guter Schritt nach vorne, des ein Enhanced Open.

00:19:12 Sprecher 2

Mit dem 4 Wege-Handshake der verschlüsselt ist und somit sollte eigentlich eine Man-in-the-Middle Attack auf jeden Fall erschwert werden.

00:19:27 Sprecher 2

Trotzdem bleibt eigentlich genau gleich zu verwenden, also der Enduser bekommt davon eigentlich nichts mit und das ist ganz normal, weiterhin ohne Kennwort zu verwenden.

00:19:41 Sprecher 2

Bei 5G würde ich das jetzt so sehen? Eben mit dem AKA-Protokoll, ist eben ein sicheres Roaming zwischen den Sendern gewährleistet und eben das sehe ich jetzt in diesem Bereich eigentlich bei 5G den größten Schritt nach vorne, was die Sicherheit angeht.

00:20:09 Sprecher 1

Okay. Wie würden Sie die jeweiligen technologischen Verbesserung der Standards beurteilen in Bezug auf Effizienz und Sicherheit? Inwieweit werden die Nutzerinnen und Nutzer dadurch profitieren?

00:20:25 Sprecher 2

Die Nutzer, ja alsogibt eigentlich bei beiden Technologien in beiden Bereichen also sowohl Effizienz als auch Sicherheit Vorteile im Vergleich zu den Vorgängern.

00:20:41 Sprecher 2

Grundsätzlich sollten eben Nutzer bei beiden Technologien sowohl im Sicherheitstechnisch als auch von der Effizienz von Datendurchsatz usw. profitieren können.

00:20:57 Sprecher 2

Die Modulationsverfahren sind verbessert worden, die Verschlüsselungen eben zum Beispiel mit WPA3.

00:21:05 Sprecher 2

Somit denke ich, ist dass der richtige Schritt nach vorne und ja, es sollten eigentlich alle davon profitieren können.

00:21:15 Sprecher 1

Okay. Das heißt, sie würden jetzt speziell keine Themen hervorheben, keine technologische Verbesserung, weil de facto, alles ein Mehrwert für den Kunden oder Nutzer eigentlich bringt, so hätte ich es entnommen.

00:21:30 Sprecher 2

Richtig, also eigentlich ist es in allen Bereichen ein Schritt nach vorn, also da muss man jetzt nicht speziell irgendwas sagen, sondern es ist wirklich eine Weiterentwicklung. Sowohl Effizienz, Datendurchsatz, Sicherheit. Ja somit profitiert eigentlich jeder in allen Bereichen.

00:21:51 Sprecher 1

Sehr gut. Ja, dann kommen wir zur letzten Frage. Möchten Sie abschließend noch etwas zum Thema Effizienz und Sicherheit in Bezug auf Wi-Fi6 und 5G erzählen oder sonstige Aspekte ergänzen?

00:22:05 Sprecher 2

Na also, ich würd sagen, grundsätzlich haben beide Technologien ihre Daseinsberechtigung. 5G natürlich eher im Außenbereich eher eben im mobilen Beriech.

00:22:18 Sprecher 2

WLAN wird nach wie vor immer im Indoor Bereich. Meiner Meinung nach eine Rolle spielen, speziell zum Beispiel auch in Bereichen, wo Mobilfunk nicht so gut versorgt ist.

00:22:34 Sprecher 2

Ist es trotzdem ,sind die Leute trotzdem immer noch angewiesen, auf ein gut funktionierendes WLAN.

00:22:42 Sprecher 2

Im Endeffekt liegt es eigentlich bei den genau, also bei den Herstellern liegt, dass die Technologie noch wirklich schnellstmöglich zugänglich gemacht werden für die Nutzer war, Gott sei Dank jetzt langsam kommen ist.

00:23:01 Sprecher 2

Und ja, ich denke dann sobald das wirklich groß ausgerollt wird, ich was ja am Laufenden ich aber sobald das wirklich verfügbar ist, kann auch jeder davon profitieren.

00:23:17 Sprecher 2

Im WLAN Bereich ist es natürlich im Vergleich zu 5G sehr interessant für Veranstaltungen im Wi-Fi6 für Indoor.

00:23:28 Sprecher 2

Ich denk beide Technologien gehen Hand in Hand und werden zukünftig auch das es wird nichts, das andere ablösen oder sonstwas sondern ich denke, dass beide nötig sind für die jeweiligen Einsatzgebiete.

00:23:49 Sprecher 1

Wunderbar dann beende ich hier mit dir Aufnahme.

00:23:54 Sprecher 1

Und vielen Dank für das Gespräch.

00:23:56 Sprecher 2

Ja gerne.

Transkript Expert*In 5

00:00:09 Sprecher 1

Ja, Hallo. Sind sie da?

00:00:1 Sprecher 2

Ja, bin ich.

00:00:12 Sprecher 1

Sehr gut, dann starten wir mit der Aufnahme wie besprochen und auch gleich mit der ersten Frage.

00:00:19 Sprecher 1

Bitte erzählen sie mir etwas über Ihren beruflichen Werdegang, seit wann sie im aktuellen Unternehmen tätig und was Ihre Tätigkeit beziehungsweise Aufgabenfelder sind.

00:00:29 Sprecher 2

Also mein beruflicher Werdegang hat begonnen, bei einer kleinen IT Firma mit hauptsächlich PC und Drucker Fokus. Bin dann aber relativ rasch zu A1 gewechselt in den Netzwerkbereich, also für Business Kunden.

00:00:42 Sprecher 2

Ich bin jetzt seit 9 Jahren tätig und habe kleinere und größere Business Kunden mit wie Fokus auf Netzwerkanbindung, das heißt Internet und MPLS, beziehungsweise mit verschiedenen Technologien wie 5G und WLAN.

00:00:59 Sprecher 2

Dann Software defined alles Mögliche. MPLS also als du durch die Bank. Dort habe ich viele unterschiedliche Kunden, kleine bis groß mit allen möglichen Technologien.

00:01:11 Sprecher 1

Alles klar? Dann da die Frage lautet, eine WLAN- und Mobilfunkinfrastruktur von den Betreibenden muss verschiedene Anforderungen erfüllen. Wie kann die Flexibilität und die Skalierbarkeit in ihrem Unternehmen auf die Anforderungen reagieren?

00:01:28 Sprecher 2

Also beginnen wir mit 5G. 5G, also allgemeine Mobilfunkinfrastruktur ist ein sehr hochautomatisierter Bereich, also gerade Mobilfunk Provider müssen fast alle 5 Jahre ihre Infrastruktur komplett erneuern. Das heißt, es wird sehr auf Automatisierung gesetzt.

00:01:48 Sprecher 2

Das heißt, es wird viele über automatisierte Technologien im Softwarebereich, also SDN Software Defined Network verwendet.

00:01:58 Sprecher 2

Das heißt soll ich kurz beschreiben, was SDN ist oder reicht das als Haupt?

00:02:05 Sprecher 1

Das reicht definitiv.

00:02:07 Sprecher 2

Okay.

00:02:08 Sprecher 2

Also gerade 5G ist ja der Fokus auf neue Technologie, die Automatik durch autonomes Fahren, etc. Das heißt, da muss man neue Technologien einführen, wie Network Slicing. Das heißt, man hat quasi für mehrere Anwendungen virtuell abgetrennte Infrastrukturen.

00:02:29 Sprecher 2

Die nichts miteinander zu tun hat, aber die Infrastruktur per se ist dieselbe. Also das heißt, man baut auf der Autobahn jetzt nicht 2 Masten nebeneinander, sondern betreibt einen Größeren und tut den virtuell über SDN Methoden, das Netzwerk trennen. Das nennt sich Network Slicing.

00:02:44 Sprecher 2

Das heißt man hat die Autofahrt, also für das mobile Fahren, hat man einen, wie soll ich es sagen, einen allgemeinen Dienst oder Kunden, wie man es sehen will. Und daneben wird die ganz normale Telefonie für den normalen User verwendet.

00:03:01 Sprecher 1

Wie ist das im WLAN-Bereich?

00:03:04 Sprecher 2

WLAN-Bereich ist das eher weniger der Fall, da WLAN ja eher für kleine, also für Betriebe ist klein Mittel groß ist jetzt egal, aber das sind eher.

00:03:15 Sprecher 2

Eher wie sozusagen hoch customisiert. Das heißt, jeder Kunde hat seinen eigenen großen Anwendungen oder kleinere. Das heißt, da kann man weniger mit Automatisierung machen, sondern dann muss der jeweilige Techniker eher auf die Kundenwünsche eingehen.

00:03:29 Sprecher 2

Und auf die Anforderungen des Kunden, weil es gibt Firmen, die wollen eher nur ein Gäste Zugang dafür haben oder wie die ganze Company mit jedem User, die in der Company ist. Quasi, die Netzverbindung über das WLAN machen, da kann man mit Automatisierung eher weniger machen.

00:03:48 Sprecher 2

Weil die Anforderung so unterschiedlich sein können, dass man als Provider eher flexibel sein muss als beim Mobilfunk, weil man sein Mobilfunk Provider die Vorgaben macht, da kann man die Automatisierung viel besser nutzen. Der größte Unterschied eigentlich.

00:04:07 Sprecher 1

Okay.

00:04:09 Sprecher 1

Weil sie erwähnt, haben die Anbindungen, bzw. gibt es da hier auch einen Unterschied also Kupfer oder LWL-Anbindung ist?

00:04:15 Sprecher 2

Also grundsätzlich bezogen jetzt auf Österreich sind.

00:04:20 Sprecher 2

Gerad bei Firmen, in größere Firmen kann. Ist gibt es also hauptsächlich beide Varianten noch sehr viel.

00:04:30 Sprecher 2

Das heißt, da kann man oft oftmals muss man dann 5G Netze verwenden für den Kunden, wo die Bandbreite für die Firma nicht da sind. Das heißt, über 5G Router, etc. Auf der Autobahn oder auf wie soll man sagen auf offenen Plätzen für den Home User Bereich sind das alles Providerstrecken das sind alle LWL-Anbindungen zu den Funknetzen, das heißt.

00:04:57 Sprecher 2

Da ist also bei 5G an sich, Ist die Infrastruktur ziemlich fix.

00:05:03 Sprecher 2

Das heißt, man kann die, dass die Bevölkerung gut versorgen über den Funk und LWL mit hohen Bandbreiten. Beim WLAN kommt es eben darauf an, wie die Anbindung ist vor Ort.

00:05:14 Sprecher 2

Ob das, wenn das Kupfer ist, muss man vielleicht dahinter sogar eine Kombi mit WLAN und 5G verwenden, um die Bandbreiten hinzubringen.

00:05:25 Sprecher 2

Ansonsten wenn LWL Anbindung bei eher bei den urbanen Gebieten, wo große Firmen ansässig sind. Wo es LWL gibt, kann man das WLAN gut über die LWL-Anbindungen versorgen.

00:05:37 Sprecher 1

Alles klar.

00:05:39 Sprecher 1

Dann glauben Sie, dass die technologischen Verbesserungen der beiden Drahtlosstandards die Kosten der Infrastruktur einsparen können?

00:05:47 Sprecher 2

Muss man unterscheiden bei 5G ist das der Fall.

00:05:51 Sprecher 2

Die Anforderungen also, die mehr und mehr anderen dazukommen. Das heißt, man muss mehr Infrastruktur eigentlich einplanen, weil man ja die Bandbreite erhöht. Das heißt, je mehr Bandbreite sowie Frequenzbandnetz für mehr Bandbreite. Das heißt, man braucht mehr Gerätschaften, also Funkzellen nennt man das. Das nun wird mit neuer Technologie die es bei bei 5G, also MIMO das mehrere Zellen mit den User der Endgeräte interagieren.

00:06:23 Sprecher 2

Das heißt, da werden die Kosten eher steigen bei der Infrastruktur, hingegen bei der WLAN-Infrastruktur, das sind die Modernisierungen.

00:06:34 Sprecher 2

Ziehen in die Standardnetzwerk Geräte ein. Das heißt zum Beispiel, es gibt Switches mit integriertem WLAN Access Points. Das heißtt da kann man sich also Hardware sparen als Kunde, weil man quasi einen Switch verwenden kann, der einen AP eingebaut hat. Das heißt man muss nicht extra beide Geräte kaufen, sondern hat einen, der beides kann.

00:06:51 Sprecher 2

Das heißt, so spart man sich schon etwas.

00:06:55 Sprecher 2

Effektiver ist für WLAN Standard, auch hingegen beim Mobilfunk 5G ist es auch so, dass da ist man abhängig von der Technologie.

00:07:09 Sprecher 2

Weil Moderne, nehmen wir die Modems her. Bisher die Modems, viel früher als bei 4G war das Modem integriert. Dieser 4G Chip war in dem Standard, Handy SOC, der den Prozessor beinhalte drinnen. Bei 5G ist es ein extra Chip.

00:07:22 Sprecher 2

Das heißt der Energieverbrauch ist höher.

00:07:26 Sprecher 2

Somit ist die Infrastruktur, alle zusammen braucht eigentlich mehr Energie im 5G Standard im Moment.

00:07:33 Sprecher 2

Wie die Zukunft aussieht, dass es sich verbessern, ob es dazu führt, dass es wirklich eine Kosteneinsparung wird, das kann man eigentlich nicht sagen. Beziehungsweise das können nur die großen Hersteller sein. Bei WLAN sehe ich es aber sehr wohl, dass es Kosten sparen wird.

00:07:57 Sprecher 1

Sehr gut, gut dann die neuen Modulationsverfahren der Drahtlostechnologien ermöglichen ja einen höheren Datendurchsatz. Wie schätzen Sie persönlich dann die Modulationsverfahren im Hinblick auf die Effizienz sein?

00:08:11 Sprecher 2

Okay also.

00:08:15 Sprecher 2

Grundsätzlich bei wie gesagt bei WLAN, diese Green-IT ist jetzt in Mode. Das funktioniert gut, also mit den neuen Technologien im Sinne von der Modulation, höhere Datendurchsatz, das hilft schon, dass man weniger Access Point verbauen muss. Und sonstiges.

00:08:34 Sprecher 2

Das heißt.

00:08:36 Sprecher 2

Sie funktionieren erheblich besser funktioniert so, dass quasi durch MIMO-Verfahren, also mehrere Antennen, kleine Antennen können mit mehreren Endgeräten reden, beziehungsweise mit einem Endgerät mehrmals auf verschiedenen Frequenzen. Das heißt die Effizienz Steuerung ist erheblich besser.

00:08:56 Sprecher 2

Und, so was muss man noch dazu sagen?

00:09:05 Sprecher 2

Okay deswegen.

00:09:14 Sprecher 2

Moment muss es noch kurz durchdenken.

00:09:22 Sprecher 1

Ja, oder 5G Bereiche vielleicht? Das ich helfe.

00:09:27 Sprecher 2

Im 5G Bereich ist es eigentlich ähnlich.

00:09:33 Sprecher 2

Da werden ja auch, die Funkzellen sind quasi dieselbe Struktur, wie WLAN Access Point, nur halt in Klein und Groß. Also bei WLAN Access Points hat man halt Antennen. Und in dem 5G Bereich.

00:09:47 Sprecher 2

Haben Sie diese in den Zellen, die halt ein hundert Faches davon sind. Aber das Funktionsprinzip ist eigentlich dasselbe, auch wenn die Modulationsverfahren ein bisschen anders sind, sie sie grundsätzlich ähnlich aufgebaut.

00:10:00 Sprecher 2

Und Sorgen dafür, dass der Datendurchsatz erheblich höher ist. Weiters ist die Bandbreite erhöht worden im Vergleich zu 4G. Das heißt die Frequenzenbreite ist höher, das heißt

die User können viel größeren Frequenzbereich verwenden und dadurch steigen die Datenraten halt enorm. Beziehungsweise nicht nur die Datenrate, sondern auch die Latenz, mit denen das Endgerät mit der Zelle reden kann.

00:10:27 Sprecher 2

Was gerade fürs autonome Fahren erheblich wichtig ist, dass die Reaktionszeit von einem Auto mit dem Sensor der im sagt, dass ein Unfall vorhin passiert. Eben relativ kurz sind.

00:10:39 Sprecher 2

Für die Zukunft sind diese diese aktuellen Technologien 5G und Wi-Fi6 auf jeden Fall vom Stand der Dinge, was notwendig ist, wobei es natürlich noch verbessert werden kann.

00:10:55 Sprecher 2

Aber eigentlich schon ausreichend sind für die neuen Technologien, die jetzt im Kommen sind.

00:11:01 Sprecher 1

Alles klar?

00:11:03 Sprecher 1

Dann am besten gleich jetzt als Übergang. Gehen Sie davon aus, dass die hohen Dichte in der Umgebung samt deren Problemen durch die technologische Verbesserung reduziert werden?

00:11:14 Sprecher 2

Also grundsätzlich.

00:11:19 Sprecher 2

Wenn man es auf die Technologie trifft, ja. Natürlich das Problem, dass seine Hauswand des Funksignal abbricht, ist bei 5G und mit 4G exakt dasselbe. Wird eben aber durch die höhere Bandbreite aufgehoben, beziehungsweise durch mehrere Zellen und mehrere Verbindungen zwischen Endgerät.

00:11:38 Sprecher 2

Und Zelle wird das natürlich aufgehoben oder verringert das Problem.

00:11:46 Sprecher 2

Beziehungsweise durch unterschiedlichen Bandbreiten und die Möglichkeit, dass unterschiedlichen Bandbreiten verwendet werden können.

00:11:52 Sprecher 2

Vom End User also quasi während der Verbindung wird dieses Problem verringert. Man bekommt nämlich durch diese MIMO Technologie mehrere Zeitschlitze auch, das heißt diese ganzen Probleme, die man eben durch so durch Bäume Mauern, was auch immer in der Infrastruktur hat, können damit gut reduziert werden. Das gilt fürs 5G genauso wie im WLAN.

00:12:19 Sprecher 2

Ja, das kann man dazu sagen.

00:12:24 Sprecher 1

Wie sehen Sie das bezüglich der Frequenzen also wenn es niedrigere oder höhere Frequenz ist. Haben sie da irgendwelche Bedenken?

00:12:31 Sprecher 2

Bedenken im Sinne von?

00:12:35 Sprecher 1

Von der Übertragung, ob es da zu irgendwie Probleme führt oder kann?

00:12:39 Sprecher 2

Also natürlich ist, hat sich zu den nicht in den niedrigeren Frequenzen, also Langwellige sind natürlich für die für die Umgebung also Landbevölkerung natürlich das Wichtige. Wenn irgendwelche Bäume Autos.

00:12:55 Sprecher 2

Weiß ich nicht, der Gebäude in der Umgebung sind natürlich dafür besser, weil hierdurch höhere Durchdringung haben und in Innenräumen werden natürlich die Kurzwelligen,

weil die Bandbreite hat, also wenn man jetzt im Office ist, braucht man natürlich viel höhere Bandbreite. Also will man natürlich, wo mehrere User mehr Bandbreite hat zur Verfügung haben.

00:13:14 Sprecher 2

Und dann noch.

00:13:15 Sprecher 2

Die, eher höheren Frequenzbänder verwendet. Deswegen gibt es auch unterschiedliche Frequenzbänder, die alle schon lizenziert sind. Also und noch freigegeben, lizensiert werden sie schon lange. Aber wirklich schon freigegeben sind und auch schon aufgebaut werden.

00:13:31 Sprecher 1

Okay, sehr gut dann bezüglich dem Nutzer.

00:13:34 Sprecher 1

Ja, also welche Erwartungen oder welche Erwartungen haben sie bei den akkubetriebenen Endgeräten der Nutzerinnen und deren Energie effizienter genutzt wird?

00:13:45 Sprecher 2

Also bei WLAN gibt es neue Features, und Ding und Möglichkeiten, das quasi der Chip nicht immer aktiv ist beziehungsweise, wenn einer Information oder Daten transferiert werden, eher quasi mehr oder weniger aufgeweckt werden. Target und Wake Mode.

00:14:02 Sprecher 2

Beim 5G ist es eher ein Problem dadurch, dass die Modemchips in 5G, also höher mehr Bandbreite, mehr Frequenzen haben. Müssen sie und auch können, wenn man das Ziel die höhere Bandbreite, indem man mehrere Frequenzen verwendet, dass dadurch also der Stromverbrauch erhöht wird.

00:14:28 Sprecher 2

Das beziehungsweise werden wir schon erwähnt SOCIS ist mit dem neuen Modem noch nicht integriert, also die Technologie im beim Herstellerbereich ist auch noch nicht so weit, wie wir es im Moment bei den älteren Technologien sind.

00:14:38 Sprecher 2

Und also im 5G Bereich ist der Energiebedarf definitiv höher und wird wahrscheinlich auch höher bleiben. Aufgrund der physikalischen Grenzen. Das wenn ich mehr Bandbreite verwende beziehungsweise auch Wechsel, weil das man kann teilweise in einer niedrigen Frequenzen und gleichzeitig einen höheren Frequenz senden und empfangen.

00:14:57 Sprecher 2

Das heißt, der Chip muss mehr Daten senden und braucht natürlich auch mehr Strom. Also im 5G-Bereich ist m Moment eigentlich keine Verbesserung, aber im WLAN Bereich ist sehr wohl.

00:15:07 Sprecher 2

Wobei da eben, nicht diese mehreren Frequenzbänder verwendet werden, sondern eigentlich nur eines.

00:15:16 Sprecher 2

Das ist halt der Unterschied.

00:15:18 Sprecher 2

Wobei der Frequenzband bei WLAN in dem Bereich, der höher ist deswegen ist auch die Datenübertragung im WLAN Bereich natürlich höher.

00:15:27 Sprecher 2

Aber es ist WLAN-Bereich muss halt nicht so adaptiv sein, wie das 5G Netz.

00:15:35 Sprecher 1

Und dann andere Fokus, also Sicherheit.

00:15:39 Sprecher 1

Es existiert eine Vielzahl an unterschiedlichen Gefahren bei Wi-Fi6 und 5G. Welche Angriffsvektoren haben das größte Potenzial und stellen die Sicherheit der Nutzer dadurch in Gefahr?

00:15:52 Sprecher 2

Also grundsätzlich gibt es neue Verschlüsselungmethoden im 5G-Bereich ,beziehungsweise auch im WLAN-Bereich.

00:16:02 Sprecher 2

Wobei die Angriffsmöglichkeiten, sich durch die neuen Technologien nicht wirklich verändert haben, also auf Provider Seite sehe ich die Infrastruktur, DDoS, die das ist nach wie vor. Einer der größten Angriffsszenarien, wenn nicht sogar größte, den es im Moment gibt.

00:16:19 Sprecher 2

Man sieht man, hört jede Woche von Angriffen auf Infrastruktur.

00:16:23 Sprecher 2

Also das heißt wenn die Infrastruktur mit erhöhten Datenraten niedergedrückt wird, und ist der Dienst nicht verfügbar. Das ist nach wie vor so, das kann auch ein neuer Verschlüsselungpotential nicht lösen.

00:16:37 Sprecher 2

Weiterhin Zero Day Lücken bei Softwarebetriebssystem. Software wenn die Updates nicht eingespielt sind oder wobei der Provider natürlich genötigt sind aktuell zu halten. Aber es gibt Zero Day Lücken, die ausgenutzt werden können um Geräteequipment zu übernehmen. Hardware mäßiger Zugriff, es gibt Möglichkeiten, wenn die Zelle irgendwo vor Ort auch auf einem ein Hausdach steht. Was sie sind, das mit Hardware Zugriff, dass er also eine Software selber einepielt oder mit einem Hammer drauf haut.

00:17:09 Sprecher 2

Werden die Sendermasten genauso zerstört oder übernommen. Das sind alles dieselben Möglichkeiten. Für den User ist wahrscheinlich die größte Bedrohung.

00:17:20 Sprecher 2

Die klassischen ich lade mir eine Applikation runter, das ist ein Virus und Mallware drauf. Das sehe ich als größte Gefahr, aber da können die neuen Technologien eigentlich auch nichts damit machen, weil das eher Betriebssystemthemen sind.

00:17:33 Sprecher 2

Aber trotzdem werden so halt die Netze dann möglicherweise unterwandert.

00:17:39 Sprecher 2

Man-in-the-Middle ist nach wie vor man liest mit, was User und Provider miteinander kommunizieren.

00:17:47 Sprecher 2

Spiegelt, spiegelt die Daten nach und kann so vielleicht sich in die Kommunikation miteinmischen oder sie zerstören. In dem falsche, wie sagt man Funktionsdaten schickt. Sozusagen die Daten gehören jetzt dorthin oder sonstiges.

00:18:05 Sprecher 2

Ja, mit und der klassische einfach mitlesen, wenn man mit dem drinnen ist und sicher über eine der Möglichkeiten rein, quasi in die Kommunikation reingesetzt hat. Das ist nach wie vor möglich, also das hat sich durch die neuen Sicherheitstechnologien nicht geändert. Natürlich ist es besser geworden.

00:18:24 Sprecher 2

Also die Sicherheit mit der neuen Verschlüsselung ist besser aber die Angriffsszenarien sind eigentlich dieselben.

00:18:32 Sprecher 1

Alles klar, dann ein sehr guter Übergang, weil die nächste Frage lautet. Inwieweit können die Protokolle und die Verschlüsselung bei Wi-Fi6 und 5G Gefahren reduzieren? Glauben Sie aus ihrer Erfahrung, dass es eine Auswirkung auf die Verwendung von WLAN-Hotspots der Nutzerinnen hat?

00:18:52 Sprecher 2

Ja, die Landschaft wie gerade gesagt, ist dieselbe Technologie. Ändert, nicht die Probleme, außer man würde einen wirklichen Technologiewechsel vollziehen der komplett anders funktioniert, was nicht passieren wird.

00:19:09 Sprecher 2

Die Auswirkungen auf WLAN-Hotspots, was den Nutzer eher nicht, weil diejenigen Leute die Nachricht, die jetzt WLAN-Hotspot verwenden aufgrund von ihrem Providerverträgen oder sonstigen werden das weiterhin nutzen.

00:19:2 Sprecher 2

Also ich glaube nicht, dass das sich das so stark ändern wird, weil das sind Gewohnheitsachen, die jetzt nicht die Sachen wirklich verändern werden, denke ich.

00:19:36 Sprecher 2

Also, für Firmen wird sich auch nichts ändern, weil wenn man WIFI bis jetzt verwendet hat, wird man es weiterhin verwenden und nicht anpassen. Warum auch.

00:19:4 Sprecher 2

Weil es gibt auch keinen Grund in Wirklichkeit.

00:19:52 Sprecher 2

Also WLAN-Hotspots werden weiterhin von denselben Nutzer verwendet werden.

00:19:55 Sprecher 2

Ist meiner Meinung. Mein, ich habe keine Studien dazu, aber bin mirziemlich sicher, dass das weiterhin so bleiben wird.

00:20:04 Sprecher 1

Okay.

00:20:04 Sprecher 2

Also Enduser hat jetzt nicht den, hat jetzt nicht darauf gewartet, dass eine neue Technologie gekommen ist, die jetzt sicher ist, dass er jetzt wieder ein WLAN-Hotspot verwendet.

00:20:19 Sprecher 1

Okay, und wie ist es generell jetzt bei einem Wi-Fi6? Ja würde ich jetzt auch sagen, Firmen verwenden das also mit der 802.1x zum Beispiel, das ist Zertifikatsbasierend. Aber wie sieht es beim 5G? Die ganzen Protokolle, die erneut gekommen, neu implementiert worden sind.

00:20:40 Sprecher 1

Gibt es da irgendwo, Auswirkungen aufgrund dessen?

00:20:51 Sprecher 2

Also für die Gefahr ist es natürlich besser.

00:20:53 Sprecher 2

Also dieses neue AKA-System, das tauscht.

00:20:58 Sprecher 2

Das Tauscht jetzt nicht mehr direkte Keys aus, sondern erzeugt andere Subcipher könnte man sagen, die ausgetauscht werden, die genauso wie Standardverschlüsselung schlecht zurückzurechnen sind. Das erhöht natürlich die Verschlüsselung enorm.

00:21:13 Sprecher 2

Beziehungsweise kann man diese, durch diesen Haupt, also, diesen schon gecipherten Key der quasi als Grund Keys ist, der aber schon verschlüsselt ist.

00:21:23 Sprecher 2

Besser verwenden für mehrere Varianten für den Datenaustausch. Natürlich betrifft es jetzt nicht nur quasi die eine Wi-Fi Verbindung oder die eine 5G Verbindung, aber wenn wir über 5G reden, gibt aber ähnliche Varianten bei Wi-Fi 6.

00:21:41 Sprecher 2

Das hilft halt, wenn man zum Beispiel Provider wechselt oder in irgendein anderes privates Netz sich einloggen würde.

00:21:51 Sprecher 2

Das erhöht enorm die Sicherheit, weil viel es schwieriger ist damit zu sniffen oder beziehungsweise zu cracken.

00:21:57 Sprecher 1

Gut. Dann, wie würden sie die jeweiligen technologischen Verbesserungen der Standards beurteilen in Bezug auf Effizienz und Sicherheit. Inwieweit werden die Nutzer dadurch profitieren?

00:22:07 Sprecher 2

Also wie gerade erwähnt mit neuen Technologien, also wie was Wi-Fi6, 5G, neue Cipher-Methoden. Neue Austauschmethoden der Cipher der Sicherheit, steigert quasi passiv für den Endnutzer. Das heißt, er profitiert auf jeden Fall einmal davon.

00:22:30 Sprecher 2

Bandbreite, ist natürlich enorm erhöht, also gerade für Leute wie Gamer, die eine niedrige Latenz brauchen. Profitieren vom 5G enorm also jetzt davon ausgenommen, sie haben keine gut genug Standleitung. Ja also von 4G mit einer eher langsamen Latenz haben natürlich keine Freude dabei. Hingegen mit 5G ist es schon sehr gut.

00:22:53 Sprecher 2

Und kaum also vom Nutzerfeeling kaum ein Unterschied im Vergleich zu einer Standleitung.

00:23:00 Sprecher 2

Das nächste große Thema autonomes Fahren, also die Industrie und die Autoindustrie kann endlich damit beginnen, diese neue Technologie einzubringen, weil mit 5G ist es relativ sicher. In Bezug auf Network Slicing, also eigene Infrastruktur, virtualisierte Hardware, extra nur für quasi die Autolommunikation. Das heißt, die Industrie profitiert davon enorm, was vorher eigentlich nicht möglich gewesen ist in der Form. Das macht es überhaupt erst möglich, durch die niedrige Latenz.

00:23:35 Sprecher 2

In Bezug auf WLAN ist es auch also Grad für Firmen, die oder muss nicht unbedingt Frima sein. Aber gerade wenn man mehrere User hat, die vielleicht hohe Bandbreiten benötigen sind mit Wi-Fi ac.

00:23:49 Sprecher 2

Irgendwann schneller, also doch relativ schnell ausgebremst, wenn jetzt 4,5,6 Leute beginnen, hier größere Daten auszutauschen.

00:24:00 Sprecher 2

Problem mit ax, jetzt wirklich durch MIMO und hohe Bandbreiten, das heißt, es können mehrfach reden und kriegen mehr Zeitschlitze, ist das ein ganz anderes Feeling und fällt dem normalen Standardnutzer dann gar nicht mehr auf, dass auf einmal 4 Leute gleichzeitig Daten transferieren, was unter dem jetzigen aktuellen ac-Standard eigentlich noch, doch spürbar ist auch für den Standarduser.

00:24:26 Sprecher 1

Okay, dann vielleicht abschließend ja, möchten Sie noch etwas zum Thema Effizienz und Sicherheit in Bezug auf Wi-Fi 6 und 5G erzählen oder sonstige Aspekte ergänzen?

00:24:36 Sprecher 2

Ja also ich, grundsätzlich mal, ich glaub das beide Technologien sehr wichtig sind und der Fortschritt weitergehen wird in den nächsten Jahren. Und wir relativ schnell mit der nächsten Generation dieser Technologien zu tun haben.

00:24:52 Sprecher 2

Grundsätzlich, es wird beides Funktechnologien, die auf ähnlich also auf dieselben Grundprotokolle zugreifen, also beide Technologien sind sehr ähnlich, und das heißt auch die Entwicklung geht Hand in Hand von beiden. Was Sicherheit, was Bandbreite betrifft, was Anwendungsfälle mehr oder weniger. Natürlich aus meiner Sicht, man muss Wi-Fi wirklich eher für konzentrierte Firmen sehen.

00:25:15 Sprecher 2

Die vielleicht weg vom Kabelverbindungen oder in einem alten Gebäude sind, wo es keine Kabelverbindungen gibt. Das heißt, sie haben wirklich, vielleicht nicht, oder vielleicht wollen sie bald nur noch, weil es einfach ist? Ich kann meinen Laptop nehmen kann, in Besprechungszimmer gehen, sonstiges und wirklich immer ein Kabel verlegen haben und sonstiges. Also das ist definitiv für viele Firmen die Zukunft. Und vielleicht ist es doch schon in Verwendung und jetzt wird es noch besser.

00:25:43 Sprecher 2

5G wird für alles außerhalb von Gebäuden, glaub ich der Standard sein und ist es wahrscheinlich auch bald und funktioniert wunderbar. Die Bandbreiten, die jeder einzelne User nutzt, werden noch höher sein. Das heißt, wir werden wahrscheinlich mit 5G in 5 Jahren vielleicht gar nicht mehr auskommen.

00:26:01 Sprecher 2

Also deswegen bin ich mir sicher.

00:26:05 Sprecher 2

Das ist die jetzigen Technologien für die jetzigen Anwendung super sind und mehr als ausreichend und in Zukunft aber wird es weiterhin noch noch schneller noch besser noch sicherer werden.

00:26:23 Sprecher 1

Okay, das ist laut Ihnen kristallisiert sich das jetzt so heraus, dass WLAN eher, also das Hand in Hand geht das beide Technologien da sind, aber das WLAN dann eher diesen Indoorbreich abdeckt.

00:26:34 Sprecher 2

Genau, also es wird sicher 5G aufgrund der unterschiedlichen, also von der aufgrund der Anbindung, wie man die Infrastruktur aufbauen meine ich.

00:26:44 Sprecher 2

Also 5G wird nicht oder kaum gibt sich ausnahmen, aber in einem Gebäude eingesetzt werden.

00:26:52 Sprecher 2

Weil es für den Provider keinen Sinn wirklich macht, sondern WI-FI ist viel besser zu konfigurieren und zu installieren.

00:27:02 Sprecher 2

Und macht doch mehr Sinn, weil aufgrund der höheren Bandbreite, die ich im Office Bereich oder im Home Bereich habe, sei es ist der Fernseher, PCs weiß ich nicht. Welche

Sachen noch verwendet werden, ist es einfach viel wichtiger, dass hohe Bandbreite im lokalen Bereich hat und vorhanden sind. Ist ganz klar der Vorteil von Wi-Fi.

00:27:25 Sprecher 1

Alles klar dann bedanke ich mich recht herzlich.

00:27:28 Sprecher 2

Ja, bitte.

00:27:29 Sprecher 1

Für das Interview.

00:27:30 Sprecher 1

Hiermit beende ich auch die Aufnahme.

Anhang B

Fragebogen

soSci
oFb - der onlineFragebogen

Liebe Teilnehmerinnen und Teilnehmer,

im Rahmen meiner Masterarbeit im Studiengang Wirtschaftsinformatik an der Ferdinand Porsche FernFH, beschäftige ich mich mit der Auswirkung von der Mobilfunktechnologie 5G auf österreichische WLAN-Provider. Für die Fragen ist kein Fachwissen notwendig, diese sind einfach mit Ihrer persönlichen Meinung zu beantworten.

Ihre Daten werden im Zuge dieser Arbeit anonym unter Einhaltung der DSGVO analysiert und streng vertraulich behandelt.

Die Befragung wird eine Zeit von etwa 3-5 Minuten in Anspruch nehmen. Es gibt keine richtigen oder falschen Antworten. Ich bitte Sie um eine ehrliche Beantwortung der gestellten Fragen.

Vielen Dank für Ihre Zeit und Teilnahme an dieser Befragung.

Bei Rückfragen stehe ich sehr gerne zur Verfügung!

Marijan Grabovac
marijan.grabovac@mail.fernfh.ac.at

soSci
oFb - der onlineFragebogen

1. Haben Sie schon einmal einen österreichischen WLAN-Hotspot benutzt?

- ○ Ja
- ○ Nein

Marijan Grabovac B.A., Ferdinand Porsche FernFH – 2022

soSci
oFb - der onlineFragebogen

1. Im folgenden Abschnitt geben Sie bitte Ihre persönliche Meinung ab, warum Sie persönlich einen österreichischen WLAN-Hotspot nutzen.

Ich ersuche Sie, die verschiedenen Aussagen spontan und ehrlich zu beantworten. Die Fragen nach dem Grad Ihres Zutreffen bewerten, es gibt dabei keine richtigen oder falschen Antworten. Bitte Beantworten Sie alle nachfolgenden Fragen.

Ich verwende österreichische WLAN-Hotspot weil,	trifft gar nicht zu ○ ○ ○ ○ ○ ○ trifft völlig zu
ich mir Datenvolumen beim eigenen Mobilfunkvertrag sparen möchte	
ich dadurch schnelleres Internet habe	
meine aufgerufenen Webseiten und Applikationen schneller laden	
das angebotene Service kostenlos ist	
mein Mobilfunkempfang im Indoorbereich schlechter ist	
mein Mobilfunkempfang im Outdoorbereich schlechter ist	
mein Mobilfunkanbieter keine gute nationale Abdeckung hat	
der Akku meines Endgeräts länger hält	

Marijan Grabovac B.A., Ferdinand Porsche FernFH – 2022

soSci
oFb - der onlineFragebogen

1. Im folgenden Abschnitt geben Sie bitte Ihre persönliche Meinung ab, ob die Nutzung von österreichische WLAN-Hotspots sicher sind.

Ich ersuche Sie, die verschiedenen Aussagen spontan und ehrlich zu beantworten. Die Fragen nach dem Grad Ihres Zutreffen bewerten, es gibt dabei keine richtigen oder falschen Antworten. Bitte Beantworten Sie alle nachfolgenden Fragen.

Die Nutzung von österreichischen WLAN-Hotspots sind sicher weil,	trifft gar nicht zu	trifft völlig zu
ich nur verschlüsselte Webseiten aufrufe	○ ○ ○ ○ ○ ○	
ich einen VPN-Dienst für die Verschlüsselung nutze	○ ○ ○ ○ ○ ○	
ich keine persönlichen Login-Daten auf Webseiten eingebe	○ ○ ○ ○ ○ ○	
der WLAN-Provider aktuelle Sicherheitsprotokolle verwendet	○ ○ ○ ○ ○ ○	
der WLAN-Provider seine Hardware und Software vor Dritten schützt	○ ○ ○ ○ ○ ○	
Hacker*Innen die Kommunikation nicht mitlesen können	○ ○ ○ ○ ○ ○	
mein Endegeräte die aktuellsten Updates besitzen	○ ○ ○ ○ ○ ○	

Marijan Grabovac B.A., Ferdinand Porsche FernFH – 2022

soSci
oFb - der onlineFragebogen

60% ausgefüllt

1. Welches Geschlecht haben Sie?

- ○ weiblich
- ○ männlich
- ○ divers

2. Wie alt sind Sie?

[Bitte auswählen]

3. Welches ist der höchste Bildungsabschluss, den Sie haben?

- ○ Pflichtschule
- ○ Lehre/Mittlere Schule
- ○ Matura
- ○ Universität/FH/Akadamien

4. Bei welchem Mobilfunkanbieter sind Sie registriert?

- ○ Magenta
- ○ A1
- ○ Drei
- ○ Bob
- ○ Yesss
- ○ HoT
- ○ Sonstige

Weiter

Marijan Grabovac B.A., Ferdinand Porsche FernFH – 2022

soSci
oFb - der onlineFragebogen

Vielen Dank für Ihre Teilnahme!

Ich möchte mich ganz herzlich für Ihre Mithilfe bedanken.

Ihre Antworten wurden gespeichert, Sie können das Browser-Fenster nun schließen.

Marijan Grabovac B.A., Ferdinand Porsche FernFH – 2022