

Kurt Behnke · Jürgen Karla
Wilhelm Mülder

Grundkurs Mobilfunk und Mobile Business

Anwendungen, Technologien,
Geschäftsfelder



Springer Vieweg

Grundkurs Mobilfunk und Mobile Business

Kurt Behnke • Jürgen Karla • Wilhelm Mülder

Grundkurs Mobilfunk und Mobile Business

Anwendungen, Technologien,
Geschäftsfelder



Springer Vieweg

Kurt Behnke
Viersen, Deutschland

Wilhelm Mülder
FB Wirtschaftswissenschaften
Hochschule Niederrhein
Mönchengladbach, Deutschland

Jürgen Karla
Wirtschaftsinformatik
Hochschule Niederrhein
Mönchengladbach, Deutschland

ISBN 978-3-658-00140-7

<https://doi.org/10.1007/978-3-658-00141-4>

ISBN 978-3-658-00141-4 (eBook)

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über <http://dnb.d-nb.de> abrufbar.

Springer Vieweg

© Springer Fachmedien Wiesbaden GmbH, ein Teil von Springer Nature 2022

Das Werk einschließlich aller seiner Teile ist urheberrechtlich geschützt. Jede Verwertung, die nicht ausdrücklich vom Urheberrechtsgesetz zugelassen ist, bedarf der vorherigen Zustimmung des Verlags. Das gilt insbesondere für Vervielfältigungen, Bearbeitungen, Übersetzungen, Mikroverfilmungen und die Einspeicherung und Verarbeitung in elektronischen Systemen.

Die Wiedergabe von allgemein beschreibenden Bezeichnungen, Marken, Unternehmensnamen etc. in diesem Werk bedeutet nicht, dass diese frei durch jedermann benutzt werden dürfen. Die Berechtigung zur Benutzung unterliegt, auch ohne gesonderten Hinweis hierzu, den Regeln des Markenrechts. Die Rechte des jeweiligen Zeicheninhabers sind zu beachten.

Der Verlag, die Autoren und die Herausgeber gehen davon aus, dass die Angaben und Informationen in diesem Werk zum Zeitpunkt der Veröffentlichung vollständig und korrekt sind. Weder der Verlag noch die Autoren oder die Herausgeber übernehmen, ausdrücklich oder implizit, Gewähr für den Inhalt des Werkes, etwaige Fehler oder Äußerungen. Der Verlag bleibt im Hinblick auf geografische Zuordnungen und Gebietsbezeichnungen in veröffentlichten Karten und Institutionsadressen neutral.

Planung: Petra Steinmüller

Springer Vieweg ist ein Imprint der eingetragenen Gesellschaft Springer Fachmedien Wiesbaden GmbH und ist ein Teil von Springer Nature.

Die Anschrift der Gesellschaft ist: Abraham-Lincoln-Str. 46, 65189 Wiesbaden, Germany

Vorwort

Mobile Telefonie und Mobilkommunikation haben in den vergangenen Jahrzehnten die Welt verändert. Die Einflüsse reichen von der privaten Kommunikation über veränderte Geschäftsprozesse bis zu autonom operierenden, vernetzten Systemen. Die Idee zu unserem Buch entstand, als die ersten Managerinnen und Manager ihre Smartphones im Geschäftslben nicht mehr ausschließlich zum mobilen Telefonieren, sondern auch zur Unterstützung der anderen geschäftlichen Aktivitäten nutzen wollten. Im Fokus stand somit die Möglichkeit, mit dem Smartphone Business zu betreiben. Der Titel war damit zunächst klar: „Mobile Business“.

Dabei ist die Mobilität nicht nur ein Feature der Entwicklung der digitalen Kommunikation und des Internet, sondern sie bestimmt in vielen Bereichen ihre Richtung. Das vorliegende Buch befasst sich mit den technologischen und betriebswirtschaftlichen Aspekten der Mobilkommunikation. Anwendungen mobiler Technik hängen in hohem Maß von den Möglichkeiten und Gegebenheiten dieser Technik selbst ab.

In der – zugegeben recht langen Phase des Niederschreibens – wurde immer deutlicher, dass im Grunde genommen alles, was per Laptop und Internet-Anschluss möglich ist, inzwischen auch über mobile Endgeräte möglich war. Das Display ist ggfs. kleiner und für Ungeübte eignet sich die Touchscreen-Tastatur auch nicht unbedingt zum Anfertigen langer Texte. Dennoch: Für den tatsächlichen mobilen Gebrauch – beim Frühstück die E-Mails abrufen, unterwegs mal schnell eine mobile Videokonferenz durchführen oder ein Bahnticket kaufen, vor dem Abendessen die Termine für den nächsten Tag prüfen – eignen sich Smartphones weitaus besser als Laptops. Wir haben deshalb versucht, uns auf diejenigen Anwendungsbereiche zu konzentrieren, für die mobile Endgeräte am besten geeignet sind.

Ein Verständnis mobiler Anwendungen setzt ein Basisverständnis der verwendeten Technologie voraus. Aus diesem Grund werden wesentliche Aspekte der mobilen Nachrichtentechnik und der wichtigsten Mobilfunknetzwerke behandelt. Dazu gehören die heute weltweit installierten öffentlichen Mobilfunknetze in lizenzierten Frequenzbändern, aber auch lokale Netze und Weitverkehrsnetze im nicht lizenzierten Spektrum. Wir streben dabei aber nicht an, die elektrotechnischen, nachrichtentechnischen oder informatischen Grundlagenwerke zu ersetzen. Angestrebt ist die Schaffung eines grundlegenden

Verständnisses der Technologie. Dies ist ein Fundament für Lösungen, die Antworten auf die Herausforderungen generieren, die durch den Einsatz der mobilen Kommunikation in Unternehmen und für Privatpersonen geschaffen werden. Die Erfahrungen aus einer Reihe von Lehrveranstaltungen an der Hochschule Niederrhein und an der RWTH Aachen University sind in die Auswahl der Inhalte und die Bestimmung der Darstellungstiefe eingeflossen.

Im Rahmen unserer Recherchen zu diesem Buch stellten wir auch fest, dass es zwar einige technische Anleitungen zur Entwicklung mobiler Apps gab, über die technologischen Grundlagen der verschiedenen Mobilfunkgenerationen 2G bis 5G wurde aber eher wenig in Lehrbüchern geschrieben. Dies gilt insbesondere, wenn der Leserkreis über Studierende der Nachrichtentechnik hinaus gehen und ein interdisziplinäres Publikum im Rahmen eines „Grundkurs“ angesprochen werden soll. Wir haben daher großen Wert auf eine tiefergehende und dennoch verständliche Erläuterung der Mobilfunktechnologie in den aktuellen Mobilfunkgenerationen gelegt. Zum besseren Verständnis erläutern wir auch die physikalischen Grundlagen und geben einen kurzen historischen Überblick über die Entwicklung der Kommunikationstechnik.

Wer ein Buch über Mobile Business schreibt, läuft Gefahr, dass die Inhalte rasch veralten. Dies ist einer der Gründe, warum in den letzten Jahren das eine oder andere Kapitel mehrmals von Grund auf neu geschrieben wurde. Möglicherweise besteht hierin der Grund, dass es kaum aktuelle Lehrbücher zu diesem Thema gibt. Sehr deutlich wurde dies bei den Ausführungen über mobile Endgeräte, die sich bekanntlich in der Vergangenheit durch technische Neuerungen, aber auch bedingt durch die Marketing-Strategien der Hersteller nahezu jährlich änderten. Deshalb finden Sie keine tagesaktuellen Beschreibungen von Smartphone-Modellen. Stattdessen zeigen wir die historische Entwicklung bei den mobilen Endgeräten auf.

Unser Lehrbuch eignet sich als Grundlagenwerk für Vorlesungen und Seminare im Rahmen von Studiengängen der Betriebswirtschaftslehre, Wirtschaftsinformatik, Informatik, Kommunikationstechnik und des Wirtschaftsingenieurwesens. Sie müssen unser Buch nicht vom Anfang bis zum Ende durchlesen. Jedes Kapitel kann eigenständig genutzt werden. Querverweise erleichtern das Auffinden anderer Kapitel, in denen ein bestimmtes Thema bereits genauer behandelt wurde. Am Schluss jedes Kapitels finden Sie Fragen zur Lernkontrolle. Diese Fragen könnten auch beispielsweise im Rahmen einer Prüfung genutzt werden. Auf der Website zu diesem Buch finden sich ergänzende Materialien:

<http://www.grundkurs-mobilfunk.de>

Die Autoren sind unter buch@grundkurs-mobilfunk.de erreichbar. Dozierenden stellen wir über die Webseite gerne Material in Form von Abbildungen und Foliensätzen als Download zur Verfügung.

Wir haben unser Buch im Rahmen unserer eigenen Vorlesungen und Seminare eingesetzt und erprobt. Die Teilnehmerinnen und Teilnehmer dieser Veranstaltungen haben uns mit ihren Fragen und Anmerkungen geholfen, die Inhalte dieses Buches zu präzisieren und zu konkretisieren.

Wir wünschen Ihnen viel Vergnügen beim Lesen bzw. Durcharbeiten dieses Buchs. Den Studierenden, die über die behandelten Inhalte Prüfungen ablegen müssen, wünschen wir darüber hinaus viel Erfolg. Falls Ihnen in unserem Buch Fehler auffallen oder Sie Verbesserungsvorschläge haben, können Sie uns diese gerne per E-Mail mitteilen.

Mönchengladbach, Deutschland
November 2021

Kurt Behnke
Jürgen Karla
Wilhelm Mülder

Inhaltsverzeichnis

| | |
|---|----|
| 1 Grundlegende Begriffe und Konzepte im Mobilfunk und im Mobile Business | 1 |
| 1.1 Einführung und Lernziele | 1 |
| 1.2 Mobile Business | 1 |
| 1.3 Mobilfunk | 4 |
| 1.4 Treiber im Mobile Business. | 5 |
| 1.4.1 Mobile Breitbandzugänge | 5 |
| 1.4.2 Smartphones und Tablets | 6 |
| 1.4.3 Tarifstrukturen | 7 |
| 1.4.4 Mobile Apps und Mobile Games | 7 |
| 1.4.5 Steigende Mediennutzung | 8 |
| 1.4.6 Maschine-zu-Maschine-Kommunikation und Internet der Dinge | 9 |
| 1.5 Geschichte der Mobilkommunikation | 10 |
| 1.5.1 Die Anfänge | 10 |
| 1.5.2 Optische Telegrafen | 10 |
| 1.5.3 Mobilkommunikation auf Basis elektromagnetischer Wellen | 13 |
| 1.5.4 Mobile Telefonie | 16 |
| 1.6 Fragen | 24 |
| Literatur. | 24 |
| 2 Allgemeine Grundlagen des Mobilfunks | 25 |
| 2.1 Einführung und Lernziele | 25 |
| 2.2 Systeme und Netze des Mobilfunsks. | 26 |
| 2.2.1 Mobilfunknetze und Festnetze | 26 |
| 2.2.2 Architektur eines Mobilfunknetzes | 27 |
| 2.2.3 Das Radio-Netzwerk: Basisstationen und Mobilfunkzellen | 28 |
| 2.2.4 Das Kern-Netz | 31 |
| 2.2.5 Systeme zum Netzmanagement, zur Netzüberwachung und Abrechnung | 32 |
| 2.3 Die SIM-Karte und die Authentifizierung der Teilnehmer | 33 |
| 2.4 Prozeduren und Abläufe im Mobilfunkbetrieb | 36 |

| | | |
|----------|--|-----------|
| 2.4.1 | Identifikation des Netzes | 36 |
| 2.4.2 | Anmeldung am Netz | 37 |
| 2.4.3 | Teilnehmer-Authentifizierung | 38 |
| 2.5 | Abläufe bei mobiler Telekommunikation | 40 |
| 2.5.1 | Abgehendes Gespräch im Mobilfunknetz | 41 |
| 2.5.2 | Ankommendes Gespräch im Mobilfunknetz | 42 |
| 2.5.3 | Kurznachrichten und Cell-Broadcast | 43 |
| 2.5.4 | Mobile Datenübertragung | 44 |
| 2.5.5 | Handover (Übergabe) von Basisstation zu Basisstation | 46 |
| 2.5.6 | Roaming | 48 |
| 2.6 | Fragen | 50 |
| | Literatur | 51 |
| 3 | Technische Grundlagen des Mobilfunks | 53 |
| 3.1 | Einführung und Lernziele | 53 |
| 3.2 | Funksignale und Datenübertragung | 54 |
| 3.2.1 | Elektromagnetische Wellen | 54 |
| 3.2.2 | Die Ausbreitung von elektromagnetischen Wellen | 57 |
| 3.2.3 | Antennen | 60 |
| 3.2.4 | Reichweite und Abdeckungsbereich einer Funkzelle | 65 |
| 3.2.5 | Bewegte Objekte und der Doppler Effekt | 67 |
| 3.3 | Datenübertragung durch elektromagnetische Wellen | 69 |
| 3.3.1 | Modulation | 69 |
| 3.3.2 | Fehlerquellen und Fehlerkorrektur | 77 |
| 3.3.3 | Vielfach-Nutzung: Medienzugriffsverfahren und Multiplexverfahren | 80 |
| 3.4 | Fragen | 90 |
| | Literatur | 92 |
| 4 | Lizenzierte Mobilfunksysteme | 93 |
| 4.1 | Einführung und Lernziele | 93 |
| 4.2 | Die Entwicklung der Standards der digitalen Mobilkommunikation | 94 |
| 4.3 | GSM Überblick | 95 |
| 4.3.1 | GSM-Systemarchitektur | 95 |
| 4.3.2 | GSM-Funkschnittstelle | 97 |
| 4.3.3 | GSM Besonderheiten und Ausblick | 100 |
| 4.4 | Systeme der dritten Generation | 101 |
| 4.4.1 | Die Architektur von W-CDMA-Netzen | 101 |
| 4.4.2 | Die 3G-Radioschnittstelle | 102 |
| 4.5 | Systeme der vierten Generation nach dem LTE-Standard | 104 |
| 4.5.1 | LTE-Netzwerk Architektur | 104 |
| 4.5.2 | Die LTE-Funkschnittstelle | 106 |

| | | |
|----------|---|------------|
| 4.5.3 | LTE-Besonderheiten | 112 |
| 4.5.4 | Erweiterungen und Anwendungen von LTE | 117 |
| 4.6 | Mobilfunk der 5. Generation (5G) | 125 |
| 4.6.1 | 5G Überblick | 125 |
| 4.6.2 | Anforderungen an 5G | 125 |
| 4.6.3 | Technische Lösungen in 5G | 127 |
| 4.6.4 | 5G-Frequenzbänder und Bandbreiten | 128 |
| 4.6.5 | 5G-Architektur | 132 |
| 4.6.6 | Sichere Kommunikation und Internet der Dinge in 5G | 134 |
| 4.6.7 | Virtuelle Strukturen in 5G | 135 |
| 4.6.8 | Cloud Edge Computing | 135 |
| 4.7 | Fragen | 136 |
| | Literatur | 137 |
| 5 | Lizenzfreie Kommunikationstechniken | 139 |
| 5.1 | Einführung und Lernziele | 139 |
| 5.2 | Lizenzfreie Funkfrequenzen | 140 |
| 5.3 | Radio Frequency Identification (RFID) | 141 |
| 5.3.1 | Transponder | 142 |
| 5.3.2 | Lesegeräte | 146 |
| 5.3.3 | Backend-System | 147 |
| 5.3.4 | RFID Betriebsfrequenzen | 148 |
| 5.4 | NFC | 149 |
| 5.5 | Optische Erfassung mittels Barcode und Mobile Tagging | 152 |
| 5.6 | Bluetooth | 153 |
| 5.6.1 | Bluetooth „Classic“ | 153 |
| 5.6.2 | Bluetooth Low Energy | 155 |
| 5.6.3 | iBeacon | 157 |
| 5.7 | Zigbee | 158 |
| 5.8 | WLAN | 162 |
| 5.8.1 | WLAN Übersicht | 162 |
| 5.8.2 | WLAN Funktechnik | 165 |
| 5.8.3 | WLAN und IoT | 167 |
| 5.8.4 | WLAN-Nutzung | 168 |
| 5.8.5 | Vergleich der Personal- und Local-Area Technologien im Internet of Things | 168 |
| 5.9 | Low Power Wide Area Netze | 170 |
| 5.9.1 | LoRaWAN | 172 |
| 5.9.2 | SigFox | 173 |
| 5.10 | Fragen | 174 |
| | Literatur | 176 |

| | |
|--|-----|
| 6 Mobile Endgeräte | 177 |
| 6.1 Einführung und Lernziele | 177 |
| 6.2 Geschichte der mobilen Endgeräte | 178 |
| 6.2.1 Entstehung der Bezeichnung „Handy“ | 178 |
| 6.2.2 Ausgewählte mobile Endgeräte in der historischen Entwicklung | 178 |
| 6.3 Endgeräteklassen | 194 |
| 6.3.1 Klassifizierungsmerkmale | 194 |
| 6.3.2 Geräteklassen | 196 |
| 6.4 Mobile Betriebssysteme | 198 |
| 6.4.1 Apple iOS, iPadOS, watchOS, tvOS | 198 |
| 6.4.2 Android OS | 201 |
| 6.5 Endgeräte für Maschine-zu-Maschine und Kritische Kommunikation | 203 |
| 6.5.1 Kritische Kommunikation | 204 |
| 6.5.2 Internet of Things | 206 |
| 6.6 Fragen | 209 |
| Literatur | 210 |
| 7 Akteure und Ecosystems im Mobile Business | 215 |
| 7.1 Einführung und Lernziele | 215 |
| 7.2 Akteure in der Mobilfunkindustrie | 216 |
| 7.2.1 Regulierung und Standards | 216 |
| 7.2.2 Netzaufbau und Netzbetrieb | 220 |
| 7.2.3 Vertrieb und Kundenbetreuung | 224 |
| 7.3 Entwicklung der App Economy und Mobile Business Ecosystems | 227 |
| 7.4 Mobile Business Ecosystem und Platform Economies | 228 |
| 7.4.1 Entwicklung der Mobile Platform Ecosystems | 230 |
| 7.4.2 Auswirkungen auf Netzbetreiber | 233 |
| 7.5 Fragen | 237 |
| Literatur | 238 |
| 8 Mobile Anwendungssysteme | 241 |
| 8.1 Einführung und Lernziele | 241 |
| 8.2 Kunden-Apps | 242 |
| 8.2.1 Mobiles Marketing | 242 |
| 8.2.2 Mobile Commerce | 245 |
| 8.2.3 Mobile Ticketing | 246 |
| 8.2.4 Mobile Payment | 249 |
| 8.2.5 Mobile Entertainment | 253 |
| 8.2.6 Mobile Health & Fitness | 255 |
| 8.3 Business Apps | 255 |
| 8.3.1 Mobiles CRM | 256 |
| 8.3.2 Mobiles SCM | 256 |
| 8.3.3 Mobiles Human Resource Management | 258 |

| | | |
|----------|---|------------|
| 8.4 | Apps für Maschinen | 260 |
| 8.4.1 | Maschine zu Maschine Kommunikation | 260 |
| 8.4.2 | Gebäudemanagement und Smart Metering | 262 |
| 8.4.3 | Umwelt- und Katastrophenschutz | 264 |
| 8.4.4 | Autonomes Fahren | 264 |
| 8.5 | Mobile Geschäftsprozesse | 267 |
| 8.5.1 | Kundenzentrierte Geschäftsprozesse | 268 |
| 8.5.2 | Mitarbeiterzentrierte Geschäftsprozesse | 269 |
| 8.6 | Technologien zur Identifikation und zur Ortung von mobilen Endgeräten | 271 |
| 8.6.1 | Ortung von mobilen Endgeräten | 272 |
| 8.6.2 | Netzbasierte Ortung (Tracking) | 272 |
| 8.6.3 | Terminalbasierte Ortung (Positioning) | 275 |
| 8.6.4 | Ortung mittels Personal Area Networks | 276 |
| 8.6.5 | Personalisierung | 278 |
| 8.7 | Fragen | 279 |
| | Literatur | 280 |
| 9 | Sicherheit und Gesundheit | 283 |
| 9.1 | Einführung und Lernziele | 283 |
| 9.2 | Schutzziele | 284 |
| 9.3 | Angriffsmöglichkeiten im Mobilfunksystem | 285 |
| 9.3.1 | Sicherheit im öffentlichen Mobilfunk | 285 |
| 9.3.2 | Sicherheit im WLAN | 287 |
| 9.4 | Schutzmaßnahmen | 289 |
| 9.4.1 | Organisatorische Schutzmaßnahmen | 289 |
| 9.4.2 | Mobile Device Management in Unternehmen | 290 |
| 9.4.3 | Nutzungsformen privater mobiler Endgeräte in Unternehmen | 291 |
| 9.5 | Mobilfunk und Gesundheit | 293 |
| 9.6 | Fragen | 296 |
| | Literatur | 297 |



Grundlegende Begriffe und Konzepte im Mobilfunk und im Mobile Business

1

1.1 Einführung und Lernziele

Mobilfunknetze sind heute überall auf der Welt präsent und für praktisch jeden verfügbar. In Deutschland gibt es über 150 Millionen Mobilfunkanschlüsse – das sind deutlich mehr als es Einwohner gibt [Bundesnetzagentur 2021]. In der Gesamtmenge enthalten sind ca. 30 Millionen sogenannter M2M-Anschlüsse für die Datenkommunikation zwischen Maschinen. Gleiches gilt für praktisch alle Industrieländer, und sogar in den Entwicklungs- und Schwellenländern kann von einer Vollversorgung der Bevölkerung mit Mobilfunktechnologie gesprochen werden. Weltweit nutzen 5,2 Milliarden Menschen ein mobiles Endgerät [We are Social 2021, S. 187]. Neben den Mobilfunknetzen gibt es weitere Möglichkeiten der mobilen Datenkommunikation, z. B. über Wireless Local Area Networks (WLAN). Die technischen Möglichkeiten der drahtlosen Kommunikation sind die Basis für darauf aufbauende Dienste und Anwendungen, die sich unter dem Begriff „Mobile Business“ zusammenfassen lassen. In diesem Kapitel werden grundlegende Begriffe erläutert:

- Sie lernen wichtige Grundbegriffe zu Mobile Business kennen.
- Sie können die Begriffe „Mobilfunk“ und „Mobilfunknetz“ erläutern.
- Sie kennen die historische Entwicklung der Mobilfunktechnologien.
- Sie kennen die wichtigsten Treiber, die für den Erfolg der Mobilfunktechnologien verantwortlich sind.

1.2 Mobile Business

Mobil bedeutet transportabel, beweglich, aber auch einsatzbereit. Ursprünglich stammt dieses Wort aus der französischen Militärsprache und wird als „abmarschbereit“ übersetzt.

Wenn heute der Begriff *Mobile Business* (manchmal auch als M-Business abgekürzt) verwendet wird, dann ist gemeint, dass geschäftliche Aktivitäten dank mobiler Endgeräte und Verwendung von Mobilfunknetzen unabhängig von vorgegebenen Orten (Geschäftsräume, Büros) durchgeführt werden können. Bestehende Geschäftsprozesse werden hierdurch verbessert oder erweitert, neuartige Geschäftsfelder werden erschlossen. Mobile Business nutzt technische Eigenschaften und wirtschaftliche Potenziale, die Electronic Business (E-Business) nicht oder lediglich rudimentär aufweist. Die folgenden Merkmale und Eigenschaften erlauben die genauere Charakterisierung von Mobile Business und dienen auch zur Abgrenzung gegenüber E-Business (Abts und Mülder 2017, S. 373 f.):

- **Mobile Endgeräte**

Es werden mobile Endgeräte, insbesondere Smartphones und Tablets genutzt. Diese Geräte sind leichter und einfacher zu transportieren als Desktop-PCs oder Laptops.

- **Ortsunabhängigkeit**

Mobile Dienste sind unabhängig vom Aufenthaltsort des Anwenders überall nutzbar, vorausgesetzt, es existiert ein flächendeckendes Mobilfunknetz. Allerdings haben die Netze derzeit immer noch Lücken in der Funkabdeckung („Funklöcher“). Dies gilt insbesondere für ländliche, dünn besiedelte Bereiche.

- **Ortung**

Der aktuelle Aufenthaltsort eines mobilen Endgeräts kann in der Regel ermittelt werden, und zwar entweder über die Ortung innerhalb der Mobilfunkzelle, über lokale Netze oder durch Satellitensysteme.

- **Identifizierbarkeit**

Jeder Nutzer im Mobilfunknetz ist eindeutig identifizierbar durch den Abschluss eines Vertrags mit einem Mobilfunknetzwerkbetreiber (auch als Mobile Network Operator, abgekürzt MNO, bezeichnet).

- **Verfügbarkeit**

Mobile Geräte können aufgrund geringer Größe, Gewicht und langer Betriebsdauer ständig eingeschaltet im Stand-by-Modus mitgeführt werden und sind meist unverzüglich benutzbar.

- **Einfachheit**

Die einfache und intuitive Bedienbarkeit von mobilen Endgeräten, insbesondere mittels Touch-Interface oder Sprachsteuerung, ist ein Vorteil gegenüber dem PC. Anwender haben daher eine geringere Hemmschwelle bei der Verwendung mobiler Geräte, was zu einer höheren Akzeptanz von Mobile Business-Lösungen führt.

- **Kostengünstig**

Leistungsfähige mobile Endgeräte können zu niedrigen Preisen beschafft werden. In vielen Ländern sind mobile Endgeräte häufiger im Einsatz als PCs.

Während beim Mobile Business die mobilen geschäftlichen Aktivitäten im Mittelpunkt stehen, wird allgemein die Nutzung vernetzter mobiler Endgeräte zur Ausführung von Programmen als *Mobile Computing* bezeichnet. Hierbei stehen Hard- und Software im

Mittelpunkt. Im Kontext von Mobile Computing existieren noch weitere Begriffe: *Ubiquitous Computing* bedeutet, dass Computer überall zu finden sind und eingesetzt werden. Durch Miniaturisierung und Vernetzung steht Computerleistung praktisch überall zur Verfügung. Bei *Wearable Computing* wird der Computer vom Nutzer direkt am Körper oder in der Kleidung getragen. Anders als beim Smartphone bleiben die Hände frei, die Geräte können nicht vergessen werden und sind stets eingeschaltet. Bei *Edge Computing* findet Datenverarbeitung an den Endknoten eines Netzwerks statt. Daten werden dort erfasst und verarbeitet, wo sie entstehen. Anstatt große Datenmengen über hunderte von Kilometern von dort zum nächsten Rechenzentrum zu übertragen, erfolgt die Verarbeitung direkt an der Maschine. Besondere Bedeutung erlangt Edge Computing bei industriellen Anwendungen, die unter dem Begriff *Internet of Things* (IOT) zusammengefasst werden.

Mobile Business erweitert die Anwendungsmöglichkeiten von E-Business, indem wirtschaftliche Transaktionen, wie z. B. der Kauf eines Bahn-Tickets, vollumfänglich per Smartphone möglich sind. Außerdem eröffnen sich durch Mobile Business völlig neue Geschäftsfelder. Die verschiedenen Anwendungen lassen sich anhand der beteiligten Transaktionspartner wie folgt abgrenzen:

Business to Consumer (B2C)

B2C umfasst geschäftliche Beziehungen zwischen Unternehmen und privaten Konsumenten. Im Mobile Business lassen sich hier vier Anwendungsschwerpunkte feststellen: Transaktionen (z. B. mobiler Ticketkauf), Kommunikation (z. B. Telefonie, SMS, E-Mail), Informationen (z. B. Suchen, Abruf aktueller Nachrichten) und Unterhaltung (z. B. Podcasts, Mobile Games).

Business to Business (B2B)

Im B2B-Bereich handelt es sich bei den Transaktionspartnern um zwei oder mehr Unternehmen. Ein Beispiel ist das Tracking (Verfolgen) der Paketauslieferung eines Logistikunternehmens durch das bestellende Unternehmen.

Intra-Business und Business to Employee (B2E)

Die mobilen Anwendungen werden innerhalb eines Unternehmens eingesetzt. Im Grunde lassen sich sämtliche webbasierten Anwendungen auch über mobile Endgeräte und Mobilfunknetzwerke ausführen. Die innerbetriebliche Nutzung mobiler Systeme hat ein hohes Innovationspotenzial und kann bisherige Geschäftsprozesse grundlegend verändern. Einen Teilbereich stellen Anwendungen für Business to Employee (B2E) dar. Hierzu zählen mobile Anwendungen für Mitarbeiter. Beispielsweise können Arbeitszeiten oder Reisekosten direkt per Smartphone erfasst werden. Ferner können potenzielle Mitarbeiter und Bewerber mobile Jobangebote von Unternehmen erhalten.

Machine to Machine (M2M)

Ohne direktes Eingreifen des Menschen können Maschinen über Funktechnologie miteinander kommunizieren. Ein Beispiel hierfür sind Parkscheinautomaten, die mit Mobilfunkmodulen ausgestattet sind. Soweit eine Stromversorgung (z. B. Solarzelle) existiert,

ist der Automat autonom in der Lage, Störfälle aller Art an einen zentralen Server zu melden. Falls kein Papier für den Ticketdruck mehr vorhanden ist oder der Münzbehälter voll ist, kann so gezielt ein Servicemitarbeiter Abhilfe schaffen. Somit entfallen die regelmäßigen, häufig jedoch überflüssigen Wartungstouren.

1.3 Mobilfunk

Mobilfunk wird als Sammelbegriff für eine Vielzahl unterschiedlicher Technologien zur Übertragung von Sprache und Daten verwendet. Die erforderlichen Endgeräte werden *ortsveränderlich* (mobil) eingesetzt. Demnach zählen auch Polizei-, Taxi- und Seefunk zum Mobilfunk. Im Regelfall steht der Begriff Mobilfunk jedoch für die öffentlichen Mobilfunknetze, die in Deutschland von den Unternehmen Vodafone, T-Mobile, Telefónica-O2 und zukünftig auch von 1&1 betrieben werden. In den späteren Kapiteln dieses Buches erfolgt eine detaillierte Darstellung der technologischen und konzeptionellen Ausgestaltung moderner Mobilfunknetzwerke, im Folgenden soll lediglich die Grundidee dargestellt werden.

Das *Mobilfunknetz* besteht aus dem Zugangsnetz und dem Kern-Netz. Das Kern-Netz übernimmt leitungsgebunden die Übertragung und Vermittlung von Sprache und Daten zwischen den ortsfesten Sendestationen des Mobilfunknetzes und zu anderen Kommunikationsnetzen. Das Zugangsnetz ist verantwortlich für die Kommunikation von seinen ortsfesten Mobilfunkantennen zu den mobilen Endgeräten. Die Schnittstelle zwischen der Mobilfunkantenne und dem Gerät wird im Allgemeinen *Luftschnittstelle* oder *Funkschnittstelle* genannt.

Der Datentransport in einem Mobilfunknetz erfolgt somit im Gegensatz zu seinem Namen weitgehend über leitungsgebundene Übertragungswege, zumeist als Kupfer- oder Glasfaserkabel, oder durch stationäre Richtfunkstrecken.

Moderne mobile Zugangsnetze sind als zellulare Funknetze aufgebaut. Ein Grundgerüst von hexagonalen, nebeneinanderliegenden Waben bildet die Grundstruktur. Im Zentrum jeder Wabe befindet sich eine Basisstation (Send- und Empfangsstation), die die Fläche der Wabe mit Funksignalen versorgt. Basisstationen sind aus funktechnischen Gründen in der Höhe angebracht, häufig auf Türmen, im städtischen Umfeld aber auch an oder auf hohen Gebäuden. Eine Basisstation ist in der Regel mit mehreren Antennen ausgerüstet, von denen jede einen Sektor der Wabe (als *Funkzelle*) versorgt. Die Waben und Funkzellen überlappen sich, um eine möglichst lückenlose Abdeckung zu gewährleisten.

Der Nutzer eines Mobilfunkdienstes ist nicht an eine Funkzelle gebunden. Bewegt er sich über den Sendebereich einer Antenne hinaus, leitet das Mobilfunknetz einen Handover (Übergabe) an eine günstiger gelegene Nachbarzelle ein. Dabei wird im gemeinsamen Sendebereich der benachbarten Funkzellen eine parallele Verbindung zur zweiten Basisstation aufgebaut und im passenden Augenblick umgeschaltet. Das Grundprinzip des Mobilfunknetzes verdeutlicht Abb. 1.1.

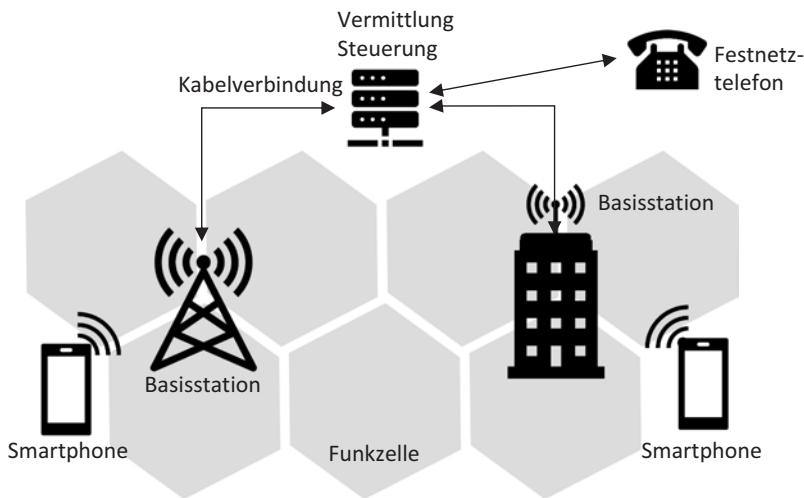


Abb. 1.1 Mobilfunknetz

1.4 Treiber im Mobile Business

Die Gründe für das enorme Wachstum und den großen Erfolg des Mobilfunks und seiner Anwendungen sind vielfältiger Natur. Fokussiert auf den Nutzer der Dienste und Technologien sind insbesondere folgende Treiber zu nennen, auf die nachfolgend näher eingegangen wird:

- Mobile Breitbandzugänge
- Smartphones und Tablets
- Tarifstrukturen
- Mobile Apps und Mobile Games
- Steigende Mediennutzung
- Vernetzung von Geräten (Maschine-zu-Maschine-Kommunikation, Internet der Dinge)

1.4.1 Mobile Breitbandzugänge

Ein *Breitbandzugang* (Breitbandanschluss) ist ein Zugang zum Internet mit hohen Datenübertragungsraten. Mobile Breitbandzugänge ermöglichen den drahtlosen schnellen Zugriff auf das Internet über mobile Endgeräte. Es werden hohe Datenübertragungsraten benötigt, um mobil beispielsweise Streaming-Angebote oder Videokonferenzen zu nutzen. Von mobilen Breitbandzugängen wird erst seit der vierten Mobilfunkgeneration (LTE) mit einer Downloadgeschwindigkeit von mindestens 50 Mbit/s gesprochen. In den

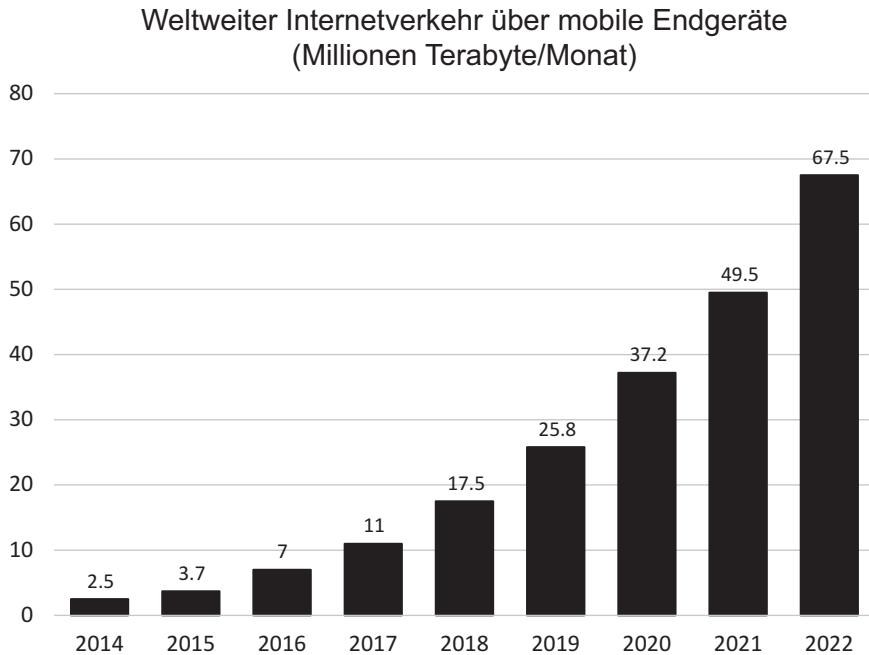


Abb. 1.2 Wachstum des Datenvolumens im mobilen Internet (Ericsson 2021)

vergangenen Jahren ist der mobile Datenverkehr stark angestiegen, dieser Trend wird auch für die Zukunft erwartet (Abb. 1.2). Besonders dynamisch verläuft die Entwicklung im Pazifischen Raum und in Nord-Amerika. In Asien wird das Wachstum vor allem durch die Zunahme der Nutzer und Endgeräte getrieben, während in Nord-Amerika das pro Endgerät generierte Datenvolumen stark wächst.

1.4.2 Smartphones und Tablets

Smartphones sind mobile Endgeräte, die mit zahlreichen Zusatzfunktionen und Kommunikationsmöglichkeiten ausgestattet sind. Im Vergleich zum Mobiltelefon (umgangssprachlich Handy) verfügen Smartphones neben den Telefonfunktionen u. a. über Kamera, Kalender, Browser, Sensoren, Bluetooth, WLAN und GPS-Verbindung. Smartphones sind die mit Abstand meist genutzten mobilen Endgeräte weltweit. Die ersten Smartphones erschienen ab dem Jahr 2000 auf dem Markt. Die damaligen Technologieführer unter den Endgeräteherstellern waren die Unternehmen Nokia, Palm und BlackBerry, die heute in diesem Bereich keine Bedeutung mehr haben. Nach der Vorstellung des Apple iPhone im Jahr 2007 drängten zahlreiche neue Anbieter mit vergleichbaren Endgeräten auf den Markt. *Tablets* sind besonders leichte, flache Computer mit Touchscreen und ohne mechanische Tastatur.

1.4.3 Tarifstrukturen

Im Mobilfunk dominierte anfangs die Sprachtelefonie. Kunden waren nahezu ausschließlich Geschäftsleute. Die Endgeräte waren teuer und wurden von den Netzbetreibern vermietet. Die Abrechnung erfolgte nach Gesprächsminuten. Mit der Einführung der digitalen Mobilfunktechnik in Deutschland ab 1990 wurde mobile Telefonie massenmarktauglich. Mit der privaten Nachfrage nach Mobiltelefonen in den 1990er- und 2000er-Jahren sanken auch Anschlussgebühren und Minutenpreise. Ab ca. 2005 ersetzte speziell bei jungen Menschen das Mobiltelefon häufig den leitungsgebundenen Telefonanschluss.

Mobile Datenkommunikation wurde durch die Digitaltechnik ermöglicht. Allerdings bestand auch hier die Zielgruppe zunächst aus Geschäftskunden. Es wurde zu prohibitiven Preisen nach Datenvolumen abgerechnet. Die Mobilfunknetzbetreiber waren seinerzeit überzeugt, dass mobile Datenübertragung nur von Geschäftsreisenden benötigt wird.

Getrieben von der Entwicklung im Festnetz („DSL Flatrates“) und der Dynamik des Marktes kam es schließlich zur Einführung von Inklusiv-Paketen, die außer einem Datenvolumen auch noch eine Anzahl von Gesprächsminuten und Kurznachrichten enthalten. Bei Überschreiten der Inklusiv-Volumina erfolgt dann in der Regel eine volumen- bzw. minutenbasierte Abrechnung zu höheren Gebühren oder eine Drosselung der Datenübertragungsrate.

Aufgrund des Wettbewerbs im (regulierten) Telekommunikationsmarkt sind die Kosten je Verbindungseinheit bzw. je genutztem Megabyte an Datenverkehr für Endverbraucher in den vergangenen Jahren deutlich gesunken. Dies gilt – aufgrund des Verbots von Roaming-Gebühren im EU-Ausland – auch für die Sprachtelefonie in ausländischen Netzen bzw. aus ausländischen Netzen in deutsche Netze. Roaming bedeutet, dass ein Nutzer in fremden Netzen sein mobiles Endgerät nutzen kann.

Mit dem aufkommenden Internet der Dinge entstand auch eine starke Nachfrage nach mobilen Maschine-zu-Maschine Endgeräten, wofür spezielle Tarife entwickelt wurden. Wegen des oft extrem geringen Datenvolumens dieser Geräte wird hier vor allem über Grund- und Anschlussgebühren abgerechnet. Es gibt aber bereits erste M2M-Tarifmodelle, die lediglich das geringe verbrauchte Datenvolumen abrechnen.

1.4.4 Mobile Apps und Mobile Games

Smartphones und Tablets bieten die Möglichkeit, die Grundfunktionalität des Endgeräts durch zusätzlich zu installierende Software – mobile Applikationen, kurz Apps – zu erweitern. Ausgehend von einfachsten Anwendungen wie beispielsweise digitalen Notizzetteln hat sich ein breites Angebot an Software für mobile Endgeräte entwickelt. Dieses geht mittlerweile sogar bis in die Einbindung von ERP-, CRM- oder Business Intelligence-Lösungen für Unternehmen. Die Abbildung dieser Funktionalitäten auf mobilen Endgeräten hat den Druck auf Softwareentwickler steigen lassen, bisherige Desktop-basierte Lösungen auch auf mobilen Endgeräten anzubieten. So lässt sich eine Konvergenz zwi-

schen Desktop-Lösungen und mobilen Apps feststellen, die insbesondere aufgrund der Einbindung von Cloud-Diensten (z. B. zur Datensynchronisierung) verstärkt wird.

Viele Apps sind kostenlos für die Nutzer, sie werden über Werbung finanziert. Apps mit In-App-Käufen werden zunächst ebenfalls kostenlos heruntergeladen, später müssen jedoch bestimmte Zusatzfunktionen oder Verbesserungen vom Nutzer bezahlt werden. Als dritte und kleinste Gruppe gibt es Apps, die von vornherein kostenpflichtig sind.

Ein besonders dynamischer Markt zeigt sich im Bereich der Mobile Games, die ebenfalls als Apps auf den mobilen Endgeräten sehr umfassend genutzt werden. Die steigende Leistungsfähigkeit der Smartphone-Hardware (Rechenleistung, Grafikchips, hochauflösende Displays) trägt dazu bei, dass die Nutzung von Mobile Games ein wesentlicher Treiber für die Entwicklung des Mobile Business ist.

1.4.5 Steigende Mediennutzung

Vor allem bei Menschen unter 30 Jahren hat sich die Mediennutzung stark in Richtung von Internetangeboten verschoben. Ein erheblicher Teil der deutschen Bevölkerung greift mittlerweile auf das mobile Internet zu. Die öffentliche Diskussion über dieses Phänomen wurde durch den Begriff „Digital Natives“ geprägt. Dieser Begriff vermittelt die Bedeutung von Medieninnovationen im Lebensalltag der jungen Generation, die im digitalen Zeitalter aufgewachsen ist. Bei Betrachtung der Ausstattung mit mobilen Endgeräten kann festgestellt werden, dass diese über alle Altersgruppen hinweg gestiegen ist. Gerade für Kinder und Jugendliche sind Smartphones zu einem unverzichtbaren Bestandteil ihres Alltags geworden. Über alle Altersgruppen und Weltregionen hinweg machen Videoinhalte bereits den größten Teil des mobilen Internet-Verkehrs aus. Abb. 1.3 zeigt, dass im welt-

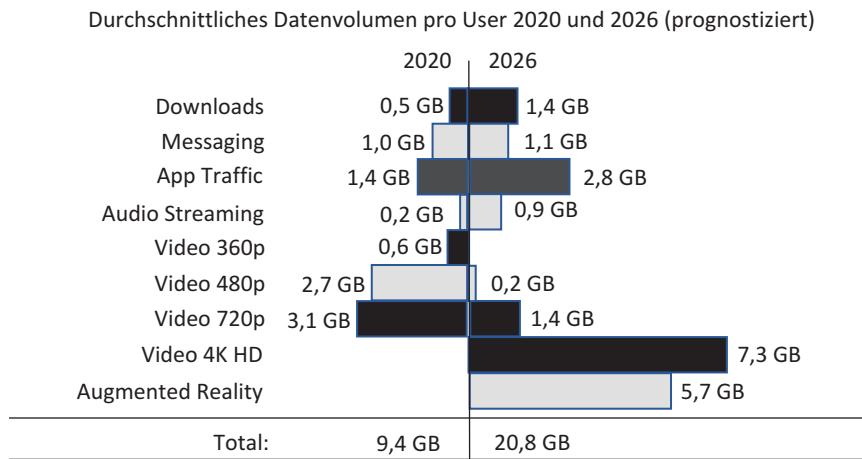


Abb. 1.3 Mobiler Datenverbrauch pro Nutzer und Monat im weltweiten Durchschnitt 2020 und als Projektion auf das Jahr 2026 (Ericsson 2021)

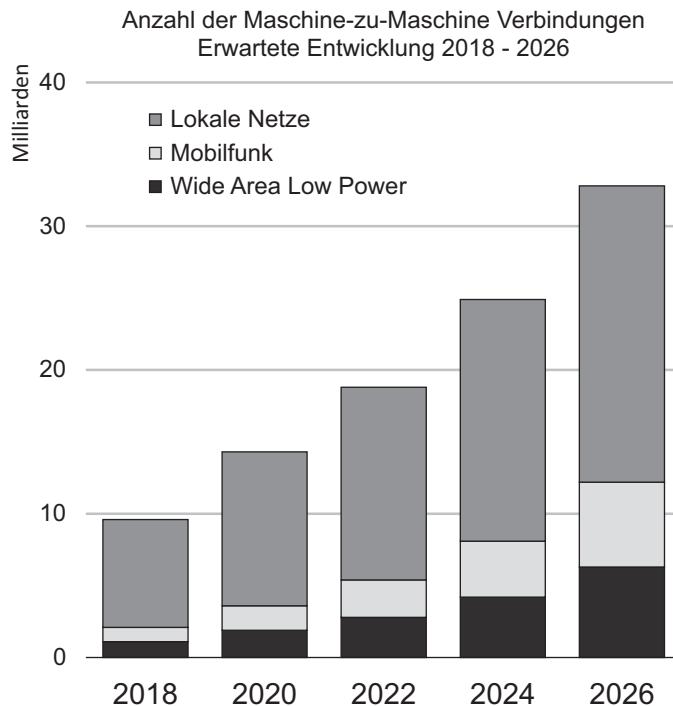


Abb. 1.4 Anzahl der Endgeräte in der Entwicklung des mobilen Internet der Dinge (Ericsson 2021)

weiten Durchschnitt bereits im Jahr 2020 Videoinhalte 68 % des gesamten mobilen Datenverbrauchs ausmachten. Bis 2026 wird sich dieser Anteil noch weiter erhöhen, während sich gleichzeitig das Gesamtvolumen mehr als verdoppeln wird.

1.4.6 Maschine-zu-Maschine-Kommunikation und Internet der Dinge

Mit dem „Internet der Dinge“ nahm auch das Bedürfnis zu, Sensoren, Aktoren, Messgeräte und Maschinen drahtlos untereinander zu vernetzen. „Jedes Objekt, das von einer Netzanbindung profitiert, wird mit dem Netz verbunden sein“ (Vestberg 2017). Bereits heute gibt es Milliarden von vernetzten Geräten. Bei größeren Entfernungen erfolgt die Anbindung über Mobilfunknetze (Kap. 4) oder über speziell errichtete Low Power Wide Area Networks (Kap. 5). Abb. 1.4 zeigt die mengenmäßige Aufteilung und die prognostizierte Entwicklung in den kommenden Jahren.

1.5 Geschichte der Mobilkommunikation

1.5.1 Die Anfänge

Kommunikation ist ein essentieller Bestandteil des menschlichen Lebens und Voraussetzung für die Entwicklung von Sozialstrukturen, Gesellschaften und Staaten. Im Lauf der Geschichte wurden Menschen mobiler und ihr Wirkungsradius wurde immer größer. Entsprechend entwickelte sich die Technik weiter: Sie ermöglichte Kommunikation über stetig wachsende Entfernung hinweg unabhängig vom Aufenthaltsort der Menschen.

Technische Hilfsmittel zur Kommunikation über große Entfernung werden schon lange genutzt. So wurde bereits vor Jahrhunderten *Licht* zur Kommunikation eingesetzt. Mittels Spiegel und Glasscherben wurden Lichtsignale gebildet durch das Umlenken von Sonnenstrahlen. Ein vorab generiertes Regelwerk – heute wird von einem Code gesprochen – über die Folge und Dauer der Lichtsignale ermöglichte so eine Kommunikation. Technisch ist dies als Amplitudenmodulation (Abschn. 3.3.1) zu bezeichnen, denn nichts anderes als eine Veränderung der Stärke des Signals erfolgt in diesem Beispiel: Der Lichtstrahl wird in eine bestimmte Richtung gelenkt oder abgeschaltet. Nicht nur aus alten Wildwest-Filmen ist die Kommunikation durch *Rauchsignale* bekannt. Sie wurde schon im antiken Griechenland genutzt (Schiller 2003, S. 25): Der griechische Dichter Aischylos beschrieb in seinem Drama Agamemnon, wie die Nachricht vom Sieg der Griechen über Troja im Jahre 1184 v. Chr. mit einer Feuerzeichenkette von Troja in das 555 km entfernte Argos gelangte. Der Historiker Thukydides berichtete über den Einsatz von Feuersignalen im Peloponnesischen Krieg (431-404 vor unserer Zeitrechnung). Aus China ist bekannt, dass Lichtsignale über eine Reihe von Signaltürmen weitergegeben wurden und hierdurch Nachrichten aus den Provinzen in die Hauptstadt übertragen werden konnten. In der Seefahrt war die Übermittlung von Informationen über *Flaggensignale* die einzige mögliche Kommunikationsform. So konnten anhand unterschiedlicher Flaggen bestimmte Codewörter übertragen werden – was technisch heutzutage über die Amplituden- und Frequenzmodulation erreicht wird (Abschn. 3.3.1). Eine Ergänzung erfolgte dann über die Flaggenbewegung (Schwenken), wodurch die Menge an übertragbaren Informationen gesteigert werden konnte. Auch heutzutage werden Flaggensignale z. B. in der Marine genutzt, um bei einem Ausfall technischer Systeme dennoch eine Kommunikationsmöglichkeit beizubehalten. Bei allen hier beschriebenen Systemen gilt, dass nur vorab im Regelwerk vereinbarte Informationen übertragen werden konnten. Der Code für die Übertragung war also vergleichsweise beschränkt.

1.5.2 Optische Telegrafien

Eine drahtlose Kommunikation über große Entfernung hinweg wurde mit dem optischen Telegrafie ermöglicht. Basis seiner Erfindung war wiederum die Entwicklung des Fernrohrs, mit der die Reichweite des menschlichen Auges erheblich erweitert wurde. Der

Abb. 1.5 Modell eines optischen Telegrafen
(Deutsches Technikmuseum, Berlin)



optische Telegraf wurde fast ein Jahrhundert als Standardkommunikationsmittel für die Überbrückung großer Entfernung eingesetzt. Er basiert auf der Zeichenübermittlung mit Hilfe von schwenkbaren Signalarmen – daher stammen die alternativen Bezeichnungen „Flügeltelegraph“ oder „Semaphor“ (Abb. 1.5). An einer gut sichtbaren Stelle wird ein Mast positioniert, an dessen oberen Ende schwenkbare Querbalken mit weiteren schwenkbaren Balken an jedem Ende angebracht sind. Anhand unterschiedlicher Ausrichtungen dieser Balken und eines festgelegten Codes können unterschiedliche Buchstaben übertragen werden.

1794 wurde eine erste Telegrafenlinie zwischen Paris und Lille eingerichtet, welche mit 22 Stationen 270 km überbrückte. Die Laufzeit für die Übertragung eines einzelnen Buchstabens lag bei beeindruckenden zwei Minuten. Jeder der beiden Signalarme konnte sieben verschiedene Stellungen einnehmen, die Querbalken zusätzlich noch jeweils zwei, dies ergaben insgesamt 196 darstellbare Zeichen (Abb. 1.6). Gerade die Flexibilität des Systems und die Geschwindigkeit der Datenübertragung überzeugten das Militär von den Vorteilen eines landesweiten, optisch-mechanischen Telegrafennetzes.

Napoléon Bonaparte verwendete die optische Telegrafie und ermöglichte damit eine bessere Kommunikation zwischen den verschiedenen Truppenteilen. Den Nachteil, dass die Signalmasten durch jeden einsehbar waren und die Nachrichten somit prinzipiell auch

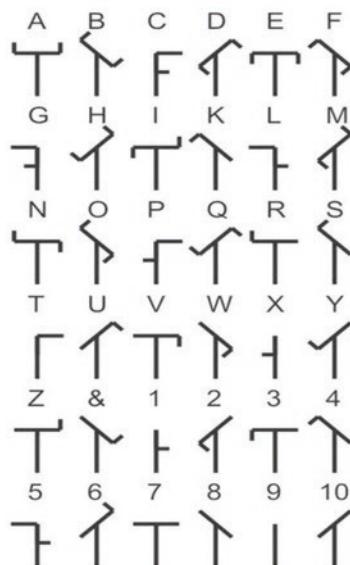


Abb. 1.6 Optischer Telegraf und Beispiel für die Codierung von Buchstaben und Ziffern (<https://shannonselin.com/2020/05/chappe-semaphore-telegraph/> (Linke Seite der Abbildung) und <https://www.podkst.de/chappe-code-2-gross/> (Rechte Seite der Abbildung))

von Unbefugten erkannt werden konnten, führte zur Verwendung von Geheimcodes. Aus diesen Anfängen entwickelte sich in Frankreich ein flächendeckendes Telegrafennetz. Eine erste optische Telegrafenlinie, die auch über deutsches Gebiet führte, war die Verbindung zwischen Metz und Mainz im Jahr 1813. Erst 1830, folgte eine weitere Verbindung zwischen Berlin und Potsdam. Der spätere Ausbau erfolgte unter Leitung von Franz August O'Etzel (1783–1850) und Carl Philipp Heinrich Pistor (1778–1847). Zwischen 1832 und 1852 bestanden Verbindungen auf einer Länge von fast 550 km. In dieser Zeit wurde der preußische Balkentelegraf mit einem Mastbaum und daran montierten sechs Flügeln eingesetzt. Mit insgesamt 4096 Flügelstellungen existierte ein komplexes Übermittlungssystem. Die in der späteren Zeit aufgebaute optische Telegrafenlinie zwischen Hamburg und Bremen war das erste deutsche, öffentlich zugängliche Kommunikationsmedium seiner Art, begründet und genutzt von Kaufleuten.

Die bis hierher verwendeten Telegrafen waren in ihrem Kern optisch-mechanischer Natur. Ab den 1830er-Jahren entwickelte sich eine andere Technologie rapide weiter, die Morsetelegrafie. Sie ermöglichte eine schnellere Datenübertragung und eine höhere Symbolrate (Kap. 2). Hinzu kam, dass die Technologie einfacher und kostengünstiger umzusetzen war und eine niedrigere Störanfälligkeit (Wetter, Tag/Nacht) aufwies. Ab Mitte der 1850er-Jahre wurde die optische Telegrafie weitestgehend eingestellt. Die optische Telegrafie bildete dennoch einen wichtigen Meilenstein in der Entwicklung der Telekommunikation, mit ihr konnten räumliche Distanzen in sehr kurzer Zeit überwunden werden.

1.5.3 Mobilkommunikation auf Basis elektromagnetischer Wellen

Die Entdeckung des *Elektromagnetismus* war für die Entwicklung der Mobilkommunikation in der heutigen Form entscheidend. Michael Faraday (1791–1867) entdeckte 1831 die elektromagnetische Induktion, die seitdem die Grundlage nahezu aller Kommunikationstechnologien bildet. Faraday konnte experimentell zeigen, dass ein stromdurchflossener metallischer Leiter ein Magnetfeld erzeugt und dass in einem Metalldraht, der durch ein Magnetfeld bewegt wird, ein elektrischer Strom „induziert“ wird. Joseph Henry (1797–1878) entwickelte die Entdeckung weiter, indem er die elektrischen Leiter zu Spulen wickelte und mit metallischen Kernen ausstattete. Er war damit in der Lage, elektrische Signale über Entfernung zu senden. Die publikumswirksame öffentliche Erstaufführung der Technologie gelang aber Samuel Morse (1791–1872), der ab 1837 die elektrische Telegrafie auf der Basis der Arbeiten von Faraday und Henry entwickelte und im Jahr 1844 eine Telegrafenverbindung von Washington nach Baltimore bauen ließ. Mit dem von ihm entwickelten Morse-Alphabet demonstrierte er, dass tatsächlich Textnachrichten über große Entfernung übermittelt werden konnten. Es folgte ein schneller Ausbau der Telegrafen-Fernverbindungen. Innerhalb eines Jahrzehnts waren Telegrafen-Leitungen von Küste zu Küste und zwischen allen großen Städten der USA installiert.

James C. Maxwell (1831–1879) trug maßgeblich zur Weiterentwicklung des Elektromagnetismus bei. Er erkannte, dass sich das Licht und alle anderen elektromagnetischen Wellen mit einer Geschwindigkeit von 300.000 km/s (im Vakuum) fortpflanzen und legte die theoretischen Grundlagen für die stürmische Entwicklung der Elektrotechnik. Heinrich Hertz (1857–1894) gelang 1888 – in einem Hörsaal der Universität Karlsruhe – der experimentelle Nachweis der von der Maxwell-Theorie vorhergesagten Wellen.

Guglielmo Marconi (1874–1937) arbeitete parallel und teilweise in Konkurrenz zu Heinrich Hertz. Er entdeckte unter anderem die Infrarot-Strahlung und Radio-Wellen und demonstrierte bereits 1895 die drahtlose Telegrafie. Dazu nutzte er Langwellen, welche mit einer sehr hohen Sendeleistung von einer Antenne abgestrahlt wurden. 1901 konnte damit erstmals eine transatlantische Übertragung durchgeführt werden, die schon 1907 in eine kommerziell genutzte ständige Transatlantikverbindung überführt wurde (Abb. 1.7). Die genutzten Antennen als Sende- und Empfangseinrichtungen mussten ihrem Zweck entsprechend groß sein (100 m Höhe) und geeignet positioniert werden (je Seite bis zu 30 Antennen)

Die Verwendung elektromagnetischer Wellen für die Kommunikation basiert auf der Nutzung bestimmter Frequenzen. Schon zur damaligen Zeit wurde deutlich, dass die Nutzung von Frequenzbereichen (bzw. Frequenzbändern) in einer zentral geregelten Form erfolgen muss, da sich ansonsten Signale überlagern und es somit zu Störungen der Signalübertragungen kommen kann. Auch Landesgrenzen werden von elektromagnetischen Wellen nicht respektiert. In drei Funktelegrafie-Konferenzen (1903, 1906 in Berlin und 1912 in London) wurde daher über die Verwendung von Funkfrequenzen im internationalen Rahmen verhandelt. Auf der zweiten Konferenz wurde in Berlin ein erster internationaler Vertrag hierüber abgeschlossen. Heute finden diese Konferenzen unter der

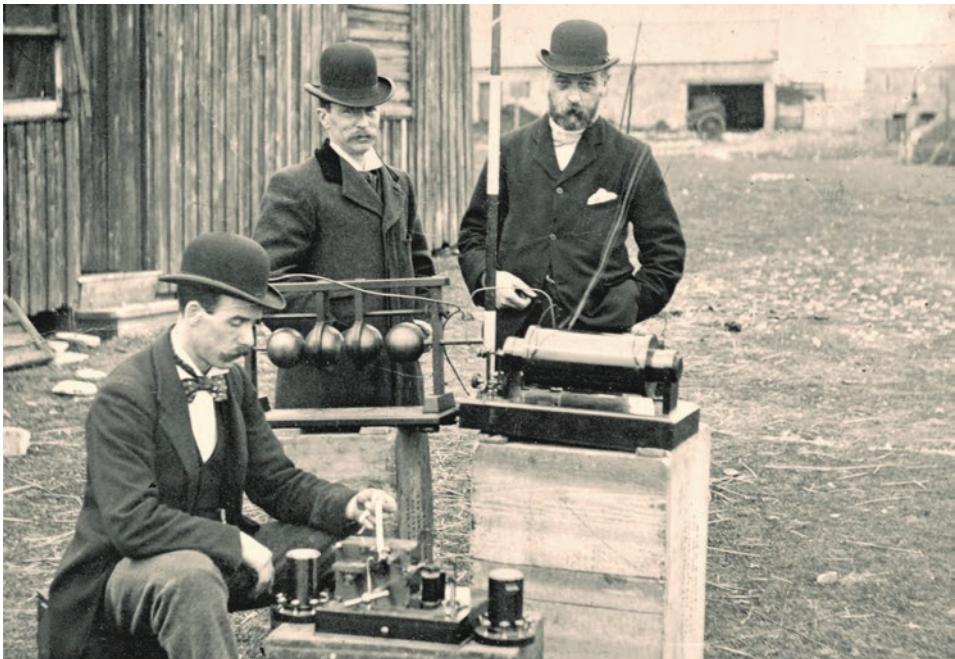


Abb. 1.7 Ingenieure des British Post Office inspizieren Guglielmo Marconis Ausrüstung für drahtlose Telegrafie während einer Vorführung auf der Insel Flat Holm am 13. Mai 1897 (<https://commons.wikimedia.org/w/index.php?curid=4012156> (CC BY 3.0 <https://creativecommons.org/licenses/by/3.0/> Nutzer: TR001))

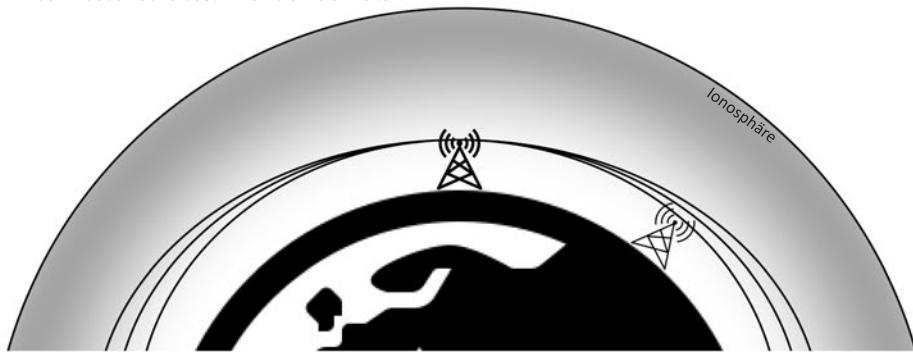
Bezeichnung World Radio Conference (WRC) regelmäßig auf Einladung der Radio-Sektion der International Telecommunication Union (ITU-R) unter Mandat der Vereinten Nationen (UN) statt.

Auch die Ausstrahlung von Radiosendungen erfolgt über elektromagnetische Wellen. Die erste Radiosendung zu Weihnachten 1906 setzte sich aus Sprach- und Musikbeiträgen zusammen. Im Jahr 1915 wurde die erste drahtlose Kommunikationsverbindung innerhalb der USA zwischen New York und San Francisco in Betrieb genommen. 1920 folgte der Aufbau einer ersten kommerziellen Radiostation, KDKA Pittsburgh. Bis zu diesem Zeitpunkt basierte die Übertragung immer noch auf Langwellen.

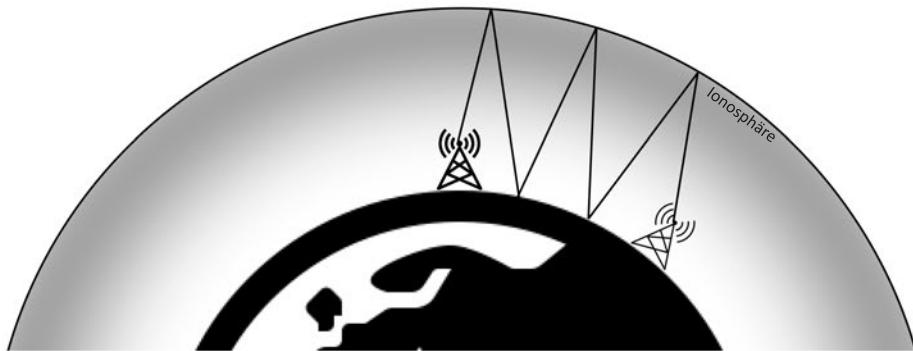
Erneut war es Marconi, der 1920 die Übertragung mittels Kurzwellen entdeckte. Diese besitzen den entscheidenden Vorteil, dass für deren Übertragung kürzere Antennen benötigt werden und eine niedrigere Sendeleistung notwendig ist. Diese Aspekte hatten grundlegenden Einfluss auf die Entwicklung der mobilen Kommunikation. Die Übertragung „rund um die Welt“ wurde erst mittels dieser Entdeckung möglich, denn nur Kurzwellen werden an der Ionosphäre und an der Erdoberfläche reflektiert und ermöglichen so eine völlig andere Anordnung der Sende- und Empfangseinheiten. Abb. 1.8 verdeutlicht die unterschiedlichen Ausbreitungswege der elektromagnetischen Wellen verschiedener

Langwellen

Die Ausbreitung erfolgt über eine Bodenwelle, der Erdkrümmung folgend. Die Frequenz und die Beschaffenheit der Erdoberfläche bestimmen die Reichweite.

**Kurzwellen**

Die Ausbreitung erfolgt über Reflexion an der Ionosphäre und der Erdoberfläche. Deren Reflexionseigenschaften bestimmen die Reichweite.

**Ultrakurzwellen**

Die Ausbreitung erfolgt ähnlich wie bei Lichtwellen. Mit steigender Frequenz steigt die Bedeutung der Sichtverbindung zwischen Sender und Empfänger.

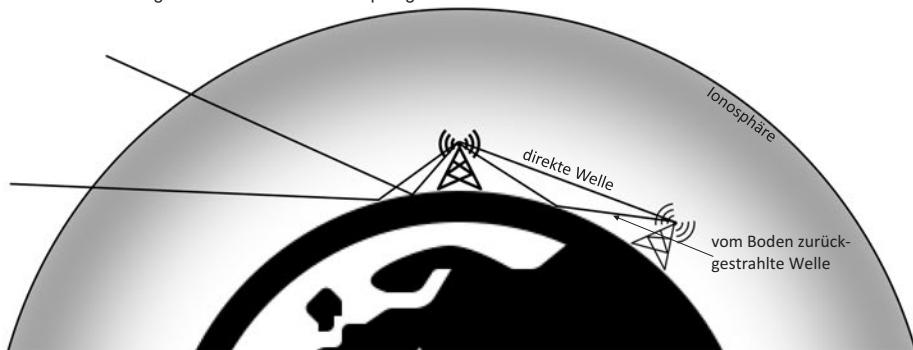


Abb. 1.8 Ausbreitungswege elektromagnetischer Wellen verschiedener Frequenzbereiche

Abb. 1.9 Philco Transitone, das erste kommerziell erhältliche Autoradio (<https://philcoradio.com/phorum/archive/index.php?thread-5987.html>)



Frequenzbereiche. Diese werden in Kap. 2 weitergehend erläutert. Der Einsatz von Anfang der 1900er-Jahre erfundenen Vakuumröhren in den Sendern und Empfängern zur Verstärkung der Signale war ein weiterer Baustein dieser Entwicklung.

Ein erstes wirklich mobiles Endgerät war die Installation eines Senders an Bord eines Zeppelins im Jahr 1911. Auch das Autoradio ist ein mobiles Endgerät zum Empfang von Daten mittels elektromagnetischer Wellen. Das erste kommerziell verfügbare Modell eines Autoradios war das Philco Transitone aus dem Jahr 1927 (Abb. 1.9).

In den 1920er-Jahren folgten zahlreiche Versuche zur Übertragung von bewegten Bildern – die Geburtsstunde des Fernsehens. Unter anderem wurden Fernsehbilder über den Atlantik übertragen. Auch bewegte Bilder in Farbe wurden übertragen. In den USA war WGY die erste Sendestation, die regelmäßige Fernsehübertragungen inklusive einer Nachrichtensendung anbot. Die Übertragungsqualität der Sendungen war anfangs nach unseren heutigen Maßstäben allerdings schlecht.

1.5.4 Mobile Telefonie

Auf dem Grundprinzip der elektromagnetischen Übertragung gelang es Philipp Reis (1834–1874) im Jahr 1860 erstmals, das gesprochene Wort per Draht zu übertragen. Der Schotte Alexander Graham Bell (1847–1922) führte diese Arbeiten fort und zeigte seine Ergebnisse auf der Weltausstellung in Philadelphia. Weitere Erfinder waren zeitgleich auf diesem Feld tätig. Um Prioritäten und die Patentierung gab es Streitigkeiten und zahlreiche Prozesse; letztlich setzte sich Bell als Rechteinhaber durch. Der deutsche Generalpostmeister Heinrich von Stephan (1831–1897), setzte das Bell'sche Sprechgerät 1877 in Friedrichsberg, nahe Berlin, als Ersatz für den Morsetelegrafen auf einer Telegrafenleitung ein und stellte es für die öffentliche Nutzung zur Verfügung. Die (leitergebundene) Telefonie

entwickelte sich auf beiden Seiten des Atlantiks rasant. In den USA und kurz danach auch in den europäischen Staaten musste das Prinzip der Anrufbereiche und Vorwahlnummern eingeführt werden, um einen geordneten Fernsprechbetrieb zu ermöglichen. Schon 1915 – 40 Jahre nach dem ersten Telefonat von Graham Bell mit seinem Kollegen Thomas Watson (seinerzeit Präsident der International Bureau Machine Corporation – IBM) – wurde das Gespräch im Wortlaut wiederholt; diesmal aber über den Atlantik hinweg.

Mobile Telefonie entstand zunächst in Form von Zug-Telefonen. Das Unternehmen Telefunken führte seit 1906 Versuche mit Nachrichtenübertragung aus Zügen durch – zunächst noch unter Verwendung der Morse-Technik. Später experimentierte die neu gegründete *Gesellschaft für Funktelegrafie* in Berlin mit der Übermittlung von Sprachnachrichten aus fahrenden Zügen heraus. Nach Unterbrechung durch den Ersten Weltkrieg wurden diese Versuche unter Beteiligung der Reichspost neu aufgenommen. 1925 kam es zu einer regulären Zugtelefon-Lösung auf der Strecke Hamburg – Berlin durch die *Zugtelefonie AG* (später *Mitropa*), die das Recht hatte, auf weiteren Strecken des Deutschen Reiches diese Lösung exklusiv anzubieten. Die Verbindung mit dem Zug wurde über eine 192 m lange Antenne auf dem Dach des Zuges hergestellt. Das Gegenstück war ein entlang der gesamten Streckenlänge gespannter Sende- und Empfangsdraht. Die Vermittlung vom und zum Zug erfolgte manuell und war exklusiv an den Endpunkten der Strecke in Hamburg und Berlin möglich. Anrufer an anderen Orten mussten erst die Sendezentrale kontaktieren, die die Verbindung mit dem Teilnehmer im Zug herstellte.

In den 1940er-Jahren nahmen die Bell System Companies (später AT&T) in Teilen der USA Netze für Autotelefone in Betrieb. Entlang der Fahrstrecke wurden Basisstationen an Funkmasten aufgestellt (Abb. 1.10 – links). Der mobile Dienst war getrennt in ländliche

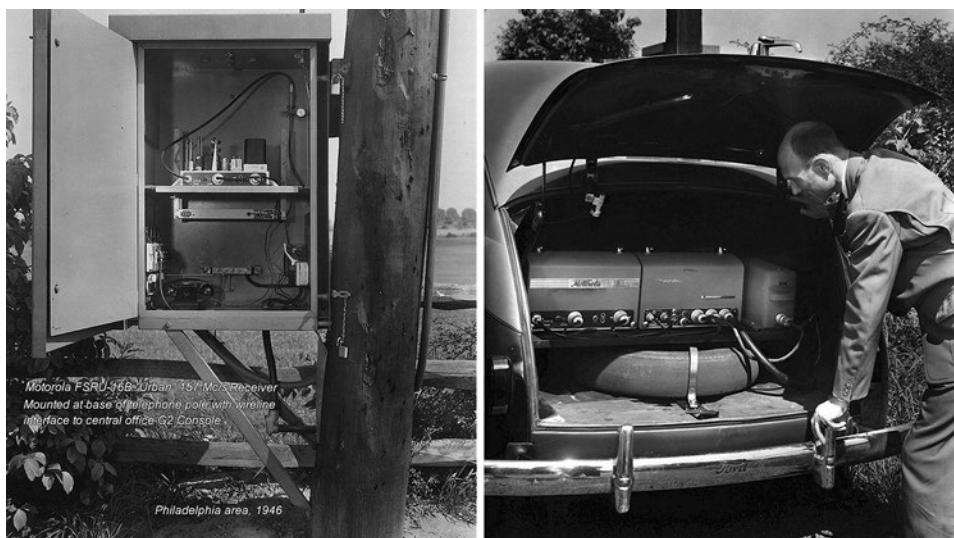


Abb. 1.10 Autotelefonie in den USA (<http://www.wb6nvh.com/MTSfiles/Carphone1.htm>)

und städtische Regionen. Dabei adressierten die ländlichen Netze in erster Linie das Transportgewerbe, während die Kunden für die städtischen Netze vor allem Taxifahrer, Ärzte und Journalisten waren. Die mobilen Telefone waren noch sehr sperrig, und füllten in der Regel den Kofferraum eines Pkw aus (Abb. 1.10- rechts). Die Funktechnik nutzte Frequenzen im Rundfunkbereich mit entsprechenden Reichweiten, so dass Funkzellen und Handover nicht nötig waren. Die Idee einer zellenartigen Netzstruktur mit Handover-Algorithmen kam zu dieser Zeit allerdings schon auf und wurde bereits 1947 an zwei Ingenieure der Bell Labs patentiert.

Funktelefone kamen als *öffentlicher beweglicher Landfunkdienst* (öBL – später als A-Netz bezeichnet) der Deutschen Bundespost ab 1958 nach Deutschland. Die Deutsche Bundespost hatte als staatliche Behörde das Monopol für Telekommunikations-Einrichtungen und für Funkverkehr. Ähnlich wie bei den amerikanischen Netzen wurde im Bereich der VHF Fernseh-Frequenzen von 156 bis 174 MHz von 136 Funktürmen gesendet. Wegen der großen Reichweite und geringen Teilnehmerzahl gab es keine Notwendigkeit einer Zellstruktur. Mobiltelefone bestanden aus einer Einheit zum Einbau in den Kofferraum sowie der Sprech-einrichtung und waren zum Einsatz in Fahrzeugen vorgesehen (Abb. 1.11). Aufgrund der Kosten richtete sich das A-Netz an eine kleine Gruppe von Entscheidungsträgern in Wirtschaft und Politik. Die Ausstattung kostete mit 10.000 bis 15.000 DM mehr als das Doppelte eines damaligen durchschnittlichen Jahresgehaltes, hinzu kamen Monatsgebühren von zunächst 66 DM und später bis zu 270 DM. Zu Spitzenzeiten hatte das A-Netz 11.000 Teilnehmer; bei seiner Abschaltung im Jahre 1977 waren es nur noch 800.

Unter der Vorwahl 010 wurde eine Hand-Vermittlungsstelle des A-Netzes erreicht, die zum mobilen Teilnehmer weiter verband. Seit dieser Zeit beginnen in Deutschland Mobilfunkrufnummern mit der Ziffernfolge 01. Der Anrufer musste dabei aber immer den Aufenthaltsbereich des mobilen Endgerätes kennen. Eine Übergabe der Verbindung zwischen



Abb. 1.11 A-Netz Telefon des Unternehmens TeKaDe, Nürnberg, zum Festeinbau im Auto (<http://www.oebL.de/A-Netz/Geraete/TeKaDe/B72/B72.html>)

verschiedenen Basisstationen war noch nicht möglich. Es war daher ratsam, während eines Telefonats den Standort nicht zu verändern.

Im Jahr 1972 startete das *B-Netz* in Deutschland. Es arbeitete im Frequenzband von 148 bis 154 MHz, und später, nach Abschaltung des A-Netzes, zusätzlich auf dessen Frequenzen. Die Kapazität betrug anfangs bis zu 16.000 Teilnehmer und wurde später auf bis zu 27.000 Teilnehmer wesentlich erweitert. Als wichtige Änderung war nun auch ein automatischer Verbindungsaufbau aus dem Festnetz zum mobilen Endgerät hin möglich. Allerdings musste ein Anrufer dazu den ungefähren Aufenthaltsort des mobilen Endgeräts kennen, damit die entsprechende Funkzelle angesprochen werden konnte. Statt der einheitlichen Vorwahl 010 des A-Netzes wurde jetzt die Ortsnetz-Vorwahl des betreffenden Bereichs gewählt (also z. B. 089 für München), anschließend die Ziffern 05, und dann die Teilnehmernummer. Die B-Netztechnologie wurde von der Deutschen Bundespost beim Nürnberger Unternehmen TE-KA-DE (später Philips Kommunikationsindustrie, inzwischen in Nokia aufgegangen) beauftragt, die bereits am A-Netz beteiligt war. Die B-Netztechnologie war in Deutschland, Österreich, den Niederlanden und Luxemburg verfügbar. Das Interesse der Postverwaltungen an der grenzübergreifenden Nutzung war trotz identischer Netztechnik auf beiden Seiten noch gering; teilweise wurde sie von den betroffenen Ländern sogar verboten.

Die Funkbereiche waren mit ca. 150 km größer als beim A-Netz; dabei hatte eine Funkzelle einen Durchmesser von bis zu 30 km. Es fand kein Handover von Funkzelle zu Funkzelle statt; bei Verlassen der Zelle wurde das Gespräch abgebrochen und musste neu aufgebaut werden – unter Umständen mit einer geänderten Vorwahl. Das B-Netz wurde in Deutschland und in Österreich im Jahre 1984 abgeschaltet. Abb. 1.12 zeigt ein B-Netz-



Abb. 1.12 B-Netz Zugtelefon „TE-KA-DE BSA31 Zugsekretariat“ (<http://gsm.alibaba.sk/B-Netz/Geraete/TeKaDe/BSA31S/BSA31Zug.htm>)

Gerät, welches von Zugsekretarien in Intercity-Zügen der Deutschen Bahn 1978 genutzt wurde. 1982 wurden die Zugsekretariate abgeschafft und durch mobile Münzfern sprecher ersetzt.

In den 1970er- und 1980er-Jahren entstand für die Telekommunikation ein internationaler Markt Platz. Vor allem in der Mobilkommunikation wurden Systeme und Netztechnologie immer seltener von den einheimischen Post- und Telekommunikationsverwaltungen selbst entwickelt, sondern auf dem Markt eingekauft. Die amerikanischen Hersteller, z. B. Motorola, waren die ersten, die auf dem Weltmarkt präsent waren. Das Motorola DynaTAC 8000X war 1983 das erste im Handel erhältliche Mobiltelefon (Abb. 1.13). Es wurde für den amerikanischen AMPS Standard (*Advanced Mobile Phone System*) entwickelt. Das von den Bell Labs und Motorola entwickelte AMPS und seine digitale Weiterentwicklung DAMPS waren in den 1980er- und 1990er-Jahren das in den USA vorherrschende Mobilfunksystem. Auch international war AMPS sehr erfolgreich. Für Europa wurde es unter dem Namen *Total Access Communication System* (TACS) an die unterschiedlichen Bedingungen und die zur Verfügung stehenden Frequenzen adaptiert. Im Vereinigten Königreich wurden zwei Mobilfunklizenzen vergeben. Beide Netze nutzten TACS als gemeinsamen Kommunikationsstandard.

Abb. 1.13 Motorola
DynaTAC 8000X mit British
Telecom Branding für den
TACS Standard (https://de.wikipedia.org/wiki/Motorola_DynaTAC#/media/Datei:DynaTAC8000X.jpg
(CC BY-SA 3.0, <https://creativecommons.org/licenses/by-sa/3.0/> Nutzer: Kozuch))



In Skandinavien entwickelten die Post- und Telekommunikationsverwaltungen von Schweden, Norwegen und Finnland gemeinsam mit den einheimischen Unternehmen Ericsson und Nokia einen offenen Standard unter der Bezeichnung NMT (Nordic Mobile Telephony). Die NMT-Netze wurden in Europa mit Ausnahme des Vereinigten Königreiches zum vorherrschenden Standard der 1980er-Jahre und ein weltweiter Erfolg. Letztlich wurde damit auch die jahrzehntelange Dominanz der beiden beteiligten skandinavischen Unternehmen im weltweiten Mobilfunkmarkt begründet. NMT war das erste zelluläre Mobilfunknetz und erlaubte durch digitale Vermittlungstechnik die einheitliche automatische Rufnummernwahl durch den Teilnehmer. Allerdings erfolgte die Sprachübertragung noch analog. Bei Zellwechsel erfolgte bereits ein automatischer Handover. Auch Roaming war ausdrücklich gewollt und wurde im Design vorgesehen. Der Begriff Roaming wurde von der NMT Entwicklergruppe geprägt. Für die Entwicklung eines multinationalen Mobilfunksystems waren auch die benötigten Frequenzen in den beteiligten Ländern zu identifizieren und zur Verfügung zu stellen. Bis heute stellt dies ein Hindernis in der Entwicklung dar: Praktisch jeder brauchbare Frequenzbereich wird bereits durch eine Organisation oder Technologie genutzt. NMT nutzte einen Frequenzbereich bei 450 MHz, der später um einen Bereich bei 900 MHz ergänzt wurde. Eine Kuriosität stellte die schwedische Lösung dar. In Schweden wurde der 450 MHz Bereich bereits durch eine militärische Anwendung genutzt, in die der Staat große Summen investiert hatte. Es erfolgte eine Einigung zwischen der Regierung und den Netzbetreibern, dass die Frequenzen in Friedenszeiten für den Mobilfunk zur Verfügung stehen sollten, im Krisen- oder Kriegsfall allerdings sofort an das Militär zurückfallen mussten.

Der offene Standard erlaubte unabhängigen Unternehmen, Netzausrüstung und Endgeräte herzustellen, so dass sich erstmals ein Herstellerwettbewerb entwickelte. Dies führte zum Beispiel zu kleineren und handlicheren Geräten, die zudem einfacher bedient werden konnten. Das weltweit erste NMT-Netz wurde 1981 durch Ericsson in Saudi-Arabien aufgebaut. In Europa folgten schnell hintereinander weitere 25 nationale Netze; NMT wurde auch in Asien genutzt. Schon 1981 gab es allein in Skandinavien 110.000 NMT-Teilnehmer.

In Deutschland wurde mit dem *C-Netz* ein Sonderweg gewählt. Eine Evaluierung des NMT als Nachfolger des B-Netzes durch die Deutsche Bundespost-Telekom war unbefriedigend ausgefallen. Zu den Kritikpunkten gehörten die fehlende Verschlüsselung der Gespräche und eine zu geringe Flexibilität für Geschäftskunden durch die in das Gerät fest einprogrammierte Telefon-Nummer. Siemens entwickelte im Auftrag der Telekom eine Mobilfunklösung, die auf den Erkenntnissen mit NMT aufbaute und weitgehend mit NMT vergleichbar, aber nicht kompatibel war. Das C-Netz war vor allem aufgrund seiner späteren Entwicklung und der Berücksichtigung von Erfahrungen mit vorhergehenden Systemen technologisch zu seiner Zeit das modernste Mobilfunknetz. Es ermöglichte zum Beispiel eine Datenübertragung per Modem mit 1 Kbit/s, was bei NMT noch nicht möglich war. Anstelle der versprochenen Verschlüsselung gab es allerdings nur eine sogenannte Verschleierung. Dies war eine Invertierung des Sprachbandes, die mit geringem technischem Aufwand rückgängig gemacht werden konnte. Zur Flexibilisierung der betrieb-



Abb. 1.14 Telekarte für das C-Netz (<http://www.oebi.de/C-Netz/Rest/Kartegelb1.JPG>)

lichen Nutzung wurde mit der Telekarte der Vorläufer der späteren SIM-Karte geschaffen (Abb. 1.14). Die Telekarte ermöglichte die von Geschäftskunden geforderte logische Trennung von Gerät und Nutzer. Die teuren Mobiltelefone konnten durch verschiedene Telekarten von verschiedenen Mitarbeitern unter eigenen Telefonnummern genutzt werden. Das C-Netz nahm Abschied von der einheitlichen Zellgröße, die in allen Systemen bis dahin befolgt wurde. Durch die Mischung großer und kleiner Funkzellen wurde eine flexible Reaktion auf regional unterschiedliche Kapazitätsanforderungen ermöglicht.

Das C-Netz ging ab 1985 in Betrieb. Die Teilnehmer waren unter ihrer eigenen einheitlichen, mit 0161 beginnenden Mobilfunk-Rufnummer aus allen Netzen durch Selbstwahl erreichbar. Im Jahr 1988 gab es ca. 100.000 C-Netz-Verträge, das waren weniger Teilnehmer als NMT bereits 7 Jahre zuvor allein in Skandinavien mit der halben Einwohnerzahl hatte. Die ursprünglich konzipierte Kapazität des C-Netzes war damit erschöpft. Durch den geheimen und proprietären Standard gab es keinen offenen Endgerätemarkt, was ein entscheidendes Hindernis für einen internationalen Erfolg darstellte. Das C-Netz blieb eine deutsche Insellösung. Neben Deutschland wurde es nur in Portugal und Südafrika eingeführt. Die Stunde des C-Netzes schlug mit der deutschen Wiedervereinigung 1989/1990. Der große Bedarf an Telefonanschlüssen in den Neuen Bundesländern konnte kurzfristig nur mit Mobilfunk befriedigt werden. Durch Kapazitätserweiterungen, wie der Verwendung von kleineren Mobilfunkzellen, konnten zusätzliche Teilnehmer aufgenommen werden. So wuchs die Teilnehmerzahl des C-Netzes schnell auf 850.000, womit die Kapazität endgültig erschöpft war. Nach 1990 verwendete die Telekom zusätzlich auch die NMT-Technik als Hausanschluss-Ersatz in den Neuen Bundesländern. Abb. 1.15 zeigt das Gerät „Porty“ von Philips exemplarisch für C-Netz-Telefone. Der Name steht für die gegenüber der A und B-Netz-Generation stark verkleinerten und „tragbaren“ Geräte, und war Namenspate für den späteren pseudo-englischen Begriff „Handy“ im deutschen Sprachraum.

Die positiven Erfahrungen mit dem NMT-450 Standard bewogen die skandinavischen Telekommunikations-Verwaltungen, der Europäischen Union die Entwicklung eines einheitlichen offenen digitalen zellulären Mobilfunkstandards der nächsten Generation vorzuschlagen. Dieser Vorschlag wurde 1982 von den EU Mitgliedern angenommen. Die

Abb. 1.15 C-Netz-Telefon
„PHILIPS porty Mobiltelefon
BSA51“ (<http://www.oebi.de/C-Netz/Geraete/Philips/BSA51/BSA51.html>)



Europäische Konferenz der Post- und Telekommunikationsverwaltungen (CEPT) richtete dafür eine Arbeitsgruppe unter der Bezeichnung GSM (Groupe Speciale Mobile) ein. Die GSM wurde 1989 in das neu gegründete European Telecommunication Studies Institute (ETSI) eingegliedert. Im Jahre 1990 wurde die Phase 1 des Standards, ein ca. 5000 Seiten umfassendes Dokument, von der ETSI verabschiedet und den verschiedenen Organisationen und Herstellern zur Implementierung zugeleitet. Mit dem Welterfolg GSM begann die aktuelle Periode der globalen offenen Mobilfunkstandards. Gleichzeitig ging die Zeit der staatlichen Monopole in der Telekommunikation zu Ende. Praktisch alle nationalen Regierungen legten den Aufbau und Betrieb von Mobilfunknetzen in die Hände von privaten Unternehmen. Die neuen, privatwirtschaftlich organisierten Netzbetreiber standen national und international in Konkurrenz und waren darauf angewiesen, neueste Technik und guten Service anzubieten. Der Mobilfunk war die Speerspitze der Deregulierung der Telekommunikationsdienste. Innerhalb eines Jahrzehnts hatte sich die Telekommunikation von einer Welt der eifersüchtig bewachten staatlichen Monopole zu einer Welt der Kommunikation ohne Grenzen verändert. Menschen konnten die ganze Welt bereisen und waren dabei praktisch überall an ihrem eigenen Mobiltelefon unter ihrer heimischen Telefonnummer erreichbar.

1.6 Fragen

- 1) Nennen Sie mindestens vier Charakteristika, die mobile Kommunikation von der Festnetzkommunikation in Bezug auf die kommerzielle Nutzung unterscheiden.
- 2) Welche Kategorien werden in der Systematik der Telekommunikationsdienste unterschieden?
- 3) Betrachten Sie das Chart zum Wachstum von mobilen Datendiensten in Abb. 1.2. In welchen Zeiträumen erfolgt näherungsweise eine Verdoppelung des Volumens?
- 4) Vergleichen Sie ein typisches Prepaid Tarifmodell mit den Tarifmerkmalen einer M2M Anwendung. Wo liegen die Unterschiede?
- 5) Wie funktioniert die drahtlose Kommunikation mittels eines optischen Telegrafen?
- 6) Welche Vorteile hat die Morsetelegrafie im Vergleich zur Verwendung von optischen Telegrafen?
- 7) Durch welche Entdeckung wurde erstmals die Übertragung von Signalen „rund um die Welt“ ermöglicht? Wie funktioniert dies?
- 8) Welches Mobilfunknetz ging in Deutschland zuerst an den Start und wo lagen die Einschränkungen?
- 9) Welchen wesentlichen Vorteil hatte das B-Netz gegenüber dem A-Netz?
- 10) Welche Netzgeneration ermöglichte als erste die automatische Wahl und den Handover von Funkzelle zu Funkzelle

Literatur

- Abts D, Mülder W (2017) Grundkurs Wirtschaftsinformatik, 9. Aufl. Springer, Wiesbaden. <https://doi.org/10.1007/978-3-658-16379-2>
- Bundesnetzagentur (2021) Teilnehmerentwicklung im Mobilfunk. Bonn. https://www.bundesnetzagentur.de/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Marktbeobachtung/Deutschland/Mobilfunkteilnehmer/Mobilfunkteilnehmer_node.html. Zugegriffen am 28.04.2021
- Eriesson (2021) Ericsson mobility report – June 2021. Stockholm. <https://www.ericsson.com/49f7c7/assets/local/mobility-report/documents/2021/june-2021-ericsson-mobility-report.pdf>. Zugegriffen am 24.04.2021
- Schiller J (2003) Mobilkommunikation, 2. Aufl. Pearson, München. 978-3-827-37060-0
- Vestberg H (2017) Up to speed. Verizon Podcast. USA: Verizon. https://www.verizon.com/about/sites/default/files/Up-to-speed-podcast-Hans-Vestberg-Transcript_0.pdf. Zugegriffen am 20.08.2021
- We are Social (2021) Global overview report. New York. <https://wearesocial.com/digital-2021/>. Zugegriffen am 28.04.2021.



Allgemeine Grundlagen des Mobilfunks

2

2.1 Einführung und Lernziele

Mobilfunknetze sind heute überall auf der Welt präsent und für praktisch jeden verfügbar. In Deutschland gibt es rund 151 Millionen Mobilfunkanschlüsse – das sind 60 % mehr als es Einwohner gibt (Bundesnetzagentur 2021). Gleiches gilt für praktisch alle Industrieländer, und sogar in den Entwicklungs- und Schwellenländern kann von einer Vollversorgung der Bevölkerung mit Mobilfunktechnologie gesprochen werden. Die elementaren Bedienaktionen am Endgerät und die entsprechenden Netz-Reaktionen können also hier also als bekannt vorausgesetzt werden.

Was nicht als bekannt vorausgesetzt werden kann, sind grundlegende Informationen über den Aufbau und die Funktionsweise eines Mobilfunknetzes. Dieses Kapitel stellt die wichtigsten Strukturen und Funktionen eines Mobilfunknetzes dar, ohne dabei Bezug auf einen konkreten Standard oder eine technische Implementation zu nehmen.

► Lernziele

- Sie verstehen die Struktur eines Mobilfunknetzes im Unterschied zu einem Festnetz.
- Sie verstehen, wie ein Teilnehmer bzw. sein Endgerät (z.B. Mobiltelefon) sein Netz identifiziert und sich anmeldet.
- Sie kennen die grundsätzlichen Abläufe beim Aufbau und der Durchführung von Verbindungen im Mobilfunknetz.
- Sie kennen die Mechanismen der beiden wichtigsten Mobilitätselemente, Handover (Übergabe) und Roaming, in der mobilen Kommunikation.

2.2 Systeme und Netze des Mobilfunks

Dieses Kapitel stellt die grundlegende Architektur eines modernen digitalen Mobilfunknetzes vor und erläutert die wichtigsten Funktionen und Prozeduren, sofern sie unabhängig von der jeweils verwendeten Funk-Technologie sind. Die Darstellung orientiert sich an den Funktionen der öffentlichen Mobilfunknetze, die weltweit genutzt werden. Die vielfältigen Funktionsweisen anderer Systeme zur drahtlosen Kommunikation werden in späteren Kapiteln angesprochen.

2.2.1 Mobilfunknetze und Festnetze

Ein Mobilfunknetz stellt dem Nutzer über sein *mobiles* Endgerät Sprach- und Datenkommunikationsdienste zur Verfügung. Bei den angebotenen Sprachdiensten handelt es sich sowohl bei mobilen als auch bei leitungsgebundenen Netzen um Telefon-Verbindungen mit anderen Teilnehmern; bei den Datendiensten sind es Text- und Multimedia-Nachrichten sowie ein allgemeiner Internet-Zugang.

In ihrer Grundfunktion erbringen Mobilfunknetze und leitungsgebundene Netze die gleichen Dienste für den Nutzer. Das spiegelt sich auch in ihrer grundsätzlichen Architektur. Beide Netztypen haben ein Kern-Netz, das die Dienste durch Vermittlung, Weiterleitung oder Speicherung von Sprache und Daten zur Verfügung stellt, sowie ein Zugangsnetz, durch das die Teilnehmer oder Nutzer mit dem Kern-Netz verbunden werden. Während die Kern-Netze zumindest vom Grundsatz her sehr ähnlich sind, unterscheidet sich der Netzzugang für mobile und für leitungsgebundene Netze erheblich.

Bei traditionellen, leitungsgebundenen Netzen, wie etwa den Festnetzen der Telekommunikationsunternehmen erfolgt der Zugang zum Netz über eine fest installierte Kabelverbindung. Die Leitung zum Teilnehmer ist fest durchgeschaltet und statisch. Der Teilnehmer wird durch seine Anschlussleitung identifiziert: Der Netzbetreiber setzt voraus, dass der Nutzer sich an seiner vertraglich registrierten Adresse befindet und sich dort mit dem vorgesehenen Netzzuschlusspunkt (Telefon- oder Datenbuchse) verbindet. Ein eingehendes Signal am Kern-Netz wird direkt dem unter dieser Anschlussleitung registrierten

Kunden zugeordnet. Dabei werden stillschweigend die häuslichen Wireless Local Area Network-Zugänge (WLAN) als Ersatz einer Anschlussbuchse eingeschlossen.

Im Unterschied zu einem leitungsgebundenen Kommunikationsnetz kann der vom Mobilfunknetz angebotene Dienst in Anspruch genommen werden, wo auch immer der Nutzer sich aufhält. Das gilt insbesondere, während der Nutzer im engeren Sinne des Wortes mobil ist, sich also in Bewegung von einem Ort zum anderen befindet. Der Zugang zum Mobilfunknetz ist daher im Vergleich komplexer. Das Zugangsnetz besteht aus den sogenannten Basisstationen, aus Übertragungsstrecken, die Basisstationen untereinander und mit dem Kern-Netz verbinden, sowie zusätzlichen Kontroll-Einheiten. Basisstationen sind Funkstationen, die oft auf eigens dafür errichteten Masten installiert sind.

Die Kommunikation zwischen Endgerät und Basisstation mittels elektromagnetischer Wellen (umgangssprachlich auch als Funksignale bezeichnet) wird in Kap. 3 eingehender besprochen. Ähnlich dem UKW Radio- oder TV-Empfang über Antenne können mit Hilfe der Funksignale analoge (Sprache und andere Audiosignale) oder digitale Daten (u. a. Bilder, digitales Fernsehen, DAB Radio) übertragen werden. Mit ihren Antennen senden und empfangen sie Funksignale zu und von den mobilen Endgeräten, die gleichfalls passende Sender und Empfänger besitzen.

Mobile Teilnehmer können sich grundsätzlich überall aufhalten (sogar irgendwo auf der Welt; dies wird als Roaming bezeichnet, auf Deutsch: Herumstreifen). Daher muss die Identifikation durch das Netz auf einer logischen Ebene erfolgen. Wenn das Endgerät im Funkbereich einer Basisstation ist, tauscht es mit dem für die Zulassung im Netz verantwortlichen Knoten über die Basisstation eine verschlüsselte, weltweit eindeutige Kennung aus.

Bewegt sich der Teilnehmer mit seinem Endgerät aus dem Funkbereich einer Basisstation in den Funkbereich einer anderen Basisstation, leitet das Netz ein automatisches Handover ein. Dabei wird die bestehende Verbindung nicht unterbrochen. Da das Netz nicht nur Verbindungswünsche behandelt, die vom Teilnehmer ausgehen, sondern auch für eingehende Verbindungen Kontakt zum Endgerät aufnehmen müssen, ist es notwendig, dass der Aufenthaltsbereich des Endgerätes mit einer für die Herstellung der Verbindung hinreichenden Genauigkeit bekannt oder schnell zu ermitteln ist. Dafür hält das Kern-Netz eine umfangreiche Datenbank vor, die über die Teilnehmer-Registratur eines leitungsgebundenen Netzes hinaus Ortsdaten enthält und ständig aktualisiert wird (Home Subscriber Server, HSS).

2.2.2 Architektur eines Mobilfunknetzes

In Abb. 2.1 werden die grundsätzlichen Strukturen und Datenwege eines Mobilfunknetzes dargestellt. Das Netz kann in die Bereiche Kern-Netz und Radio-Netz gegliedert werden. Das Radio-Netzwerk (englisch: Radio Access Network, RAN) sorgt mit seinen auf Türmen, Masten oder Hausdächern installierten Antennen für die Verbindung mit den mobilen Endgeräten. Die mit den Antennen verbundene Elektronik-Installation zum Austausch

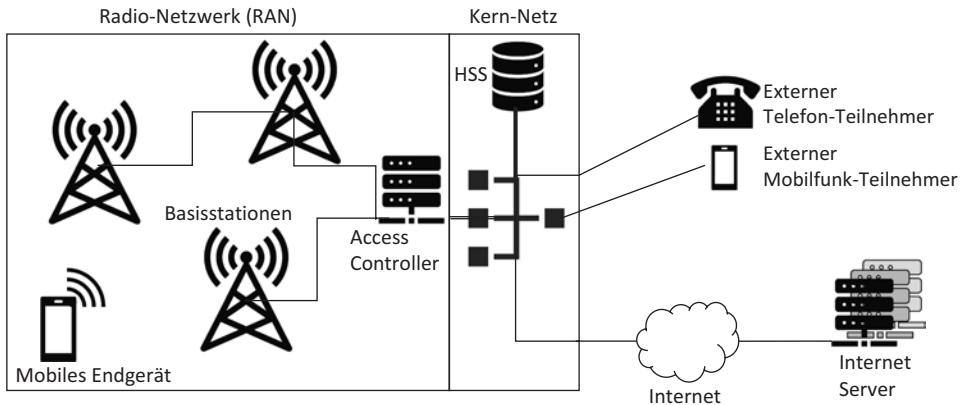


Abb. 2.1 Prinzipieller Aufbau eines Mobilfunknetzwerks

von Funksignalen mit dem mobilen Endgerät über die Antennen wird als Basisstation bezeichnet. Das Kern-Netz stellt die gewünschte Verbindung des mobilen Endgerätes mit einem externen oder netzinternen Endgerät her. Dabei kann es sich um ein herkömmliches Telefon, ein Mobiltelefon, einen Server im Internet oder ein Datenterminal handeln.

2.2.3 Das Radio-Netzwerk: Basisstationen und Mobilfunkzellen

Das Radio-Netzwerk ist der für die Öffentlichkeit sichtbare Teil eines Mobilfunknetzes. Die Antennen tragenden Türme und Masten sind oft mehr als 30 m hoch, und auf hohen Häusern in Städten finden sich teilweise eindrucksvolle Antennenkonfigurationen (Abb. 2.2). Um alle Teilnehmer versorgen zu können und um die Mobilität der Teilnehmer zu gewährleisten, muss ein Mobilfunknetz einen großen Teil der Landesfläche abdecken. Ein Radio-Netzwerk in Deutschland hat daher mindestens 10.000, typischerweise heute jedoch ca. 30.000 Standorte. Die Leitungswege im Radio-Netzwerk verbinden die Basisstationen mit dem Kern-Netz. Es handelt sich sowohl um leitungsgebundene Übertragungswege („Standleitungen“) als auch um Richtfunkverbindungen. Access-Controller bündeln und steuern den Verkehr zwischen Radio-Netzwerk und Kern-Netz. Ihr genauer Funktionsumfang hängt von der eingesetzten Mobilfunk-Technologie ab.

Eine Basisstation besitzt eine oder mehrere Antennen, über die Funksignale mit den mobilen Endgeräten ausgetauscht werden. Jede Mobilfunkantenne wird mit einem eigenen unabhängigen Signal gespeist und definiert eine Mobilfunkzelle. In Gebieten mit wenig Mobilfunkverkehr kommen sogenannte Rundstrahler zum Einsatz, deren Signale eine annähernd kreisförmige Fläche abdecken. Häufiger werden jedoch Kombinationen von drei Antennen verwendet, die jeweils gerichtet in einen Sektor von 120 Grad abstrahlen. Schematisch wird der Abdeckungsbereich gern als Sechseck mit der Basisstation in der

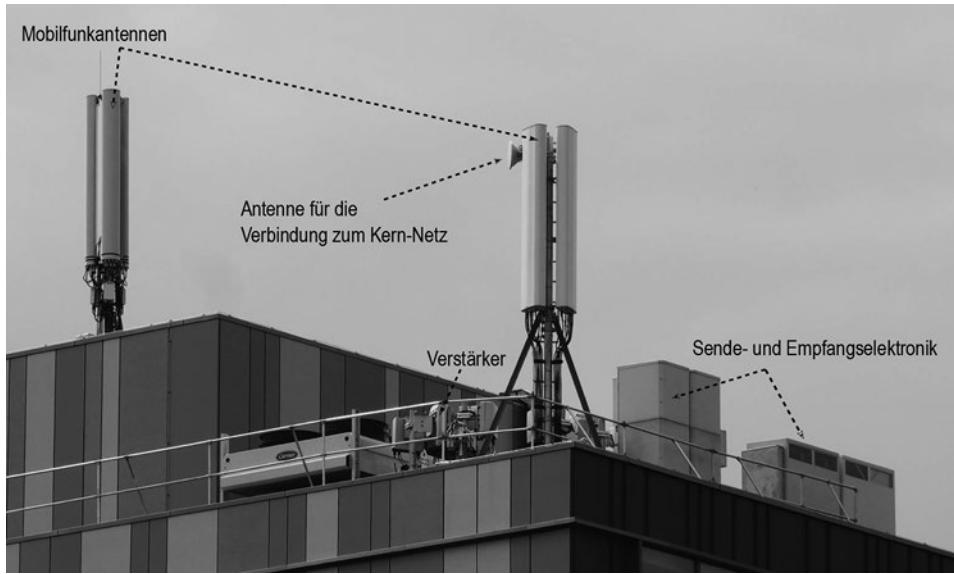


Abb. 2.2 Mobilfunk-Basisstation auf Dachstandort

Mitte dargestellt. Endgeräte innerhalb einer Mobilfunkzelle müssen die Basisstation mit ihrer geringen Sendeleistung erreichen können. Geländeform, Bodenbeschaffenheit und Bebauung beeinflussen die Reichweite des Signals der Endgeräte. Hierdurch wird die tatsächliche Größe und Gestalt der Mobilfunkzelle festgelegt (Abb. 2.3).

Das Grundmuster eines Funknetzwerkes mit Sektor-Antennen zeigt Abb. 2.4. Die Sechsecke lassen sich nahtlos aneinanderfügen, so dass theoretisch eine lückenlose Abdeckung erzielt werden kann.

In der Realität lässt sich das sechseckige Grundmuster aufgrund der wechselnden Boden- und Bebauungsverhältnisse allerdings nicht durchhalten, wie der Blick auf eine realistische Verteilung in der Abb. 2.5 zeigt. Die markierten Stellen bezeichnen die Standorte der tatsächlich installierten Basisstationen des D1-Netzes in der Kölner Innenstadt.

Die begrenzten Radien der Mobilfunkzellen haben zur Folge, dass ein mobiles Endgerät während einer Verbindung nacheinander möglicherweise mit mehreren Basisstationen kommunizieren muss. Für einen störungsfreien Betrieb muss es beim Wechsel der Zelle automatisch von einer Basisstation zur nächsten „übergeben“ werden. Die Verbindung zur ersten Basisstation wird getrennt, und eine Verbindung zur neuen Basisstation wird aufgebaut. Dabei soll es nicht zur Unterbrechung der Verbindung oder des laufenden Dienstes kommen. Dies ist die Grundforderung, die hinter dem Begriff „mobil“ steht. Für die Mobilität ist jedoch nicht das Radio-Netzwerk allein verantwortlich. Sowohl der Access Controller als auch Komponenten des Kern-Netzes spielen dabei eine wichtige Rolle.

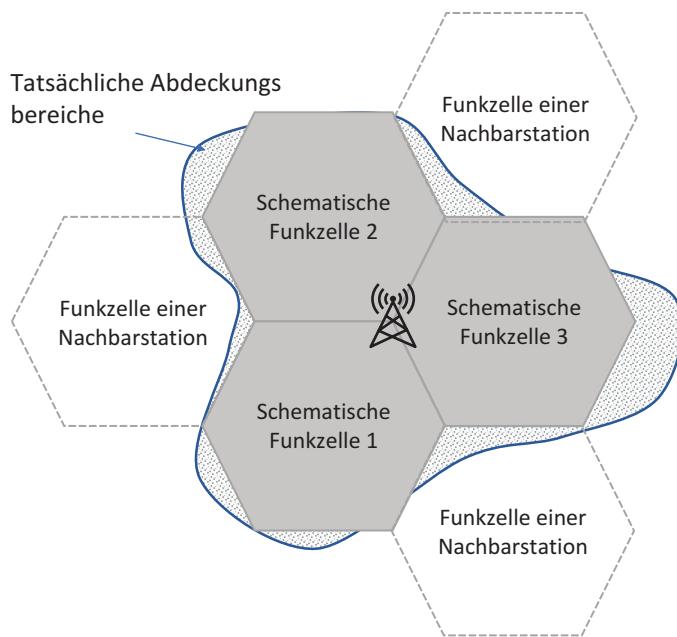


Abb. 2.3 Mobilfunkstation mit drei Funkzellen und idealisiertem sechseckigen und typischem tatsächlichem Abdeckungsbereich

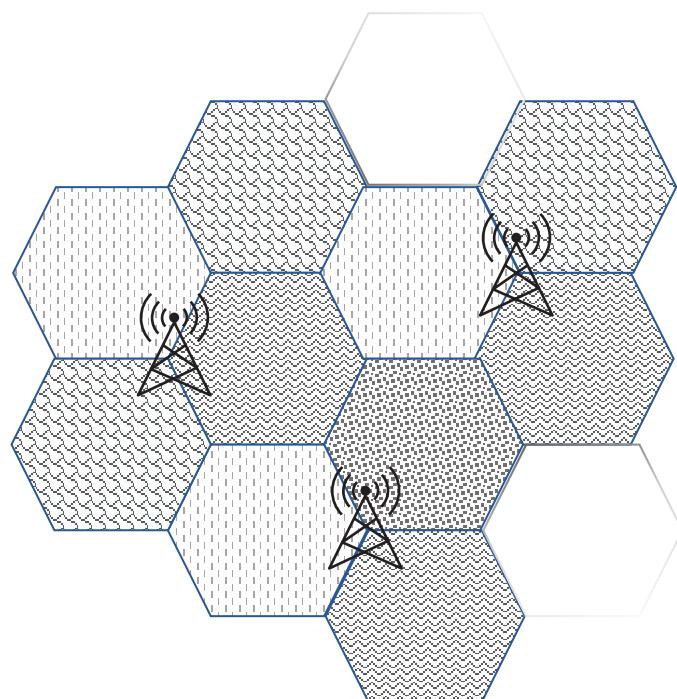


Abb. 2.4 Sechseckiges Grundmuster in der theoretischen Darstellung

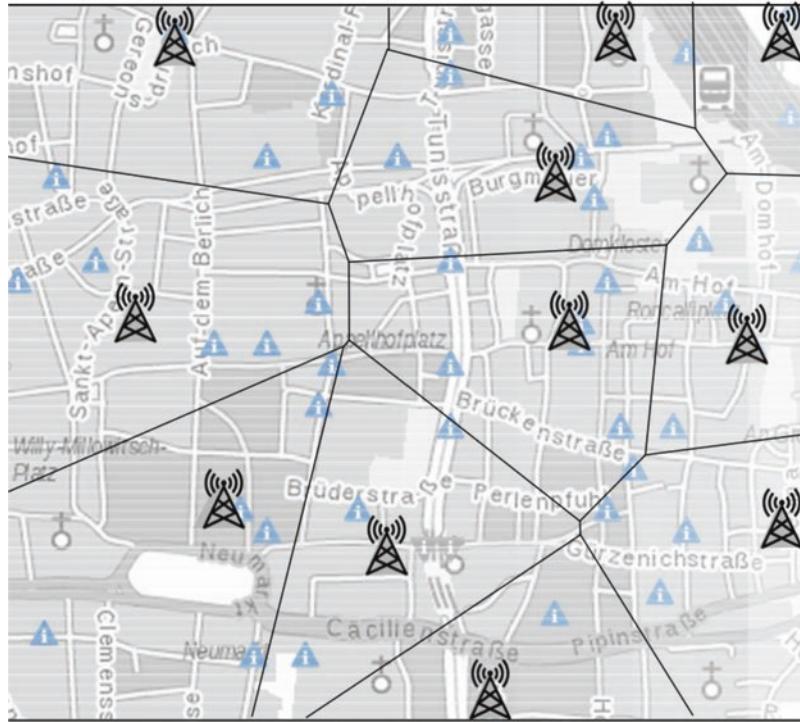


Abb. 2.5 Die Mobilfunkstationen eines Netzes in der Kölner Innenstadt

2.2.4 Das Kern-Netz

Das Kern-Netz ist das „Gehirn“ des Mobilfunknetzes. Die wesentlichen Funktionen des Kern-Netzes sind

- Kontrolle und Steuerung der Radio-Basisstationen
- Zulassung von Netzzugriffen der Endgeräte
- Schaltung von Verbindungen zwischen mobilen Endgeräten und zu Endgeräten oder Telefonen außerhalb des eigenen Netzes
- Schaltung von Verbindungen mobiler Endgeräte zu netzeigenen Dienste-Servern oder in das Internet
- Verfolgung der Positionen aller Endgeräte im Netz und Kontrolle des Handover von Endgeräten zwischen Basisstationen
- Erzeugung von Abrechnungsdaten für in Anspruch genommene Dienste aller Endgeräte

Das Kern-Netz speichert im Rahmen der gesetzlichen Anforderungen Zeiten, Netzadressen und Positionen des Zugriffs der mobilen Endgeräte, und stellt Schnittstellen zum Abhören von Verbindungen durch Sicherheits- und Strafverfolgungsbehörden bereit.

Die Architektur des Kern-Netzes hat sich seit Beginn des digitalen Mobilfunks stark verändert. Einzelne Aufgaben wurden ursprünglich von spezialisierten Knoten ausgeführt, die von Generation zu Generation ergänzt, zusammengelegt oder aufgetrennt wurden. Ein modernes Kern-Netz wird heute über Cloud Computing-Infrastrukturen realisiert. Eine detailliertere Diskussion der Architekturen in den einzelnen Generationen des Mobilfunk erfolgt in Kap. 4. An dieser Stelle erfolgt eine Konzentration auf die Ausführung der wichtigsten Aufgaben.

Ein Herzstück des Kern-Netzes ist der Home Subscriber Server (HSS). Die HSS-Datenbanken sind für die wichtigen Funktionen Authentifizierung der Netzteilnehmer und Autorisierung der tariflichen Dienste verantwortlich, und speichern dazu die Tarif-Informationen jedes einzelnen Netzteilnehmers. Jeder Teilnehmer-Datensatz ist mit einer weltweit eindeutigen Teilnehmerkennung (IMSI) abgelegt. Der HSS ist auch der Speicherort für die Zugangscodes und Verschlüsselungs-Daten der Teilnehmer. Der aktuelle Aufenthaltsort jedes im Netz enthaltenen Endgerätes wird gespeichert und ständig aktualisiert. Da mobile Endgeräte laufend ihre Position verändern können, wird umgekehrt ihr Aufenthaltsort von den Knoten des Kern-Netzes zur Herstellung von Verbindungen abgefragt.

Das Kern-Netz besitzt in der Regel Schnittstellen zu verschiedenen Netzen. Darunter sind andere Mobilfunknetze, leitungsgebundene Telefonnetze, öffentliches Internet, Datennetzwerke von direkt angeschlossenen Unternehmen, sowie Netze des eigenen mobilen Netzbetreibers, über die Dienste wie Multimedia Messaging oder Internet-Telefonie angeboten werden.

2.2.5 Systeme zum Netzmanagement, zur Netzüberwachung und Abrechnung

Ein netzweites Überwachungs- und Kontrollsysteem sorgt dafür, dass Störungen oder Ausfälle von Diensten und von einzelnen Knoten erkannt und behoben werden. Im Störfall wird ein Alarm an das Netzmanagement gesendet. Darüber hinaus werden zahlreiche Ereignisse im Netz, wie etwa der Abbruch von Verbindungen, von Zählern in den Netzknoten erfasst und regelmäßig vom Netzmanagement abgefragt. Sie dienen als Grundlage für Qualitätsberichte und zur Netzauslastung. Nicht alle Störungen lassen sich online beheben; deshalb gibt es auch Service-Kräfte, die vor Ort tätig werden.

Zu den Aufgaben des Netzmanagements gehört die Konfiguration des Netzes, die laufend aktualisiert werden muss. Zum Beispiel erfordern neue Wohngebiete oder Industriean-siedlungen bessere Mobilfunkversorgung. Regelmäßig müssen Standorte verlegt werden, weil ein Gebäude abgerissen wird, der Mietvertrag für den Standort ausläuft oder ein Neubau einen Funksektor abschattet. Dies erfordert in der Regel die Umplanung der Zellen in der ganzen Region.

Für die Netzbetreiber ist die Abrechnungsfunktion von kritischer Bedeutung. Jeder Netzknopen erzeugt laufend teilnehmer- und verbindungsbezogene Abrechnungsdaten, die über ein separates Daten-Netzwerk zum Abrechnungssystem übertragen werden. Dort werden die Daten konsolidiert, und der resultierende Betrag wird entweder vom Guthabenkonto des Teilnehmers abgezogen (Prepaid) oder in einer monatlichen Abrechnung mit Einzelnachweisen zusammengefasst (Postpaid). Für Prepaid-Teilnehmer wird vor der Herstellung einer Netzverbindung grundsätzlich auch der Stand des Guthabenkontos abgefragt.

2.3 Die SIM-Karte und die Authentifizierung der Teilnehmer

Die SIM-Karte ist allen Teilnehmern an einem Mobilfunknetz wohlbekannt. Sie wird hier weiter unter ihrer populären Bezeichnung geführt. Offiziell ist die Bezeichnung allerdings Universal Integrated Circuit Card (UICC). Die Bezeichnung SIM erhält sie von der darauf gespeicherten und auf der Karte ablauffähigen Applikation *Subscriber Identification Module*. Seit der Einführung von UMTS im Jahre 2002 enthält die Karte auch die verbesserte Applikation USIM (Universal SIM). Die SIM-Karte ist unabhängig vom mobilen Endgerät und muss vor Inbetriebnahme in einem Netz typischerweise in den dafür vorgesehenen Schacht am Endgerät eingesetzt werden.

Die SIM-Karte ist in verschiedenen Formaten erhältlich. Durch die Anforderungen der Mobiltelefon-Designer wurden immer kleinere Kartenformate entwickelt und spezifiziert. Bei der Einführung durch den GSM-Standard (Global System for Mobile Communication, Abschn. 4.3) hatten SIM-Karten das gebräuchliche Scheckkarten Format. Nach und nach kamen dann kleinere Formate in Gebrauch. Abb. 2.6 zeigt die Formate Mini-, Mikro- und Nano SIM mit den vorgestanzten Rändern der jeweils kleineren Formate. Beim Wechsel des SIM-Karten Formates muss so nicht jedes Mal eine neue Karte angefordert werden. Der eigentliche Chip ist allerdings dabei in allen Formaten unverändert.

Seit kurzem gibt es mit der embedded SIM (eSIM), rechts in Abb. 2.6, eine Abkehr von der klaren physikalischen Trennung von Telefon und SIM-Karte. Die eSIM ist ein im mobilen Endgerät fest eingebautes Modul, das vor unautorisierten Zugriffen geschützt ist,



Abb. 2.6 SIM-Formate: Mini, Mikro und Nano, sowie eSIM von Gieseke+Devrient Mobile Security

und vom Netzbetreiber über eine vom Mobilfunknetz unabhängige Datenverbindung (z. B. WLAN) mit den SIM-Daten geladen werden kann. Ein Vorteil von eSIM für den Kunden ist die Möglichkeit, Mobilfunkverträge zu 100 % online ohne Verzögerung durch Postwege abzuschließen. Der Vorteil für die Hersteller besteht in der größeren Flexibilität des Designs durch Wegfall eines Karten-Slots. eSIM wird bereits von den meisten Mobilfunkunternehmen unterstützt und es ist davon auszugehen, dass diese Technik die herkömmliche SIM-Karte ersetzen wird.

SIM und USIM sind so etwas wie der Reisepass des Teilnehmers zum Eintritt in das Netzwerk. Mit ihrer Hilfe und durch sie stellt das Netzwerk die Identität des Teilnehmers fest, und sichert ab, dass die erbrachten Dienste auch abgerechnet werden können. Bei der moderneren USIM-Applikation weist sich auch das Netzwerk gegenüber dem Teilnehmer aus.

Das Netzwerk entscheidet, ob SIM oder USIM gefordert werden. Ab der 4. Generation des Mobilfunk ist USIM allerdings von den internationalen Standards vorgeschrieben. Außer den Daten für die Identifikation des Teilnehmers berechnen SIM und USIM die Startwerte von Verschlüsselungsalgorithmen, mit denen der Funkverkehr gegen Abhören abgesichert werden kann. Das von USIM unterstützte Verschlüsselungsverfahren ist dabei deutlich stärker als das herkömmliche SIM Verschlüsselungs-Verfahren.

Die SIM-Karte gehört zum Mobilfunk-Teilnehmer und seinem Abrechnungskonto bzw. Vertrag. Sie gehört nicht zum mobilen Endgerät. Diese Trennung zwischen Teilnehmer/Vertrag und Endgerät war eine der Hauptursachen für den seit den 1990er-Jahren bis heute anhaltenden Endgeräte-Boom. Früher war ein Mobiltelefon immer an einen Vertrag gebunden, und konnte auch nur vom Netzbetreiber erworben oder gemietet werden. Durch die SIM-Karte konnten Mobilfunk-Teilnehmer nun eigenständig ihr Gerät wechseln, ein neues Telefon kaufen und ein gebrauchtes Telefon verkaufen. Anbieter von Consumer-Elektronik konnten sich unabhängig von den Netzbetreibern mit attraktiven Angeboten am Endgeräte-Markt platzieren. Heute führende Anbieter wie Samsung oder Apple hätten sich in einem von den Netzbetreibern gelenkten Endgerätemarkt kaum erfolgreich etablieren können.

Die wichtigsten auf der SIM-Karte gespeicherten Daten sind

- Die International Mobile Subscriber Identity (IMSI).
- Eine geheime Schlüsselzahl K_i , die zur Authentifikation und zur Erzeugung von Schlüsseln für die Datenübertragung genutzt wird.
- Eine Reihe von kryptografischen Algorithmen zur Erzeugung von Authentifikations- und Verschlüsselungsdaten.
- Der für Datendienste benötigte Access Point Name (APN), eine Adresse (URL) für den Netzübergang bei Datenverbindungen - Eine laufende Nummer (Sequenznummer), die die Wiederverwendung mitgeschnittener Anmeldedaten (Replay-Attacke) verhindert.

Die kryptografischen Daten stehen in einem besonders geschützten Bereich und können nicht ausgelesen oder überschrieben werden. Weitere administrative Daten finden sich sowohl im ungeschützten als auch im geschützten Bereich; darunter sind die eigene

Telefon-Nummer und die Zugangsdaten zu Datennetzen. Für jeden Teilnehmer finden sich die Zugangsdaten der SIM-Karte auch unter dem Eintrag im HSS.

Die dem Teilnehmer zugeordnete Mobilfunknummer ist keine verlässliche Identifikation. Eine Mobilfunknummer identifiziert nicht zwingend das zugehörige Netz, und die gleiche Nummer kann in verschiedenen Ländern genutzt werden. Im Gegensatz dazu ist die IMSI eine weltweit eindeutige Teilnehmerkennung. Unter dieser Kennung wird der Teilnehmer auch im HSS geführt. Sie ist eine hierarchisch aufgebaute Kennung, die aus einem Ländercode, einem Netzwerk-Code und einer eindeutigen Kennung des Teilnehmers im Netzwerk besteht (Tab. 2.1) Die IMSI-Teilnehmer-Kennung ist aus Sicherheitsgründen völlig unabhängig von der Telefonnummer des Teilnehmers.

Die IMSI ist das primäre Schlüsselattribut für den Zugriff auf die im Home Subscriber Server gespeicherten Daten des Teilnehmers und die für die Anmeldung am Netz genutzte Kennung.

Ein weiteres wichtiges Datum ist der International Mobile Equipment Identifier (IMEI). Er gehört allerdings nicht zu den Daten der SIM-Karte, sondern als international standardisierte Serien-Nummer zum mobilen Endgerät. Der IMEI wird bei jeder Anmeldung übermittelt, und kann genutzt werden, um als gestohlen oder verloren gemeldete Endgeräte für den Netzbetrieb zu sperren. Zusätzlich können Netzbetreiber mittels IMEI ganze Serien von technisch nicht zugelassenen Endgeräten sperren. Auch einige Netzapplikationen nutzen die IMEI als Identifikationsmerkmal. Sie wollen damit verhindern, dass über dasselbe Endgerät durch Verwendung verschiedener SIM-Karten mehrfache Accounts angelegt werden. Durch die standardisierte Tastenkombination *#06# kann die IMEI eines Gerätes im Display angezeigt werden (Tab. 2.2).

Tab. 2.1 Die Struktur der IMSI mit Datenfeldern und typischen Werten

| Feld: | Region | Land | Netz | Teilnehmer-Kennung |
|--------------|--|---|---|--------------------|
| Feldlänge: | 1 Ziffer | 2 Ziffern | 2 Ziffern | Bis 10 Ziffern |
| Beispiel: | 2 | 62 | 01 | 2233445678 |
| Erläuterung: | <i>Regionen:</i> 1 Europa, 2 Nordamerika, 3 Asien, 4 Australien, 5 Afrika | 262 Deutschland, 232 Österreich, 228 Schweiz, 310 bis 316 USA, 460, 461 China | <i>Netze in Deutschland:</i> 01, 06: T-Mobile, 02, 04: Vodafone, 03, 07: O2. | |

Tab. 2.2 Struktur der Endgeräte-Kennung IMEI

| Feld-Name | TAC Type Allocation Code | | SNR | CD | SVN |
|------------------|-----------------------------|-----------------------------|-----------------|---|------------------|
| Feld-Bedeutung | Kennzeichnung des Modells | | Seriennummer | Prüfziffer | Software Version |
| Subfeld-Name | Organisation | Hersteller& Modell | des Herstellers | | |
| (Sub)-Feld-Länge | 2 | 6 | 6 | 2 | 2 |
| Beispiel | 35 (UK) | 660508 (Apple iPhone SE) | 372832 | Nicht ans Netz übertragen Im Display angezeigt | |

2.4 Prozeduren und Abläufe im Mobilfunkbetrieb

Die folgenden Beschreibungen von Mobilfunk-Prozeduren sind möglichst allgemein und technologienutral gehalten. Auch werden zur besseren Übersichtlichkeit einzelne Schritte ausgelassen oder zusammengefasst. Grundsätzlich folgt die Darstellung den Abläufen in den lizenzierten (öffentlichen) Mobilfunknetzen. Sie unterscheiden sich in den verschiedenen Mobilfunktechnologien und Generationen in Details, die zwar für die technische Implementation wichtig, für das allgemeine Verständnis des Ablaufs allerdings unwesentlich sind.

Der Zugriff eines mobilen Endgerätes auf das Mobilfunknetz erfolgt in mehreren Schritten:

- Das Endgerät muss das richtige Netz finden
- Ein Funkkontakt zwischen Endgerät und Basisstation wird hergestellt
- Schließlich erfolgen die Anmeldung und Authentifikation am Kern-Netz.

Wenn im Folgenden von Kanälen oder Nachrichtenkanälen die Rede ist, handelt es sich bei den meisten Mobilfunktechnologien um Zeit- und Frequenzabschnitte, die einem Endgerät oder mehreren Endgeräten zum Austausch von Protokoll-Nachrichten mit dem Netz zugewiesen werden. Auf diese Weise wird unter anderem der Umfang der Nachrichten an der Funkschnittstelle reduziert.

2.4.1 Identifikation des Netzes

Ein mobiles Endgerät muss nach dem Einschalten oder einem Verbindungsverlust das richtige Netz auswählen. Das Endgerät findet dazu die Netz-ID und die IMSI des Teilnehmers auf der SIM-Karte.

Ähnlich wie der Sender-Scan eines FM-Radios sucht die Empfangselektronik des Gerätes dann nach Signalen der verfügbaren Mobilfunknetze. Oft hat das Endgerät bereits Informationen über die Lage dieses Signals, zum Beispiel durch die Speicherung des zuletzt genutzten Netzes. Es kann allerdings nicht davon ausgegangen werden, dass dies immer der Fall ist. Der Teilnehmer könnte in der Zwischenzeit gereist sein, oder sein Gerät nach einem Urlaubsflug in einem anderen Land einschalten. Ohne Vorabinformation kann die Suche nach einem Netz mehrere Minuten dauern.

In der Regel wird bei der Suche das Signal mit der höchsten Empfangsleistung als erstes ausgewählt. Jedes Netz sendet über seine Basisstationen ein oder mehrere Pilot-Signale aus, die unverschlüsselt übertragen werden (Abb. 2.7, Schritt 1). In zwei Schritten erlauben sie dem Empfänger des Endgerätes, das richtige Netz zu identifizieren:

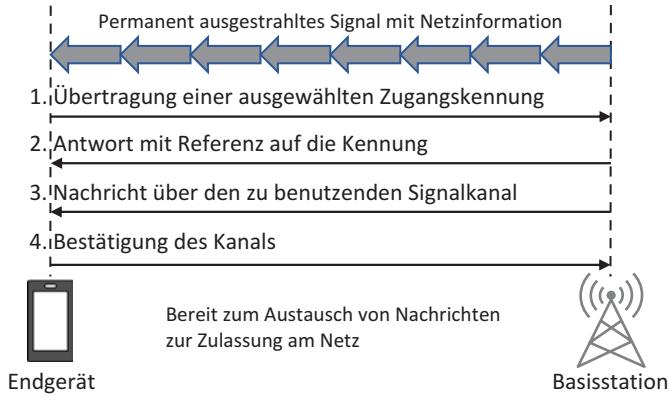


Abb. 2.7 Anmeldung eines Endgerätes am Netz

- a. Synchronisation mit dem empfangenen digitalen Signal. Das von der Basisstation gesendete Signal läuft in einem festen Zeittakt, der zunächst vom Endgerät aufgenommen werden muss. Das Signal wird durch Rahmen zeitlich strukturiert. Ein Rahmen ist eine feste Anzahl von Taktzeiten, die periodisch ablaufen. Die vom Endgerät benötigten Informationen über das Netz werden an festgelegten Taktpositionen im Rahmen übertragen. Daher ist es für das Endgerät zwingend notwendig, den Rahmenbeginn und die Taktfrequenz zu kennen.
- b. Auslesen der Netzinformation. Neben dem Netz-Namen, der Netz-Kennung und Zugriffs-Informationen kann das Netz an dieser Stelle bereits eine Überlastsituation oder die Nicht-Zulassung bestimmter Endgeräte-Kategorien mitteilen.

Handelt es sich um eine „falsche“ Netz-ID, wird das Verfahren abgebrochen, und das Endgerät fährt mit dem nächsten Signal fort. Bis zu dieser Stelle funktioniert ein mobiles Endgerät ausschließlich als Empfänger, sendet also keine eigenen Daten. Wird ein Netz mit einer zulässigen Netzkennung gefunden, beginnt es mit der Anmeldeprozedur.

2.4.2 Anmeldung am Netz

Hat ein mobiles Endgerät ein passendes Netz gefunden, muss es sich bekannt machen und für den Datenverkehr zugelassen werden. Dies geschieht durch die Zugangs-Prozedur. Der mögliche Zeitpunkt des Startes der Zugangsprozedur ist eine der Informationen, die aus dem Piloten-Signal entnommen wird. Das Endgerät wählt eine zufällige Kennung aus einem durch den Standard vorgegebenen Vorrat aus und sendet sie als Signal an die Basisstation.

(Abb. 2.7, Schritt 1). Das Netz empfängt das Signal und antwortet darauf (Abb. 2.7, Schritt 2) über einen Kanal, der ebenfalls durch die Pilot-Signale vorgegeben wird. Die positive Antwort enthält eine Referenz auf die übersandte Kennung. Es ist möglich, dass zwei Endgeräte zur gleichen Zeit die gleiche Kennung senden. Eine Koordination durch die Endgeräte über die zu verwendenden Kennungen ist nicht vorgesehen. Im Falle einer solchen Kollision wird die Anfrage nicht durch die Basisstation beantwortet und das Gerät versucht den Zugang nach zufälliger Wartezeit erneut. Als Ergebnis einer erfolgreichen Anmelde-Prozedur richtet die Basisstation einen Kanal ein (Abb. 2.7, Schritt 3), über den das Endgerät weitere Anmeldedaten übermitteln kann. Dieser Kanal wird in Schritt 4 vom Endgerät bestätigt. Es gibt aber zu diesem Zeitpunkt noch keine Möglichkeit für das mobile Endgerät, Nutzdaten oder Sprache zu empfangen oder zu senden.

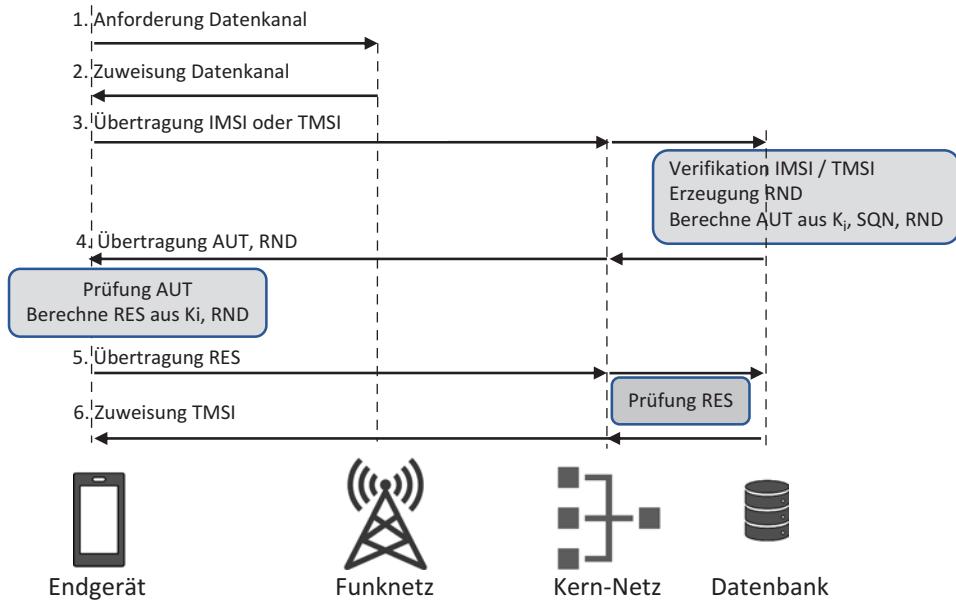
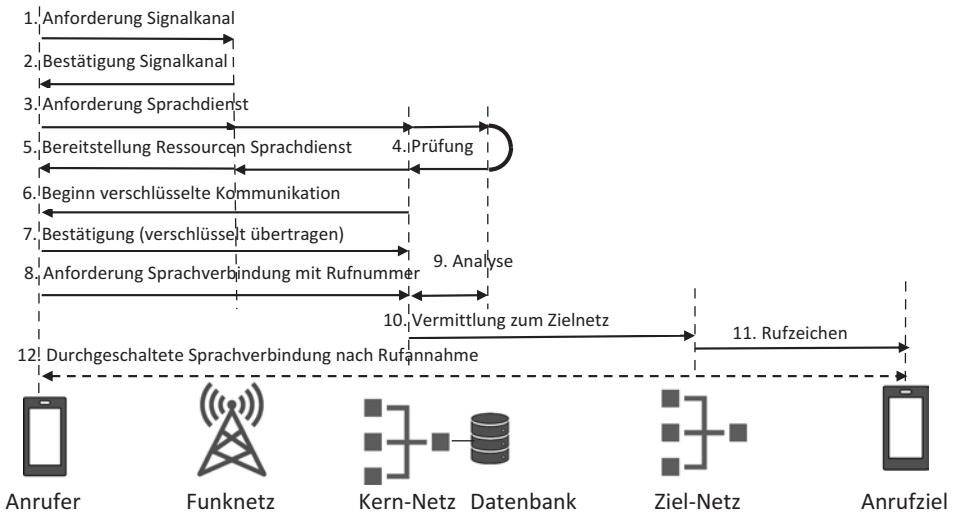
Im Fall des Handover des Endgerätes von einer Basisstation zu einer benachbarten Station erfolgt eine vereinfachte Version dieser Anmeldung. Dabei wird eine Kennung aus einem reservierten Bereich vorab ausgewählt, so dass keine Kollision entstehen kann. Diese Kennung wird von der empfangenen Basisstation an die abgebende Station und von dort an das Endgerät übertragen.

Die Pfeile in der Abb. 2.7 zeigen, wie auch in den folgenden Abb. (2.8, 2.9 und 2.10), zwischen welchen Instanzen und in welcher Richtung der jeweilige Nachrichtenaustausch stattfindet. Die zeitliche Reihenfolge ist von oben nach unten.

2.4.3 Teilnehmer-Authentifizierung

Im nächsten Schritt beantragt und erhält das Endgerät eine Sendeberechtigung (Abb. 2.8, Schritt 1 und 2) und übersendet die von der SIM-Karte ausgelesene Teilnehmer-IMSI als Kennung über den vom Netz eingerichteten Kanal (Abb. 2.8, Schritt 3). Die IMSI wird an das Kern-Netz und dort an den HSS weitergeleitet und überprüft. Bei der Überprüfung spielen die für den Teilnehmer unter seiner IMSI gelisteten Berechtigungen, aber auch sein Tarifstatus eine Rolle. Erfolgt die Anmeldung am Netz eines fremden Betreibers, zum Beispiel im Ausland, muss der Kontakt mit dem Heimatnetz hergestellt werden, das sich aus der IMSI ergibt. Zusammen mit der IMSI wird auch die Endgeräte IMEI übertragen. Sie wird vom HSS mit der dort gespeicherten Liste gestohlener oder verlorener Endgeräte verglichen. Bei einem Treffer wird der Zugang verweigert und der Prozess abgebrochen. IMSI und IMEI werden entsprechend gesetzlicher Anforderungen für die Abfrage durch Strafverfolgungsbehörden temporär gespeichert.

Die gegenseitige Authentifizierung von Netzwerk und Endgerät wird anschließend vom Netz angestoßen. Die in SIM/USIM und in der Netz-Datenbank gespeicherte geheime Schlüsselzahl K_i (Abschn. 2.3) ist das Kernelement dieses Prozesses. Sie wird allerdings niemals unverschlüsselt über das Netz ausgetauscht. USIM und Kern-Netz verwenden zusätzlich zu K_i eine mit USIM eingeführte gemeinsame Sequenznummer SQN, die Replay-Attacken verhindern soll. Das Kern-Netz sendet einen Authentifizierungscode, erzeugt durch einen kryptografischen Algorithmus aus K_i , einer Zufallszahl RND und der

**Abb. 2.8** Endgeräte Authentifizierung**Abb. 2.9** Abgehendes Gespräch aus Mobilfunknetz

Sequenznummer an das Endgerät (Abb. 2.8, Schritt 4). Die Zufallszahl RND wird zusätzlich separat übersandt. USIM überprüft AUT mit Hilfe der dort vorliegenden Daten. Im Erfolgsfall erzeugt USIM aus K_i und RND die Antwort RES, die an das Netz übermittelt wird (Schritt 5). Stimmt der Wert von RES mit dem vom Netz erwarteten überein, sind

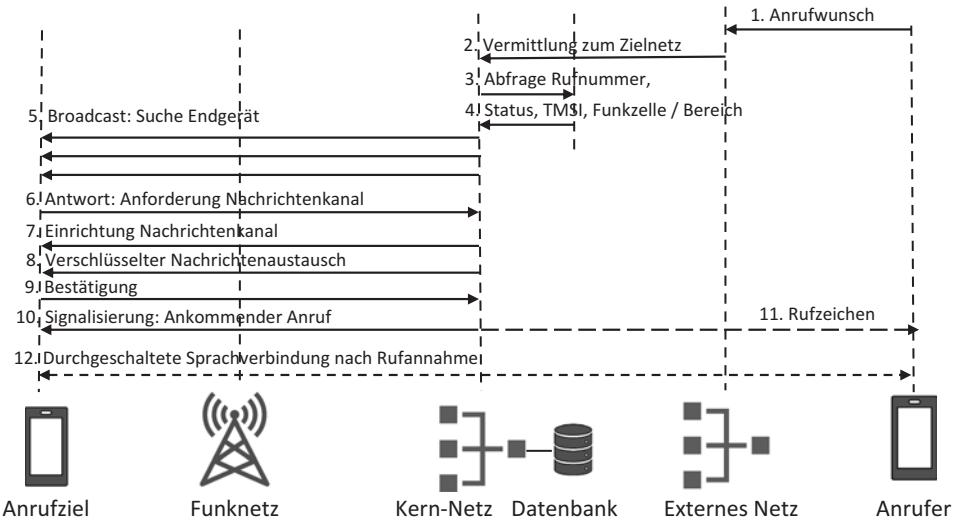


Abb. 2.10 Ankommender Anruf in einem Mobilfunknetzwerk

Endgerät und Netz gegenseitig authentifiziert. In Netzen, die lediglich SIM verwenden, kann der zweite Schritt ohne den ersten erfolgen. Ein Netz, das sich nicht selbst identifizieren will oder kann, sendet lediglich die Zufallszahl RND zur Authentifizierung des Teilnehmers. Im letzten Schritt vergibt das Netz eine temporäre Teilnehmer-ID (TMSI), unter der das Endgerät jetzt erreicht werden kann. Damit wird vermieden, dass für weitere Vorgänge jedes Mal die IMSI übertragen werden muss.

Aus dem zur Authentifizierung benutzten geheimen Schlüssel K_i leiten beide Seiten schließlich die Schlüsselparameter für die spätere Nachrichten- und Datenverschlüsselung ab.

In regelmäßigen Abständen wird ein sogenanntes Location Update durchgeführt: Das mobile Endgerät initiiert eine erneute Anmeldeprozedur. Dabei wird allerdings nicht die IMSI, sondern nur noch die temporär vergebene TMSI übertragen. Durch das Location Update wird der Aufenthalt des Endgerätes in der Datenbank aktualisiert und aus Sicherheitsgründen die TMSI neu vergeben.

2.5 Abläufe bei mobiler Telekommunikation

Es werden zwei Abläufe unterschieden: Ein abgehendes Gespräch, ausgehend vom mobilen Teilnehmer sowie ein beim mobilen Teilnehmer an kommendes Gespräch. In beiden Fällen ist der entfernte Gesprächspartner selbst Teilnehmer dieses Netzes oder an ein anderes Mobil- oder Festnetz angeschlossen. Die hier dargestellten Schritte sind als Beispiele gedacht, um prinzipielle Abläufe zu erläutern. In konkreten Netztechnologien sind unter Umständen weitere Aktionen erforderlich, die eine detailliertere Betrachtung der

Netzarchitektur erfordern. Das gilt insbesondere, wenn Gespräche als Voice-over-IP-Verbindungen (VoIP) durchgeführt werden. Mobilfunkteilnehmer merken von all diesen Schritten natürlich nichts; für sie erfolgt der Aufbau durch Eingabe einer Rufnummer und Betätigung der Anruftaste, Wahl eines Anrufziels im Telefon-Menü oder neuerdings durch Sprachkommandos.

2.5.1 Abgehendes Gespräch im Mobilfunknetz

Der Ablauf eines von einem mobilen Endgerät abgehenden Telefonats wird nachstehend und in Abb. 2.9 dargestellt.

1. Das Endgerät fordert einen Kanal für den Nachrichtenaustausch an.
2. Vom Netz (Radionetz oder Kern-Netz je nach Technologie) kommt die Bestätigung mit der Zuweisung eines Kanals.
3. Über den zugewiesenen Kanal zeigt das Endgerät eine gewünschte Sprachverbindung an.
4. Das Kern-Netz überprüft die Berechtigungen
5. Die Bestätigung durch das Netz erfolgt nach Bereitstellung der Netz-internen Ressourcen.
6. Das Kern-Netz gibt die Anweisung („Ciphering“), mit der verschlüsselten Kommunikation zwischen Endgerät und Netz zu beginnen. Die dazu benötigten Schlüssel sind bereits im Rahmen der Anmeldeprozedur berechnet worden.
7. Die Bestätigung erfolgt durch das Endgerät bereits in verschlüsselter Form.
8. Schließlich fordert das Endgerät den Aufbau eines Telefongesprächs an und übermittelt mit der Anforderung die gewünschte Rufnummer.
9. Das Kern-Netz identifiziert das Anrufziel und überprüft die Berechtigung durch Abfrage beim HSS. Bestimmte Gesprächsziele wie Auslands-Nummern oder Mehrwertdienste können tariflich gesperrt sein; bei Prepaid-Kunden wird auch das verfügbare Guthaben im Abrechnungssystem geprüft. Es stellt nach erfolgreicher Prüfung die Verbindung zum Anrufziel über das eigene Netz oder über ein anderes Mobil- oder Festnetz her.
 - a. Befindet sich das angerufene Endgerät im eigenen Netz wird entsprechend ‚Ankommendes Telefongespräch‘ (Abschn. 2.5.2) verfahren.
 - b. Ist das Anrufziel in einem externen Netz, wird entsprechend den standardisierten Protokollen der Netzbetreiber eine Verbindung zu diesem Netz hergestellt und die Rufnummer dorthin übermittelt.
10. Nach Identifizierung des Anrufziels wird eine Verbindung zum externen Netz (Fall b) hergestellt. Die dazu ausgetauschten Nachrichten werden hier nicht im Detail dargestellt.
11. Das zuständige Netz setzt eine Rufnachricht zum angerufenen Endgerät ab. Das angerufene Endgerät zeigt dem Teilnehmer optisch oder akustisch die Verbindung an.

12. Wenn der Teilnehmer das Gespräch angenommen hat, werden durch eine Sequenz von „Connect“ Nachrichten die Sprachkanäle von Ende zu Ende belegt und das Gespräch kann durchgeführt werden.

2.5.2 Ankommendes Gespräch im Mobilfunknetz

Bei ankommenden Gesprächen im Mobilfunk ergeben sich zusätzliche Anforderungen. Die Herstellung einer Gesprächsverbindung zu einem mobilen Endgerät erfordert grundsätzlich erst einmal festzustellen, wo dieses Telefon sich befindet. In Abb. 2.10 sind die Schritte illustriert.

1. Der Anrufer fordert eine Gesprächsverbindung zu einem Teilnehmer eines Mobilfunknetzes an.
2. Das für den Anrufer zuständige Netz identifiziert anhand der Rufnummer das Mobilfunknetz des Anrufziels und stellt eine Verbindung mit dem Mobilfunknetz über eine bestehende Schnittstelle her.
3. Das Kern-Netz stellt eine Anfrage beim HSS zu den Daten des Teilnehmers:
 - a. Wie ist die aktuelle TMSI?
 - b. In welcher Funkzelle befindet sich das Endgerät jetzt oder befand es sich zuletzt?
 - c. Gibt es für die Verbindung administrative Daten wie Blockierungen oder eingerichtete Rufumleitungen?
4. Das HSS beantwortet die Anfrage
5. Das Kern-Netz baut eine Verbindung zur Basisstation auf und führt einen Suchruf (Paging) in der registrierten Zelle durch. Gibt es keine Antwort, wird der Suchbereich Schritt um Schritt ausgeweitet, bis das Endgerät antwortet. Erfolgt keine Antwort, wird der Anruf abgelehnt (Besetzt-Zeichen oder Sprachansage). In vielen Netzen wird auch eine Verbindung zur Voice-Mail hergestellt.
6. Das angerufene Endgerät beantwortet die Suchanfrage mit der Anforderung eines Nachrichtenkanals.
7. Das Kern-Netz bestätigt den Nachrichtenkanal.
8. Das Kern-Netz signalisiert den Beginn der verschlüsselten Kommunikation.
9. Das Endgerät bestätigt die Verschlüsselung mit einer verschlüsselten Nachricht
10. Das Kern-Netz signalisiert dem Endgerät den ankommenden Anruf und überträgt die rufende Telefon-Nummer, sofern freigeschaltet.
11. Es meldet dies über das externe Netz an das anrufende Gerät zurück.
12. Nimmt der Teilnehmer den Anruf an, wird der Sprachkanal von Ende zu Ende durchgeschaltet. Lehnt der angerufene Teilnehmer den Anruf ab, wird ein Besetzt-Signal an den Anrufer gesendet; in vielen Netzen wird auch in dieser Situation die Verbindung zur Voice-Mail hergestellt, um dem Anrufer die Möglichkeit zu geben, eine Sprachnachricht zu hinterlassen.

2.5.3 Kurznachrichten und Cell-Broadcast

Seit den ersten Versionen des digitalen Mobilfunks ist der Austausch von Kurznachrichten zwischen mobilen Endgeräten und dem Mobilfunknetz vorgesehen. Alle Endgeräte unterstützen das Senden und den Empfang dieser Nachrichten. Übermittelt werden SMS über einen Signalisierungskanal in der Mobilfunkzelle. Eine Verbindung zwischen Endgerät und Netz wird dazu nicht aufgebaut. Es werden die Elemente Short Message Mobile Terminated (SM-MT), Short Message Mobile Originated (SM-MO) und Cell Broadcast Service (SM-CB) unterschieden. Aus ihnen setzt sich die Vielfalt der Kurznachrichtendienste zusammen.

Eine MO-Kurznachricht, wird von einem Endgerät aus an das Netz gesendet. Die Nachricht kann durch Verkettung von einzelnen Blöcken (Pages) länger sein als das bekannte Limit von 160 Zeichen. Abhängig von der Implementierung kann sie auch Binärdaten wie etwa Bilder oder Töne enthalten. Die vom Endgerät abgehende Nachricht enthält Adressdaten für die Zustellung. In der Regel handelt es sich um Rufnummern oder Kurzwahlnummern. Möglich sind aber auch E-Mail-Adressen. Das Kern-Netz analysiert die Adressdaten und leitet die Nachricht an das adressierte Endgerät oder an einen mit dem Netz verbundenen Server weiter.

Eine MT-Kurznachricht, wird vom Netz an ein Endgerät gesendet. Mit Bezug auf Inhalte und Länge gilt das unter MO Gesagte. Ist das Endgerät nicht empfangsbereit, werden MT-Nachrichten in der Regel vom Netz zwischengespeichert und später zugestellt. Die Hardware des Endgerätes empfängt die Nachricht und verarbeitet sie entsprechend dem Nachrichtentyp, der vom Netz als Parameter eingefügt wird. Nachrichtentypen sind vor allem normale Textnachrichten, aber zum Beispiel auch Nachrichten mit SIM-Inhalten oder sogenannte Stille Nachrichten. Letztere werden auf dem Endgerät nicht gespeichert oder angezeigt. Sie werden ausschließlich zur Strafverfolgung eingesetzt. Durch den Empfang einer Stillen SMS entsteht genug Netzaktivität, um das Endgerät orten zu können.

Cell-Broadcast Nachrichten dienen zur regionalen Alarmierung bei Katastrophen oder Notfällen. Sie werden von einem staatlichen Cell-Broadcastcenter initiiert, das mit allen Netzen verbunden ist. Versendet wird eine CB-Nachricht an alle Endgeräte, die zum Zeitpunkt des Versands in einer der betroffenen Funkzellen eingebucht ist. Eine individuelle Adressierung der Endgeräte erfolgt dabei nicht. Es gibt auch keine Empfangsbestätigung durch Endgeräte; die Nachricht wird aber regelmäßig wiederholt. Cell-Broadcast Nachrichten lösen spezielle Alarmtöne beim Endgerät aus, und enthalten textuelle und binäre Daten. Durch Verkettung von bis zu 15 sogenannten Pages von je 82 Byte (entsprechend 93 Textzeichen in der definierten Kodierung) können sie bis zu 1230 Byte (1395 Textzeichen) lang sein und so auch umfangreiche Informationen bereitstellen. Die Priorität bestimmt das Handling durch das Endgerät. Nachrichten der Priorität 1 können nicht durch Einstellung am Telefon unterdrückt werden. Zu den niedrig-priorenen Nachrichten gehört zum Beispiel der sogenannten Amber Alert, der ein Aufruf zur Mithilfe der Bevölkerung bei der Suche nach einer vermissten Person ist.

Die EU hat unter der Bezeichnung EU-Alert ein einheitliches Alarmierungsschema unter der Verwendung von SMS-CB definiert, und den Mitgliedsstaaten aufgegeben, dies bis 2022 einzuführen. Deutschland hat die Einführung nach den Erfahrungen aus der Flutkatastrophe im Sommer 2021 in Angriff genommen.

2.5.4 Mobile Datenübertragung

In dieser Erläuterung erfolgt eine Beschränkung auf den häufigsten Fall einer Datenverbindung: Die mobile Internet-Nutzung. Es wird dabei von einem im Netz angemeldeten mobilen Daten-Endgerät ausgegangen. Die Voraussetzungen für den Empfang und den Versand von Datenpaketen im Internet sind ein Anschluss an das globale Netz und die Zuordnung einer öffentlichen IP-Adresse. In Mobilfunknetzen gehören dazu neben der Teilnehmer-IMSI auch noch eine Reihe von netzinternen Adressen für das flexible Routing der Nutzdaten. Der Datentransport innerhalb des Mobilfunknetzes muss sich an die Ortsveränderungen der mobilen Endgeräte anpassen. Die Gesamtheit der Daten für die Datenverbindung eines mobilen Endgerätes wird als Packet Data Protocol-Kontext (PDP-Kontext) bezeichnet. Der PDP-Kontext repräsentiert eine Ende-zu-Ende Verbindung zwischen Endgerät und Übergang in ein Internet.

Hier kommt der, vielen Nutzern vertraute Access Point Name (APN) ins Spiel. Der APN ist ein Uniform Ressource Locator (URL), der auf der SIM-Karte des Teilnehmers gespeichert ist. Er bezeichnet die für den Teilnehmer vorgesehene Schnittstelle zum Internet oder zu anderen Datennetzen, zu der die Datenübertragung des Teilnehmers geroutet wird. Das Mobilfunknetz erzeugt den PDP-Kontext aus den unter der IMSI hinterlegten Teilnehmerdaten und dem APN. Tab. 2.3 zeigt einige APNs, die bei den deutschen Netzbetreibern gültig sind.

Der Ablauf ist wie folgt und in Abb. 2.11 dargestellt:

1. Das mobile Endgerät beantragt Zugriff auf das Netz zur Übermittlung von Kontroll-Nachrichten.
2. Die Basisstation bestätigt den Zugriff und vergibt Senderressourcen.

Tab. 2.3 Access Point Name (APN) deutscher Netzbetreiber

| Netzbetreiber | APN | Nutzung |
|--------------------------------|---------------------------|--|
| Deutsche Telekom (T-Mobile) | internet.telecom | Standard für Vertragskunden |
| | internet.t-mobile | Standard für Prepaid-Kunden |
| Vodafone | web.vodafone.de | Standard Vertrag und Prepaid |
| | home.vodafone.de | „Fixed Wireless Anschlüsse“ – Mobilfunk als DSL Ersatz |
| O2 | internet | Standard Vertragskunden |
| | pinternet. interkom.de | Standard Prepaid-Kunden |

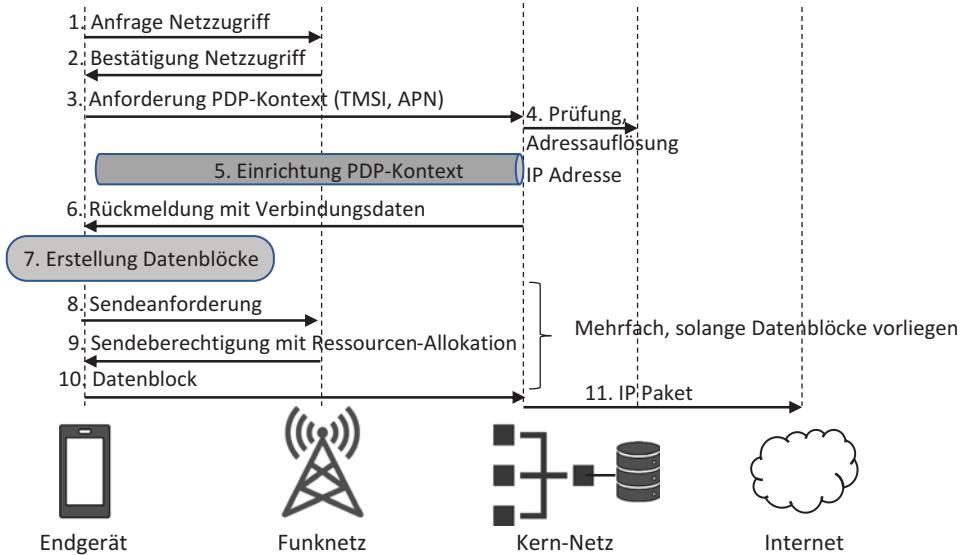


Abb. 2.11 Ablauf bei mobiler Datenübertragung

3. Das Endgerät fordert eine Datenverbindung an und überträgt dazu TMSI und APN.
4. Das Kern-Netz prüft mittels HSS-Abfrage die Berechtigung des Teilnehmers zum Datentransfer und identifiziert durch Adress-Auflösung die zum APN gehörige Internet-Schnittstelle.
5. Das Kern-Netz vergibt eine öffentliche IP-Adresse für das Endgerät und erzeugt den PDP-Kontext.
6. Die Rückmeldung über den erfolgten Verbindsaufbau wird an das Endgerät zurückgesandt.
7. Das Endgerät zerlegt die zu sendenden Daten in Blöcke, deren Größe von den Sendee- und Empfangsbedingungen abhängt.
8. Die Sendeberechtigung für jeden einzelnen Block wird bei der Basisstation beantragt.
9. Die Basisstation teilt den genauen Zeitpunkt und die Frequenzressourcen für die Sendung des Blocks mit.
10. Das Endgerät sendet den Datenblock. Die Schritte 7 bis 10 werden wiederholt, so lange noch Datenblöcke zur Übertragung anstehen.
11. Das Kern-Netz fügt die Blöcke an der Internet-Schnittstelle wieder zu IP-Paketen zusammen.

An der Schnittstelle zum Internet werden tarifliche Beschränkungen wie die maximale Datenrate oder das freie Datenvolumen eines Teilnehmers kontrolliert.

Bewegt sich das mobile Endgerät, ändert das Kern-Netz die Datenroute entsprechend. Die Schnittstelle zum Internet bleibt aber während der bestehenden Datenverbindung unverändert. Auch bei Datenverbindungen aus ausländischen Netzen erfolgt der Übergang

ins Internet immer aus dem Heimatnetz. Entsprechend wird die IP-Adresse, die dem mobilen Endgerät zugeordnet wird, immer aus dem Adressvorrat des Heimatnetzes vergeben. Abb. 2.11 zeigt die IP-Adresse eines mobilen Endgerätes aus Deutschland, das in einem niederländischen Netzwerk eingebucht war. Die Wiedergabe des Smartphone Displays zeigt das Gastnetz (Vodafone NL (1)), die vergebene öffentliche IP-Adresse (2), sowie unter (3) die zusätzlichen Daten, aus denen hervorgeht, dass die IP-Adresse zu einem deutschen Adress-Pool gehört (Abb. 2.12).

2.5.5 Handover (Übergabe) von Basisstation zu Basisstation

Die definierende Charakteristik eines Mobilfunknetzes ist, dass der Nutzer die Leistungen des Netzes ohne räumliche Beschränkung nutzen kann. Dazu gehört auch, dass sich Nutzer und Endgeräte während einer bestehenden Netzverbindung von einer Mobilfunkzelle zur nächsten bewegen können, ohne dass sie dadurch eine Service-Einschränkung erfahren oder der Dienst unterbrochen wird. Dies erfordert ein automatisches Handover des Endgerätes von einer Basisstation zu einer anderen, benachbarten Basisstation.

Während einer bestehenden Netzverbindung misst und registriert ein mobiles Endgerät die Empfangsstärke und Signalqualität der Basisstation, mit der es gerade verbunden ist, sowie gleichzeitig von allen anderen Basisstationen des gleichen Netzes, von denen es Signale empfängt. Diese Messwerte werden laufend an die verbundene Basisstation

Abb. 2.12 IP-Adresse eines mobilen Endgerätes



Ihre IP-Adresse lautet:

② **109.40.2.232**

Ihre IPv6-Adresse lautet:

nicht vorhanden ?

Ihre System-Informationen:

apple iOS 12.2 Mobile Safari 12.1

③

Deutschland

übermittelt. Ist das Signal von einer benachbarten Basisstation besser als das der aktuell verbundenen, erfolgt im Prinzip ein Handover. Ein Kanal zur neuen Basisstation wird aufgebaut, und die Verbindung mit der alten Basisstation wird gekappt. Dabei können jedoch vielfältige Probleme auftreten:

- Normale Signalschwankungen, wie beispielsweise durch das Passieren eines Hindernisses erzeugt, können zum Hin- und Herschalten zwischen Basisstationen führen.
- Daten, die während der Umschaltung übertragen werden, können verloren gehen.
- Die neue und die alte Verbindung können sich durch Überlagerung der Signale stark stören, so dass die Verbindung beeinträchtigt wird.
- Die neue Basisstation kann bereits mit zu vielen Endgeräten verbunden sein und muss die Übernahme ablehnen.
- Die neue Basisstation kann mit einem anderen Netzknoten im Kern-Netz verbunden sein, so dass beim Handover nicht nur die Basisstation gewechselt, sondern der gesamte Pfad bis ins öffentliche Telefonnetz oder ins Internet verändert werden muss.

Die genannten Handover-Probleme werden von der Technik nach den Abläufen und Vorschriften der definierten Standards automatisch gelöst. Eine Mitwirkung des Nutzers ist dabei nicht erforderlich.

Grundsätzlich gibt es verschiedene Anforderungen an einen Handover, die auch von dem Dienst abhängen, der vom Netz zur Verfügung gestellt wird.

- a. Es wird die Verbindung zur alten Basisstation abgebaut und das Endgerät meldet sich erneut am Netz an – dabei wird es sich automatisch mit der am besten positionierten Basisstation verbinden. Die bestehenden Verbindungen, gleich ob Sprache oder Daten, werden dabei allerdings verloren gehen.
- b. Der Handover erfolgt ohne Datenverlust, aber möglicherweise mit einer (kurzen) Unterbrechung einer bestehenden Verbindung.
- c. Der Handover erfolgt unterbrechungsfrei. Dies ist die aufwändigste Variante, die eine Beteiligung von Netzelementen bis in das Kern-Netz erfordert.

Handover werden in den verschiedenen Mobilfunktechnologien unterschiedlich durchgeführt. Auch haben sich die Anforderungen an das Netz über die Jahre und Jahrzehnte verändert. Für ein reines Sprachnetz, wie das GSM-Netz in den Anfangsjahren der digitalen Mobilkommunikation, ist beim Handover zwischen zwei Basisstationen unbedingt ein unterbrechungsfreier Dienst zu gewährleisten. Ein reines Datennetz, wie LTE seit 2010, legt dagegen stärkeres Gewicht auf die Vollständigkeit der empfangenen Daten.

2.5.6 Roaming

Der Begriff Roaming genießt in der Öffentlichkeit einen schlechten Ruf. Das hängt in erster Linie mit den zum Teil hohen Mobilfunk-Rechnungen nach einem Urlaubaufenthalt zusammen. Seit 2007 gab es in der Europäischen Union eine politische Diskussion zur Abschaffung oder zumindest Deckelung der innereuropäischen Roaming-Gebühren. Im Jahre 2017 wurde innerhalb der EU für Teilnehmer aus EU-Staaten die Erhebung von Roaming-Gebühren untersagt. Außerhalb der EU sind Roaming-Gebühren aber nach wie vor üblich.

Roaming ist unabhängig von der aktuell eingesetzten Mobilfunktechnologie. Daher soll an dieser Stelle eine kurze Darstellung erfolgen. Roaming ist eine der großen Errungenschaften des GSM-Standards von 1990. Roaming bedeutet „Herumwandern“ oder „Herumstreunen“. Gemeint ist die Möglichkeit, als Kunde eines nationalen Mobilfunknetzes bei einem Aufenthalt im Ausland ohne weiteren bürokratischen oder technischen Aufwand die Dienste eines dort ansässigen Netzbetreibers nutzen zu können. Die technischen Voraussetzungen für Roaming sind mit den internationalen Standards gegeben. Damit Roaming tatsächlich stattfinden kann, sind im Wesentlichen folgende Kriterien zu erfüllen

- Es muss ein Vertrag zwischen zwei Netzbetreibern geschlossen werden, der die Nutzungsmodalitäten und die Abrechnung regelt.
- Es muss eine Schnittstelle zwischen den beiden Netzen geben, über die Daten ausgetauscht werden können. Durch diese Schnittstelle fließen Signale und Nutzdaten (Sprache, Daten).
- Die Kern-Netze müssen Informationen über die Erreichbarkeit der Partner-Netze mit Roaming-Abkommen haben.

Roaming-Gebühren können im Grundsatz gerechtfertigt werden, weil neben dem Heimatnetz-Betreiber auch der Gastnetz-Betreiber Aufwände hat. Der Besucher nutzt die Netz-Ressourcen und die anfallenden Gebühren müssen erfasst und abgerechnet werden. Die Leitungen, die die Netze verbinden, sind meist Mietleitungen, für die anteilige Nutzungsentgelte anfallen.

Große Netzbetreiber haben Hunderte von Roaming-Abkommen und Schnittstellen. Kleine Netzbetreiber sind häufig Broker-Diensten angeschlossen, die die Vermittlung der Dienste übernehmen und als Clearing-Stelle für die Abrechnung dienen.

Folgende Standardsituationen treten beim Roaming auf:

1. Authentifizierung eines Teilnehmers bei Auslandsaufenthalt durch ein Gastnetz.

Bei der Anmeldung eines Mobilfunkteilnehmers an einem ausländischen Netz (Gastnetz) wird anhand der IMSI das Heimatland und das Heimatnetz identifiziert (Abb. 2.13). Das Gastnetz prüft, ob ein Roaming-Abkommen mit dem Heimatnetz besteht, und sendet die Authentifizierungs-Anfrage an das Heimatnetz. Die Authentifizierung erfolgt dann zwi-

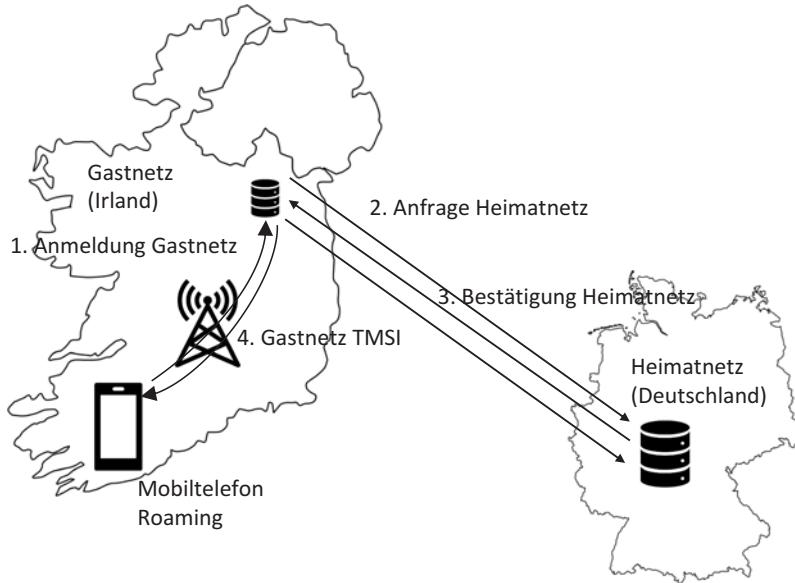


Abb. 2.13 Anmeldung im Gastnetz beim Roaming

schen Endgerät und Heimatnetz. Dabei ist das Gastnetz in die Kommunikation eingeschaltet. Nach erfolgter Authentifizierung erhält der Teilnehmer eine TMSI vom Gastnetz, die durch einen Netzwerk-Code ergänzt wird. Im HSS des Heimatnetzes ist registriert, dass der Teilnehmer sich im Gastnetz aufhält und welche TMSI ihm dort zugewiesen wurde.

2. Abgehender Sprachanruf im Gastnetz

Wählt der Teilnehmer im Gastnetz eine Rufnummer für ein Telefongespräch, so wird eine Anfrage nach der Berechtigung beim HSS des Heimatnetzes gestellt. Die Vermittlung des Gespräches zum Anruflziel erfolgt dann aber durch das Gastnetz.

3. Ankommender Sprachanruf für Roaming-Kunden im Heimatnetz

Ein ankommender Anruf für den Teilnehmer erreicht in jedem Fall zunächst sein Heimatnetz. Dort stellt sich bei der Abfrage des HSS heraus, dass der Teilnehmer im Gastnetz eingebucht ist. Das Gespräch wird daraufhin an das Gastnetz unter Nutzung der dort vergebenen TMSI weitervermittelt.

4. Datenverkehr im Gastnetz

Ein mobiles Endgerät, das vom Gastnetz aus auf Datendienste wie etwa das Internet zugreift, erreicht zunächst den Datendienst des Gastnetzes. Nach Autorisierung des Dienstes durch das Heimat-HSS wird der Datentunnel vom Gastnetz zum Heimatnetz und dort bis zur Internet-Schnittstelle aufgebaut.

2.6 Fragen

1. Wo sind die Daten über Aufenthaltsorte von Mobilfunkgeräten im Netz gespeichert?
2. Wie identifiziert ein Endgerät ein Netz, auf das es zugreifen kann?
3. Welche Kennung muss vom Endgerät an das Netz übersandt werden, um den Teilnehmer korrekt zu identifizieren?
4. Welches sind die wesentlichen Unterschiede zwischen SIM und USIM?
5. Wie hat die Einführung der SIM-Karte die Entwicklung des Gerätemarkts und der Geschäftsmodelle der Mobilfunkindustrie beeinflusst?
6. Unter welchen Umständen kann ein Mobilfunknetz ein gestohlenes oder verlorenes Endgerät erkennen?
7. Wie wird bei einem ankommenden Telefonanruf im Mobilfunknetz das angerufene Gerät geortet?
8. Was ist ein APN? In welcher Form liegt ein APN eines Teilnehmers vor?
9. Für eine Verbindung eines mobilen Endgerätes mit einem externen Datenserver wird eine IP-Adresse benötigt. Wer vergibt diese Adresse?
10. Ist die externe IP-Adresse eines Mobiltelefons ausschließlich diesem Gerät zugeteilt?
11. Erfolgt die Zuteilung der IP-Adresse an ein mobiles Endgerät auf Dauer?
12. Was ist ein PDP-Kontext? Beschreiben Sie die Art der beteiligten Information und die Nutzung.
13. Beschreiben Sie eine Situation, die auftreten könnte, wenn keine regelmäßigen Location Updates durchgeführt würden.
14. Unter welchen Bedingungen kommt es zu einem Handover eines mobilen Endgerätes von einer Basisstation zu einer anderen?
15. Lesen Sie sich das nachstehende Szenario durch und beantworten Sie im Anschluss die gestellten Fragen.

Frau A ist Vertriebsbeauftragte eines Unternehmens und reist von Deutschland aus zu einem Geschäftstermin in die Niederlande. Am Zielort angekommen möchte sie per Anruf im Büro in Deutschland noch einmal das letzte Update ihres Angebotes durchgehen. Die Kollegen im deutschen Büro klären eine abschließende offene Frage und rufen sie zurück. Herr B, ein Kollege, der am selben Tag auf Geschäftsreise in Spanien ist, ruft Frau A von dort aus an. Er teilt Frau A mit, dass er bei der Angebotspräsentation einen Fehler entdeckt hat, und erklärt, wie sie ihn beheben kann. Anschließend meldet sich Frau A mit ihrer frisch korrigierten Präsentation beim Kunden an. Nach dem Kundenmeeting verabredet sie sich telefonisch mit einem Kollegen aus ihrem Büro, der zufällig in der gleichen Stadt zu einem weiteren Kundengespräch ist, zu einem Erfahrungsaustausch.

- a. Was geschieht mit Frau As Mobilfunkverbindung beim Überschreiten der Grenze zu den Niederlanden?
 - b. Das Büro in Deutschland hat die (angenommene) Nummer 0211-7890. Welche Nummer wählt Frau A in den Niederlanden für den Anruf im Büro?
 - c. Unter welcher Rufnummer erreichen die Kollegen aus Deutschland Frau A in den Niederlanden? (Frau A hat die deutsche Mobilrufnummer 015674567891.)
 - d. Welche Rufnummer muss Herr B in Spanien wählen, um Frau A in den Niederlanden zu erreichen?
 - e. Muss Frau A eine internationale Vorwahl benutzen, um sich bei Ihrem Kunden vor Ort anzumelden?
 - f. Verwendet Frau A für die Kontaktaufnahme mit dem deutschen Kollegen eine internationale Vorwahl?
16. Informieren Sie sich im Internet, in der Presse oder Literatur zum Thema „nationales Roaming in Deutschland“. Was ist damit gemeint? Wie funktioniert es? Wie ist der Stand der Diskussion?

Literatur

Bundesnetzagentur (2021) Teilnehmerentwicklung im Mobilfunk. Bundesnetzagentur. Bonn. https://www.bundesnetzagentur.de/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Marktbeobachtung/Mobilfunkteilnehmer/artikel.html?nn=268232. Zugegriffen am 29.08.2021



Technische Grundlagen des Mobilfunks

3

3.1 Einführung und Lernziele

In diesem Kapitel sollen die wichtigsten physikalischen und technischen Grundlagen des Mobilfunks beschrieben werden. Für eine grundständige und umfassendere Auseinandersetzung mit dem Thema wird auf die einschlägigen Lehrbücher der Physik und Nachrichtentechnik verwiesen.

In den bisherigen Kapiteln wurde das Übertragungsmedium des Mobilfunks als gegeben vorausgesetzt. Die nun zu behandelnden Fragen sind

- Was sind elektromagnetische Wellen?
- Wie breiten sie sich aus?
- Wie werden sie mittels Antennen gezielt eingesetzt?
- Wie können Sprache und Daten mittels elektromagnetischer Wellen übermittelt werden?
- Wie wird eine zuverlässige Übermittlung durch Fehlerkorrektur-Verfahren erreicht?
- Wie können viele Sender und Empfänger gleichzeitig auf einen Frequenzbereich zugreifen?

► Lernziele

- Sie kennen die wichtigsten Kenngrößen elektromagnetischer Wellen.
- Sie wissen, welche Frequenzbereiche für die technische Nutzung in der drahtlosen Kommunikation Verwendung finden.
- Sie verstehen, wie elektromagnetische Wellen technisch erzeugt werden, wie sie durch Antennen ausgestrahlt und empfangen werden und wie sie sich im Raum ausbreiten.
- Sie kennen die Grundbegriffe Modulation, Multiplex und Fehlerkorrektur und verstehen, wie sie zur Datenübertragung eingesetzt werden.

3.2 Funksignale und Datenübertragung

Die Grundlage für jede drahtlose Übertragung sind die Erzeugung, Ausbreitung und der Empfang von elektromagnetischen Wellen. Die Erforschung des Elektromagnetismus war die entscheidende Grundlage für die Entwicklung der Kommunikationstechnologie und des Mobilfunks. Berühmte Wissenschaftler des 19. Jahrhunderts wie Michael Faraday (1791–1867), James Clerk Maxwell (1831–1879) und Heinrich Hertz (1857–1894) standen am Beginn der Entwicklung. In den folgenden Kapiteln wird die Übermittlung von Daten durch elektromagnetische Wellen beschrieben.

3.2.1 Elektromagnetische Wellen

Elektrische Felder werden durch elektrische Ladungen erzeugt. Wenn sich die Ladungsträger beschleunigt bewegen, entstehen zusätzlich magnetische Felder. Elektrische und magnetische Felder bedingen und beeinflussen sich gegenseitig; sie werden unter dem Begriff Elektromagnetismus zusammengefasst. Die elektrische Feldstärke, also die Stärke des elektrischen Feldes, wird in Volt pro Meter gemessen. Sie gibt an, welche Kraft das gegebene Feld auf einen Ladungsträger ausübt, der zur Messung in das Feld gebracht wurde. Die Richtung dieser Kraft wird durch die Feldlinien angegeben, mit denen das Feld üblicherweise visualisiert wird (Abb. 3.1). Das elektromagnetische Feld ist der Träger von Energie. Da es räumlich unbestimmt ist, wird statt der gesamten Energie die Energiedichte betrachtet, gemessen in Joule pro Kubikmeter. Die Energiedichte eines elektromagnetischen Feldes ist an jedem Ort proportional zum Quadrat der elektrischen Feldstärke.

Die Anregung eines elektromagnetischen Feldes durch Einbringen von zusätzlichen Ladungen oder durch Bewegung von Ladungen führt zur Entstehung und Ausbreitung von elektromagnetischen Wellen. Das entspricht der Entstehung und Ausbreitung von Wellen auf einer glatten Wasserfläche, in die ein Stein geworfen wird. Abb. 3.1 illustriert die Entstehung von elektromagnetischen Wellen an einem stromdurchflossenen Leiter. Ein Stab, wie in der Abb. 3.1 gezeigt, wird als *Dipol* bezeichnet, weil sich bei Anregung einer elektrischen Schwingung durch eine elektrische Wechselspannung phasenweise und im Wechsel an den Enden ein Plus- und ein Minuspol ausbilden. Nach dem Anlegen der elektri-

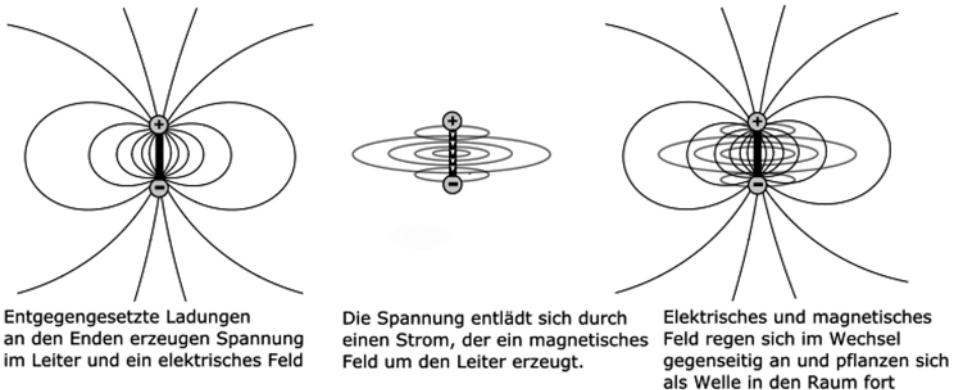


Abb. 3.1 Die Erzeugung elektromagnetischer Wellen

schen Spannungsquelle baut sich zwischen dem positiv geladenen und dem negativ geladenen Ende ein elektrisches Feld auf, das danach strebt, die Ladungsunterschiede durch einen Stromfluss auszugleichen (Abb. 3.1, links). Der dadurch einsetzende Strom vom positiven zum negativen Ende erzeugt ein Magnetfeld (Abb. 3.1, Mitte). Liegt am Leiter eine Spannungsquelle an, die regelmäßig wechselnd positive und negative Ladungen an den Enden erzeugt, wiederholt sich die Entstehung von sich abwechselnden elektrischen und magnetischen Feldern periodisch (Abb. 3.1, rechts). Die Felder breiten sich in den umgebenden Raum aus und pflanzen sich als Welle fort. Dabei ist noch zu unterscheiden zwischen dem Nahfeld, dem Bereich in der Nähe des Leiters, und dem Fernfeld. Erst dort kommt es zu einer freien Ausbreitung der Welle. Elektromagnetische Wellen üben ihrerseits eine Kraft, die *Lorentzkraft*, auf elektrische Ladungen aus. Durchdringen sie leitende Materialien, in denen die Ladungsträger beweglich sind, erzeugen sie dort umgekehrt wieder elektrische Ströme. Dieses von Michael Faraday entdeckte Phänomen wird als elektromagnetische Induktion bezeichnet. Induktion ist die Grundlage für Elektromotoren, Generatoren und Transformatoren, aber eben auch für die Datenübertragung. Im Nahfeld ist die Induktion eine Kopplung zwischen Sender und Empfänger mit Rückwirkung auf den Sender, was für manche Nahfeld-Kommunikationslösungen von Bedeutung ist.

Elektromagnetische Wellen benötigen, anders als etwa Schallwellen, kein Medium, in dem sie sich fortpflanzen. Die Ausbreitungsgeschwindigkeit elektromagnetischer Wellen wird allgemein Lichtgeschwindigkeit genannt und mit dem Buchstaben c bezeichnet. Der Name röhrt daher, dass diese Geschwindigkeit erstmals im Zusammenhang mit der Ausbreitung von Licht gemessen wurde. Die Lichtgeschwindigkeit beträgt im Vakuum ungefähr 300.000 km/s, durch Wechselwirkung mit Materie kann sie aber bei Durchgang durch Luft, Wasser oder Glas auch geringer sein.

Phänomene wie Radiowellen, Mikrowellen, Wärmestrahlung, Licht, Röntgenstrahlen und die radioaktiven Gamma-Strahlen sind elektromagnetische Wellen. Die wichtigste

Kenngröße zur Unterscheidung von elektromagnetischen Wellen ist ihre *Frequenz*, das ist die Anzahl der Schwingungen pro Zeiteinheit (meist Sekunde) am Ort eines Beobachters. Eine Schwingung ist dabei der Durchlauf eines Wellenberges und des folgenden Wellentales. Berge und Täler sind in diesem Zusammenhang aber lediglich Modellvorstellungen für die Wirkung des Feldes auf Ladungsträger. Die Frequenz wird in der Einheit Hertz (Hz) angegeben; 1 Hz bedeutet eine Schwingung pro Sekunde. Die Einheit Hz ist gleichbedeutend mit „pro Sekunde“, abgekürzt als 1/s. Die Frequenzen der in Natur und Technik vorkommenden elektromagnetischen Wellen werden in Zehnerpotenzen der Grundeinheit 1 Hz angegeben. Abb. 3.2 gibt einen Überblick. Häufig vorkommend sind

- Kiloherz (1 kHz = 1000 Hz = 10^3 Hz)
- Megahertz (1 MHz = 1.000.000 Hz = 10^6 Hz)
- Gigahertz (1 GHz = 1.000.000.000 Hz = 10^9 Hz)

Zum Beispiel unterscheiden sich die verschiedenen Farben des Lichtes allein durch ihre Frequenz.

Elektromagnetische Wellen werden üblicherweise in Form von Sinus-förmigen Wellen dargestellt (Abb. 3.3). Für die technische Verwendung von elektromagnetischen Wellen ist die Kenntnis einiger Größen wichtig:

- Die Wellenlänge ist der Abstand zwischen zwei aufeinander folgenden Wellenbergen. Sie wird mit dem griechischen Buchstaben Lambda (λ) bezeichnet. Zwischen Wellenlänge λ , Frequenz f und Lichtgeschwindigkeit c gibt es die einfache Beziehung $c = \lambda * f$. Beispielsweise beträgt die Wellenlänge eines FM-Radiosenders von ca. 100 MHz in etwa $(300.000.000 \text{ m/s})/(100.000.000 1/\text{s}) = 3 \text{ m}$. Für diese Rechnung wird die Lichtgeschwindigkeit in der Einheit m/s genutzt. Die Wellenlänge eines GSM-Mobilfunksenders (900 MHz) ist entsprechend etwa gleich $(300.000.000 \text{ m/s})/(900.000.000 1/\text{s}) = 0,33\text{m}$.

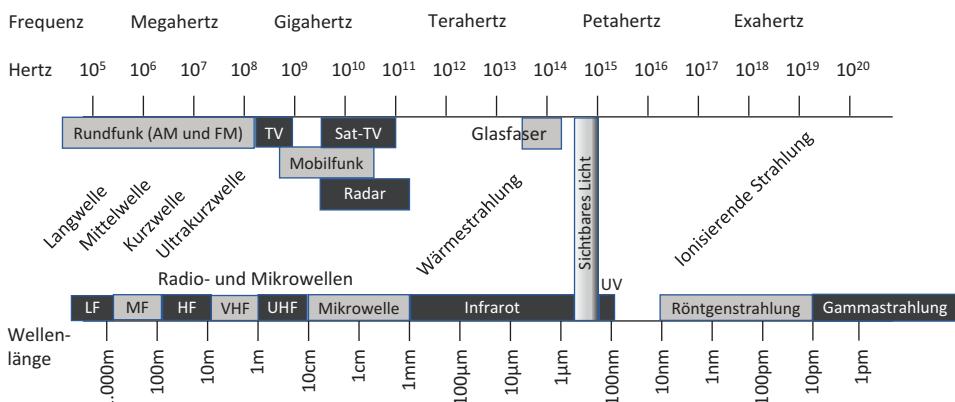


Abb. 3.2 Das elektromagnetische Spektrum mit traditionellen Bezeichnungen der Bereiche und technischen Anwendungen

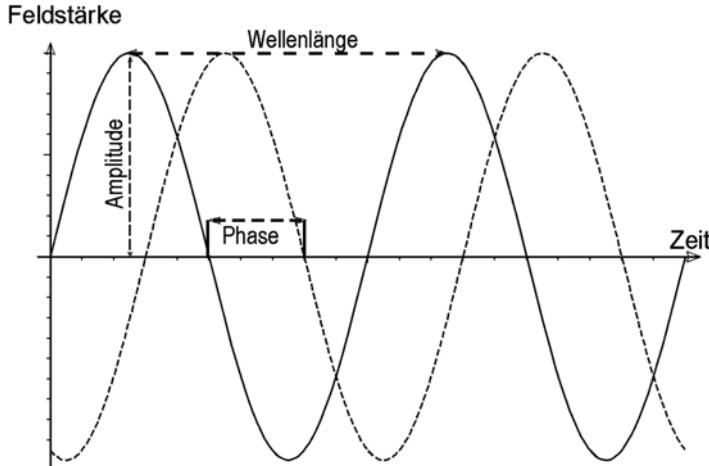


Abb. 3.3 Skizze einer elektromagnetischen Welle mit wichtigen Kenngrößen

- Die Amplitude ist der maximale Wert des Wellenausschlags (entsprechend der Höhe des Wellenberges über der Wasserfläche bei einer Wasserwelle). Der Wert der Amplitude ist die in Volt pro Meter gemessene elektrische Feldstärke E.
- Die Phase ist die relative Verschiebung von zwei Wellenzügen gegeneinander. Die gestrichelt gezeichnete Welle in Abb. 3.3 ist gegenüber der durchgezogen dargestellten Welle verschoben. Zwei Wellen mit gleicher Frequenz und Amplitude können sich bei unterschiedlicher Phase durch Addition sowohl verstärken als auch teilweise oder ganz auslöschen. Bei Schallwellen (die im Unterschied zu elektromagnetischen Wellen ein materielles Trägermedium wie Luft oder Wasser benötigen) wird dies zur Auslöschung von Umgebungslärm bei Kopfhörern sowie im Lautsprecherbau zur Trennung von Richtungsinformationen bei Stereosignalen aus einer Tonquelle genutzt. Im Mobilfunk werden Phasendifferenzen in vielfältiger Weise verwendet.

3.2.2 Die Ausbreitung von elektromagnetischen Wellen

Elektromagnetische Wellen transportieren Energie. Wie bereits in Abschn. 3.2.1 erläutert wird bei elektromagnetischen Feldern nicht die totale Energie des Feldes gemessen, sondern die Energiedichte, also die Verteilung der Energie auf das betrachtete Volumen. Die Einheit der Energie ist Joule. Damit ist die Energiedichte anzugeben in Joule pro Kubik(-zentimeter).

Leistung ist erzeugte oder verbrauchte Energie pro Zeiteinheit und wird in der Einheit Watt gemessen. Ein Watt ist definiert als 1 Joule pro Sekunde. Für das Joule hat sich daher auch die alternative Bezeichnung Wattsekunde mit den größeren Einheiten Kilowattstunde etc. eingebürgert. Eine Wattsekunde (Joule) entspricht der aufgewendeten oder

| | | | | | |
|------------------------------------|---|----|-----|-----|-------|
| E, Elektrische Feldstärke (V/m) | 1 | 5 | 10 | 50 | 100 |
| S, Intensität (mW/m ²) | 3 | 66 | 265 | 663 | 26525 |
| Dezibel (dBmW/m ²) | 4 | 18 | 24 | 38 | 44 |

Abb. 3.4 Elektrische Feldstärke und Intensität elektromagnetischer Wellen

verbrauchten Energie bei einer Leistung von 1 Watt während der Dauer von einer Sekunde. Der Transport von Energie durch Strahlung wird über die Flächenleistungsdichte gemessen. Sie ist der Quotient der durch eine senkrecht zur Ausbreitungsrichtung liegende Fläche strömende Energiemenge und der Größe der Fläche und wird oft auch als Intensität bezeichnet. Ihre Einheit ist Watt pro Quadratmeter. Der Begriff ist aus der Alltagssprache vertraut, und wird dort im gleichen Sinn verwendet: eine intensive Sonneneinstrahlung liefert eine hohe Leistung pro Flächeneinheit.

In der öffentlichen Diskussion werden häufig die Werte der elektrischen Feldstärke benutzt. Abb. 3.4 gibt für einige typische Feldstärkewerte die zugehörige Flächenleistungsdichte wieder. Die in der letzten Zeile angegebenen Dezibel-Werte werden im Abschn. 3.2.3 erläutert.

Wenn elektromagnetische Wellen sich gleichmäßig von der Quelle (Sender) in alle Richtungen ausbreiten, verteilt sich die Leistung P_0 des Senders auf die Oberfläche einer gedachten Kugel vom Radius d mit der Oberfläche $4\pi d^2$. Dies führt zu einem Abfall der Intensität mit dem Quadrat der Entfernung:

$$P_d = \frac{P_0}{4\pi d^2}$$

Als Beispiel wird in Abb. 3.5 ein Sender mit einer rundum gleichmäßig (isotrop) abgestrahlten Leistung von $P_0 = 500$ Watt betrachtet. Der Ausschnitt in dieser Abbildung zeigt einen Raumwinkel von etwa 0,5 sr (Steradian, Einheit des Raumwinkels). Dieser Raumwinkel schneidet 4 % der Fläche einer gedachten Kugel um den Sender aus ($0,5 \text{ sr}/4\pi$). Da die Abstrahlung gleichmäßig in alle Richtungen erfolgt, entfällt auf den gezeigten Ausschnitt 4 % der Gesamtleistung, also etwa 20 Watt. Der Ausschnitt wächst wie die Gesamtfläche der Kugel mit dem Quadrat der Entfernung, und ist in 100 m Entfernung auf 5000 m² angewachsen ($0,5 \text{ sr} * R^2$). Die Leistung von 20 Watt verteilt sich gleichmäßig auf diese Fläche und ergibt eine Intensität von $20 \text{ Watt}/5000 \text{ m}^2 = 0,004 \text{ W/m}^2$. In 300 m Entfernung verteilt sich die gleiche Leistung auf 45.000 m² mit einer Intensität von nur noch 0,00044 W/m².

Die vom Sender abgegebene Leistung schwächt sich also mit wachsender Entfernung sehr schnell ab. Daher senden Rundfunk- und Fernsehstationen, die Empfänger über viele Kilometer erreichen müssen, mit einer hohen Leistung, zum Beispiel mit 100 Kilowatt = 100.000 Watt. Die Sendeanlagen des Mobilfunks arbeiten dagegen mit Leistungen unter 20 Watt.

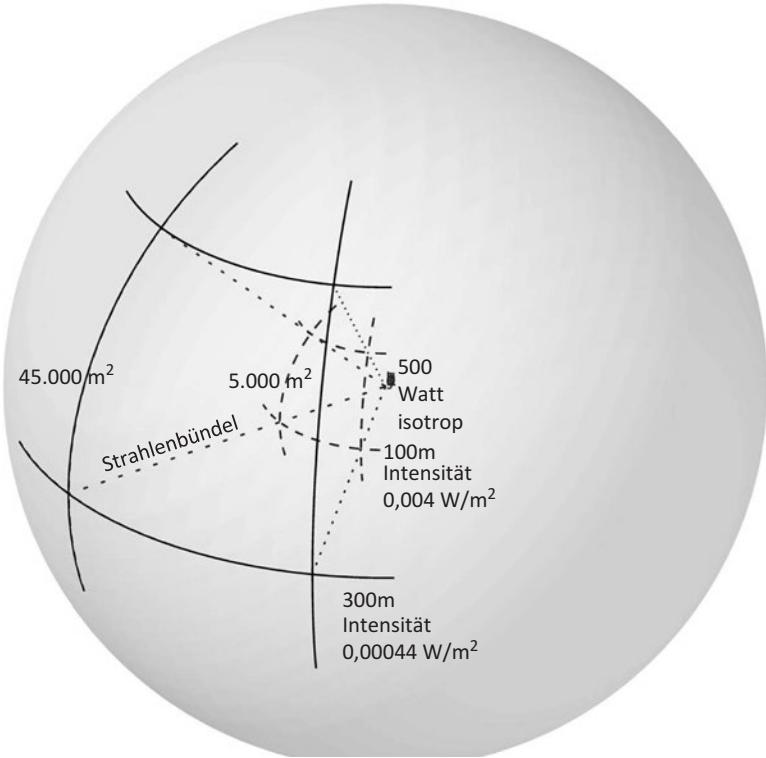
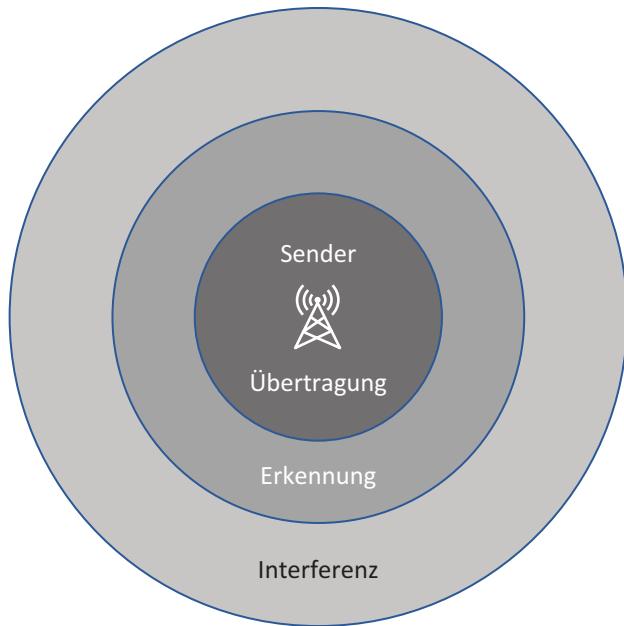


Abb. 3.5 Ausbreitung und Abschwächung einer elektromagnetischen Welle mit der Entfernung

Für Wellen im Frequenzbereich des heute genutzten Mobilfunks, die in Erdnähe abgestrahlt und empfangen werden, gibt es viele zusätzliche Effekte, die die Intensität beim Empfänger weiter beeinflussen. Es treten Reflexionen an glatten Flächen und Streuungen an rauen Flächen auf. Wenn die reflektierten und die direkten Wellen sich überlagern, kann es zu gegenseitiger Auslöschung kommen: Reflektierte Wellen haben einen etwas längeren Laufweg und kommen verzögert an einem Punkt an. Mit Blick auf Abb. 3.3 ist erkennbar, dass zwei Wellenzüge, die um eine halbe Wellenlänge verschoben sind, sich bei Überlagerung vollständig auslöschen. Hindernisse können zusätzlich einen Teil der Strahlung absorbieren und den dahinter liegenden Bereich abschatten. Das gilt insbesondere für Metallflächen und Objekte aus Materialien, die gebundenes Wasser enthalten.

Die Abschwächung der von einem Sender ausgehenden Wellen hat zur Folge, dass sie trotz prinzipiell unbegrenzter Ausbreitung nur in einem abgegrenzten Bereich für die Kommunikation nutzbar sind. Dieser Bereich wird als Übertragungsbereich bezeichnet. Hier ist die Intensität der elektromagnetischen Strahlung noch stark genug, um eine Interpretation der empfangenen Wellen durch einen Empfänger zu ermöglichen. Zusätzlich werden der Erkennungsbereich und der Interferenzbereich unterschieden (Abb. 3.6). Im Erkennungsbereich wird das Signal noch als solches erkannt, erlaubt aber keine

Abb. 3.6 Übertragungs-, Erkennungs- und Interferenzbereich bei elektromagnetischen Wellen



Kommunikation mehr. Im Interferenzbereich lässt sich das vom Sender ausgehende Signal nicht mehr erkennen. Es trägt aber noch zum allgemeinen Rauschen bei und stört damit andere Signalquellen und Kommunikationsbeziehungen. Die Darstellung in Abb. 3.6 mit konzentrischen Kreisen für die drei Bereiche bezieht sich auf die unbehinderte, in alle Richtungen gleichmäßige Ausbreitung im Raum, wie in diesem Kapitel generell angenommen. In der realen Welt durchmischen sich die Bereiche nahezu beliebig. In einer städtischen Umgebung kann durch die Abschattung der von einem Mobilfunksender ausgehenden Wellen durch ein Hochhaus ein Teil des Erkennungs- oder sogar Interferenzbereichs innerhalb des Übertragungsgebietes entstehen.

3.2.3 Antennen

Zum gezielten Senden und Empfangen von elektromagnetischen Wellen werden Antennen benötigt. Elektrisch leitende Materialien, wie zum Beispiel Metalle, die von elektromagnetischen Wellen durchdrungen werden, können als Antennen dienen. Ein *Dipol* wie in Abb. 3.1 gezeigt, ist die einfachste praktisch nutzbare Antenne. Wird er mit einer Stromquelle verbunden, die periodisch Stromstärke und Stromrichtung ändert, entstehen elektromagnetische Wellen, die durch den Raum wandern. In einem elektrischen Leiter, der von diesen Wellen durchdrungen wird, bilden die von der Lorentzkraft bewegten Elektronen einen periodisch veränderlichen Strom, der ein Abbild des erzeugenden Stromes im

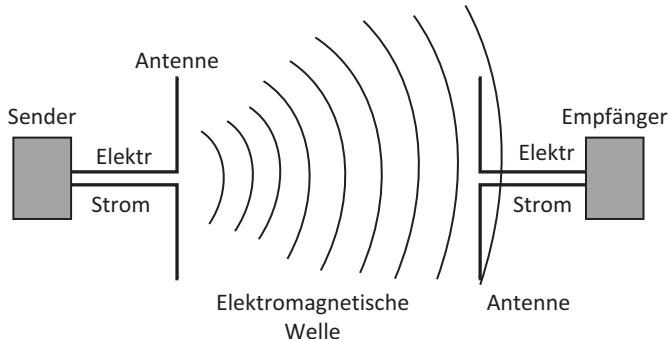


Abb. 3.7 Sende- und Empfangsvorgang mit Antennen

ersten Dipol ist. Dieser Strom kann von einem Schaltkreis aufgenommen und verarbeitet werden (Abb. 3.7).

Die empfangsbereite Antenne stellt der einfallenden Strahlung eine gedachte Fläche, die Wirkfläche oder Absorptionsfläche, entgegen, die durch elektromagnetische Induktion die Intensität der Strahlung in eine elektrische Leistung konvertiert: Das Produkt der Intensität S (W/m^2) und einer Fläche (m^2) ergibt eine Leistung P (W). In der Regel sind Antennen nicht sichtbar als Flächen gestaltet. Je nach Anwendungsfall haben sich unterschiedliche Konstruktionen und Formen herausgebildet. Sie reichen von Stabantennen auf Autodächern über TV-Antennen bis hin zu Parabolantennen für Satellitenfernsehen („Satellitenschüsseln“). Hier erfolgt eine Beschränkung der Betrachtung auf die im Mobilfunk genutzten Wellen, die im Bereich der Wellenlängen von 1 m bis 1 cm liegen (Frequenzen von 300 MHz bis 30 GHz). Die dafür technisch genutzten Antennen sind Dipole oder Gruppen von Dipolen.

Dipole und andere Antennen nehmen beim Empfang nicht die gesamte Energie der durchlaufenden Welle auf. Ein idealisierter Rundstrahler, der in alle Richtungen gleichmäßig abstrahlt und empfängt, hat bei der Wellenlänge λ eine Wirkfläche von $\frac{\lambda^2}{4\pi}$. Dieser

Faktor wird mit der Formel für die räumliche Abschwächung des Leistungsflusses zusammengefasst und ergibt die Friis-Formel (Friis 1946)

$$P_d = P_0 \left(\frac{\lambda}{4\pi d} \right)^2$$

für die in der Entfernung d von der Quelle in einem idealisierten Rundum-Empfänger empfangene elektrische Leistung. Das Beispiel aus Abb. 3.5 ergibt für eine Frequenz von 1 GHz (Wellenlänge 30 cm) in der Entfernung von 100 m die von einem Rundstrahler empfangene Leistung von 0,000028 Watt, also 28 Mikrowatt (Millionstel Watt). Die in der Funktechnik verwendeten Leistungsgrößen umfassen einen enormen Wertebereich: Von Sendeleistungen von bis zu 100.000 Watt bei großen Rundfunksendern bis zu empfange-

nen Leistungen von 100 Attowatt ($1 \text{ Attowatt} = 10^{-18} \text{ Watt}$) besteht ein Verhältnis von 21 Zehnerpotenzen.

Zur besseren Handhabung solcher sehr großen oder kleinen Größenverhältnisse wird in der Technik oft das *Dezibel* benutzt, ein Begriff, der den meisten Menschen aus der Akustik als Maß für die Lautstärke vertraut ist. Das Bel (Einheitenzeichen B) ist eine nach Alexander Graham Bell benannte Hilfsmaßeinheit zur Kennzeichnung des dekadischen Logarithmus des Verhältnisses zweier Größen der gleichen Art bei Pegeln und Maßen. Ein Verhältnis von 500 Watt Sendeleistung zu 28 Mikrowatt empfangener Leistung ($500/0,000028 \approx 18$ Millionen) wird vereinfachend aufgrund der Logarithmusfunktion als 72 Dezibel dargestellt, abkürzend als 72 dB. Eine Verdoppelung entspricht in der Dezibel-Terminologie einem Antennengewinn von 3 dB, eine Verstärkung um den Faktor 100 entspricht einem Antennengewinn von 20 dB. Abschwächungen werden durch negative Dezibel-Werte dargestellt. Mathematisch definiert wird der Dezibel-Wert des Verhältnisses von zwei Messgrößen A und B als

$$10 \log_{10} \frac{A}{B}$$

also dem 10-fachen des dekadischen Logarithmus dieses Verhältnisses. B stellt hier den Referenzwert dar, auf den Bezug genommen wird und der abhängig vom Anwendungsfall unterschiedlich definiert ist. Absolute Werte werden durch Dezibel dargestellt, indem sie ins Verhältnis zu dieser Referenzgröße gesetzt werden.

In der Akustik wird die Schallleistung von 10^{-12} W als Referenzwert verwendet. Ein Schall von 80 dB entspricht also einer gemessenen Schallleistung von 10^{-4} W .

In der Nachrichtentechnik ist das Dezibel mit Bezug auf die Leistung von 1 Milliwatt (Tausendstel Watt) gebräuchlich. Abkürzend wird es mit dBm bezeichnet. Der Dezibel-Milliwatt Wert einer Leistung von 500 Watt wie oben ist dann entsprechend

$$10 \frac{500 \text{ W}}{1 \text{ mW}} = 10 \frac{500.000 \text{ mW}}{1 \text{ mW}} = 10.500.000 \approx 10 * 5,6989 \approx 57 \text{ dBm}$$

Die 0,000028 Watt Empfangsleistung aus obigem Beispiel sind in Dezibel

$$10 \frac{0,000028 \text{ W}}{1 \text{ mW}} = 10 \frac{0,028 \text{ mW}}{1 \text{ mW}} = 100,028 \approx 10 * (-1,5528) \approx -15 \text{ dBm}$$

Dabei zu beachten ist, dass negative Dezibel-Werte lediglich bedeuten, dass der Messwert kleiner als der Referenzwert ist. Die Differenz $57 \text{ dBm} - (-15 \text{ dBm}) = 72 \text{ dBm}$ entspricht genau dem Verhältnis der gesendeten Leistung von 500 Watt zur errechneten Empfangsleistung: Anstatt Multiplikation oder Division der Originalwerte werden die entsprechenden Dezibel-Werte einfach addiert oder subtrahiert.

Durch technische Konstruktionen wird versucht, einen hohen Wirkungsgrad einer Antenne zu erreichen. Dies gelingt jedoch immer nur in einer bevorzugten Richtung. Eine Antenne ist eine passive Einrichtung und kein Verstärker. Je stärker die Antenne in der bevorzugten Richtung abstrahlt oder empfängt, desto enger wird der Sektor, in dem sie

wirksam ist (Winkelausschnitt der Abstrahlung). Der *Antennengewinn* G ist der Faktor, um den der Wirkungsgrad einer technischen Antenne gegenüber dem idealisierten, isotropen Rundum-Sender oder -Empfänger in der Vorzugsrichtung erhöht ist. Antennengewinn und Richtwirkung stehen in einem umgekehrt proportionalen Verhältnis zueinander. Ein Antennengewinn von G bedeutet, dass die abgestrahlte Leistung in einem Teil von 1/G des vollen Raumwinkels erfolgt. Je höher der Antennengewinn, desto enger ist die abgestrahlte Leistung gebündelt. Der Antennengewinn wird oft auch in Dezibel angegeben. Die Referenz ist dabei der idealisierte Rundstrahler. Die Angabe eines Antennengewinns erfolgt mit dem Zusatzbuchstaben „i“, also als dBi. Das i steht für das Adjektiv *isotrop*, gleichmäßig in alle Richtungen.

Beim Dipol bilden sich bei der Abstrahlung sogenannte stehende Wellen aus: regelmäßige Verteilungen von Spannung und Stromstärke mit Bäuchen (hohe Werte) und Nulldurchgängen (niedrige Werte). An den Enden liegt bei der Stromverteilung immer ein Knotenpunkt (Nullwert), denn die Elektronen können ja nicht weiter strömen. Je höher die Ausschläge, desto stärker ist Beschleunigung der Ladungsträger im Strom und damit die entstehende Welle. Abb. 3.8 illustriert, dass der maximale Ausschlag dann erreicht wird, wenn es nur die beiden Knotenpunkte an den Enden gibt. Die optimale Länge einer Dipolantenne ist also gleich der halben Wellenlänge ($\lambda/2$).

Die Ausstrahlung und der Empfang eines $\lambda/2$ -Dipols sind am größten in der Richtung senkrecht zum Antennenstab. Bei einem Winkel von 39 Grad zur Senkrechten auf den Antennenstab fällt die Intensität auf den halben Wert, und in Stabrichtung ist sie gleich Null. Der Antennengewinn des $\lambda/2$ -Dipols ist $G=1,64$ bzw. $2,15 \text{ dBi}$, und die Wirkfläche

$$\text{bei einer Wellenlänge } \lambda \text{ ist } A_w = G \frac{\lambda^2}{4\pi} = \frac{\lambda^2}{7,7} \text{ (Wiesbeck 2005).}$$

Eine Welle der Frequenz 1 GHz hat eine Wellenlänge von ca. 30 cm, und damit eine optimale Dipol-Antennenlänge von ca. 15 cm. In einem mobilen Endgerät ist in der Regel ein einfacher Stab oder Draht mit $1/4$ Wellenlänge (also $\lambda/4$) als Antenne verbaut, der zusammen mit dem Anschlusskabel den Halbwellen-Dipol „simuliert“. Ein größerer Antennengewinn beim Endgerät ist nicht sinnvoll, denn wegen des damit verbundenen kleineren Abstrahlwinkels müsste der Nutzer mit seinem Gerät dann ständig auf die Basisstation „zielen“.

Die Antennen der Basisstationen sind in den rechteckigen Kästen enthalten, die an Mobilfunktürmen zu sehen sind (Abb. 2.1 und 3.9). Den Aufbau einer Mobilfunkantenne zeigt Abb. 3.9. Im rechteckigen Gehäuse befinden sich an der Rückwand montierte Di-

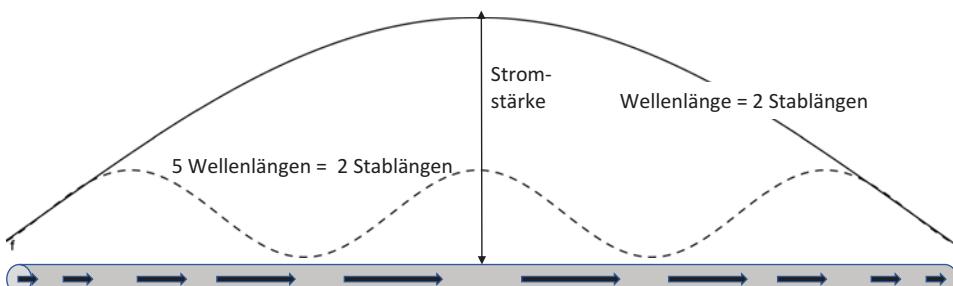


Abb. 3.8 Stehende Wellen am Dipol

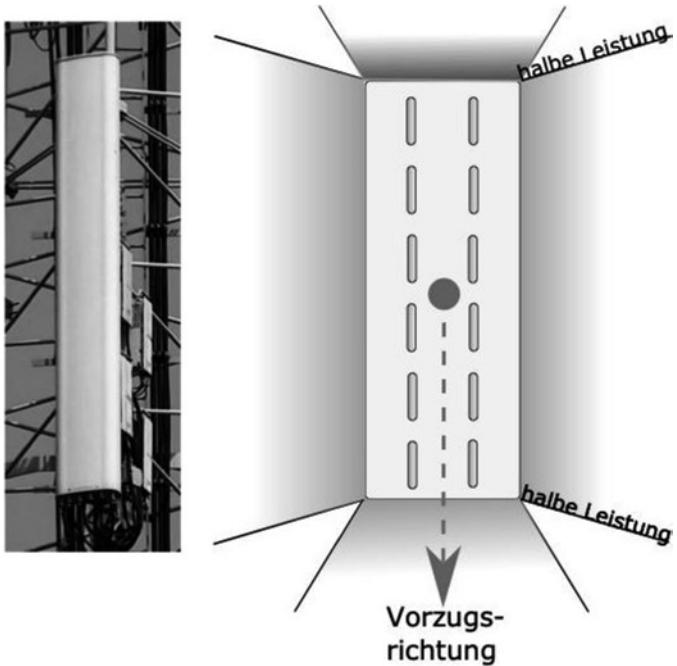
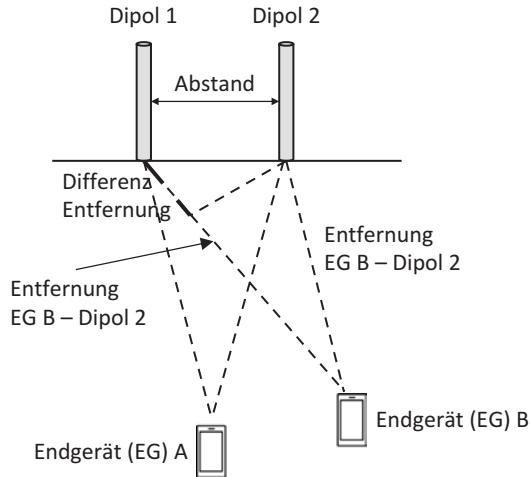


Abb. 3.9 Aufbau einer Mobilfunkantenne

pole, die in einem rechteckigen Schema angeordnet sind. Die Rückwand besteht aus einem Material, das Mikrowellen reflektiert. Solche Antennen werden als *Gruppenantennen* bezeichnet. Die Anzahl der Dipole, ihre Anordnung und ihre Abstände im Verhältnis zur ausgestrahlten Frequenz bestimmen den Abstrahlwinkel und den Antennengewinn. In der Hauptstrahlrichtung ist der Antennengewinn einer Gruppe angenähert die Summe der Antennengewinne der Einzelstrahler. Eine reflektierende Rückwand verdoppelt den Antennengewinn nochmals. Im dargestellten Beispiel berechnet sich der Antennengewinn als Produkt aus 2 (Reflektion an der Rückwand), 12 (Anzahl Dipole) und 1,64 (Antennengewinn Dipol) zu 40 oder in Dezibel ausgedrückt gleich 16 dBi. Bei 30 Grad seitlicher und 8,5 Grad senkrechter Abweichung von der nach vorn gerichteten Hauptstrahlrichtung ist die Abstrahlleistung auf die Hälfte abgefallen. Insgesamt überdeckt dieser Antennentyp einen horizontalen Sektor von 120 Grad, so dass drei solcher Antennen benötigt werden, um die Umgebung des Standortes mit Funksignalen abzudecken.

Abb. 3.10 erläutert das Wirkungsprinzip einer Gruppenantenne am Beispiel von zwei parallel angeordneten Dipolen. Das senkrecht vor der Antennenebene befindliche Endgerät EG A hat von beiden Dipolen die gleiche Entfernung. Werden die Dipole mit identischen elektrischen Schwingungen gespeist, treffen bei EG A zwei identische Wellenzüge ein, die sich verstärkend überlagern. Für Endgerät EG B ist Dipol 2 um die markierte Differenz-Entfernung näher als Dipol 1. Um diese Strecke ist die Welle von Dipol 1 ge-

Abb. 3.10 Wegunterschiede der Wellen von verschiedenen Dipolen führen zu Richtwirkung der Antenne



genüber der von Dipol 2 verschoben. In der Überlagerung ergibt sich daraus eine Abschwächung, die bei passendem Winkel bis zur gegenseitigen Auslöschung der Wellenzüge geht.

Die Empfangs- und die Sendewirkung einer Antenne sind völlig symmetrisch. Ein Gewinn von 16 dBi gilt genauso für die Empfangsleistung; die entsprechende Antenne wird in der Hauptrichtung um diesen Faktor empfindlicher und unterdrückt gleichzeitig seitlich einfallende Wellen.

3.2.4 Reichweite und Abdeckungsbereich einer Funkzelle

Mit Hilfe des Antennengewinns ist es möglich, eine ungefähre Aussage über die Größe einer Mobilfunkzelle zu treffen. Ein von einem Sender ausgehendes Signal kann von einem entfernt platzierten Gerät dann empfangen werden, wenn die dort eintreffende Leistung größer als die Empfindlichkeit des Empfängers ist. Die in Dezibel gemessene Differenz zwischen Ausgangsleistung und Empfänger-Empfindlichkeit bestimmt den maximalen Dämpfungswert, der in der Literatur auch als Pfadverlust bezeichnet wird. Der Pfadverlust hängt wie beim Friis-Modell von der Entfernung zum Sender ab. Für das Friis-Modell der freien Ausbreitung im Raum ergibt sich bei 1 GHz Frequenz (Wellenlänge ca. 30 cm) aus der Formel in Abschn. 3.2.3 die Dämpfung im Abstand d km in Dezibel

$$L = 86 + 20d$$

Die freie Ausbreitung im Raum ist für ein landgestütztes Mobilfunknetz nicht gegeben. Abschattungen durch natürliche Objekte und Bauten sowie Reflexionen mit Überlagerung der reflektierten Wellen führen zu zusätzlichen Ausbreitungsverlusten. Es gibt eine Reihe von Formeln, die die Dämpfung unter *realistischen* Bedingungen modellieren (European Commission 1999). Sie haben alle die Form

$$L = a + 10nd$$

Dabei ist die Größe a je nach Modell abhängig von Faktoren wie der Wellenlänge, der Höhe des Senders oder der Antenne über Grund, sowie von der Landschaftsform und der Bebauungsdichte. Der *Ausbreitungskoeffizient* n hängt vorwiegend von Wellenlänge und Antennenhöhe ab. Typische Werte für a liegen für 1 GHz Frequenz bei 120 dB; in den meisten Fällen liegt der Wert von n zwischen $n = 3$ und $n = 4$ (im Vergleich zu $n = 2$ beim Friis-Modell).

Die Empfindlichkeit des Empfängers wird wesentlich bestimmt durch das von Molekülschwingungen erzeugte Rauschen. Rauschen hängt von der Temperatur und der Bandbreite des Signals ab. Für eine elektromagnetische Welle mit 1 MHz Bandbreite ist der Wert unter normalen Temperaturbedingungen (300 K = 27 Grad C) gleich -114 dBm. Unter Berücksichtigung von Eigenrauschen und gegenseitiger Beeinflussung von Sendern ergibt sich der Systemgewinn wie in der nachstehenden Abb. 3.11. Dabei muss immer vom leistungsschwächeren Gerät ausgegangen werden, in diesem Fall also vom Endgerät.

Abb. 3.12 zeigt den Verlauf der entfernungsabhängigen Dämpfung, der empfangenen Leistung und des sich ergebenden Signal-Rauschabstands auf der Basis der Daten aus Abb. 3.11. Dabei wurden reale Dämpfungswerte in einer städtischen Umgebung zugrunde gelegt ($a = 120$, $n = 3,7$). Die Werte beziehen sich auf ein Endgerät im Freien; in Innenräumen ergeben sich nochmals deutlich höhere Dämpfungswerte. Bei einem Rauschabstand von 0 dB wird die Basisstation Schwierigkeiten haben, das vom Endgerät ausgehende Signal noch zu verarbeiten.

Abb. 3.13 illustriert schließlich die Gesamtsituation der Kommunikation zwischen der Basisstation und dem Endgerät. Vom Leistungsverstärker der Basisstation wird das elektrische Signal durch Kabel zur Antenne übertragen, von wo es in der Hauptstrahlrichtung verstärkt als Welle ausgesandt wird. Die hier verwendete Abschwächung der Leistung von 120 Dezibel entspricht dem Wert aus Abb. 3.12 in der Entfernung von 1 km. Durch die Antenne des mobilen Endgerätes wird das Signal in elektrische Schwingungen verwandelt und an die Elektronik zur Verarbeitung weitergegeben. In der umgekehrten Richtung vom Endgerät zur Basisstation erfolgt die Verstärkung durch die Antenne im Endgerät. Die

| | | | |
|---|----------------------------|----------|---|
| 1 | Ausgangsleistung | 23 dBm | Standard-Wert für Endgeräte |
| 2 | Thermodynamisches Rauschen | -114 dBm | Physikalische Konstante, 1 MHz Bandbreite, 300 K Temperatur |
| 3 | Empfänger-Rauschen | 5 dB | Angenommener Wert |
| 4 | Störungen, Interferenz | 2 dB | Angenommener Wert |
| 5 | Gesamtwert Rauschen | -107 dBm | (2) + (3) + (4) |
| 6 | Antennengewinn Empfänger | 15 dB | Standard für Mobilfunk-Antenne |
| 7 | Systemgewinn | 145 dB | (1) - (5) + (6) |

Abb. 3.11 Typische Berechnung Systemgewinn

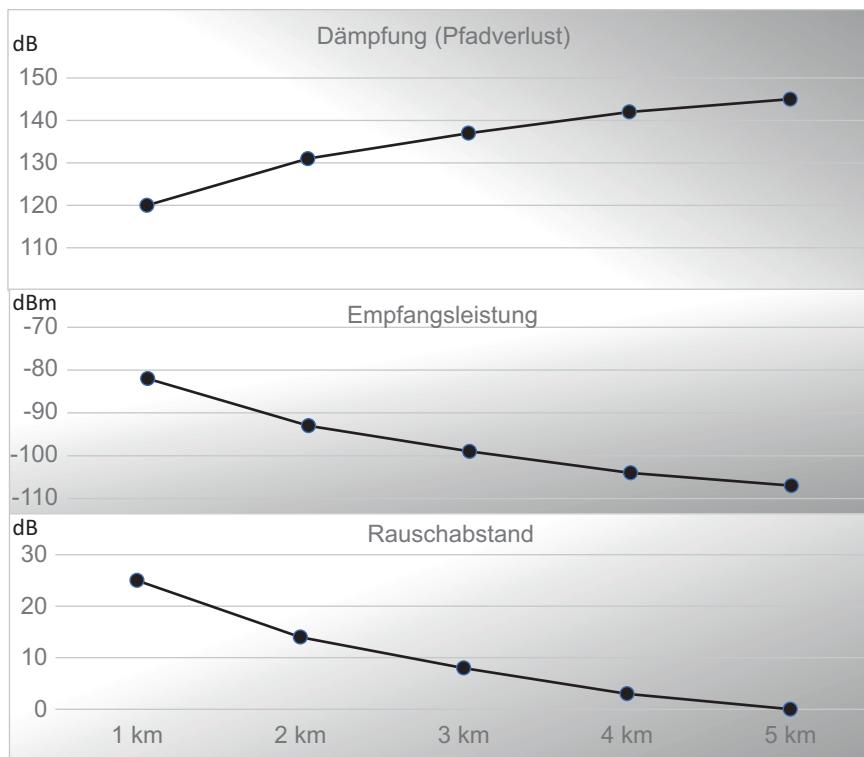


Abb. 3.12 Dämpfungswerte, empfangene Leistung und Signal-Rauschabstand in Dezibel-Milliwatt oder Dezibel in Abhängigkeit von der Entfernung

vom Endgerät ausgehenden Wellen unterliegen demselben Dämpfungsverlust wie diejenigen von der Basisstation. Verstärkt durch den Antennengewinn erreicht das Signal schließlich die Elektronik der Basisstation. Das Niveau des Rauschens in der Illustration entspricht der Tabelle in Abb. 3.11.

Die „Reichweite“ einer Basisstation wird bestimmt durch die Sendeleistung der verbundenen mobilen Endgeräte, deren maximale Leistung 20 dB unterhalb der von Basisstationen liegt. Solange die Wellen des Endgerätes die Basisstation mit einer Leistung oberhalb des Rauschniveaus erreichen, kann die Leistung der Basisstation entsprechend angepasst werden.

3.2.5 Bewegte Objekte und der Doppler Effekt

Elektromagnetische Wellen, die von bewegten Objekten wie mobilen Endgeräten ausgesandt oder von ihnen empfangen werden unterliegen dem Doppler-Effekt. Es handelt sich um eine Frequenzverschiebung, die oft im Bereich der Schallwellen demonstriert wird:

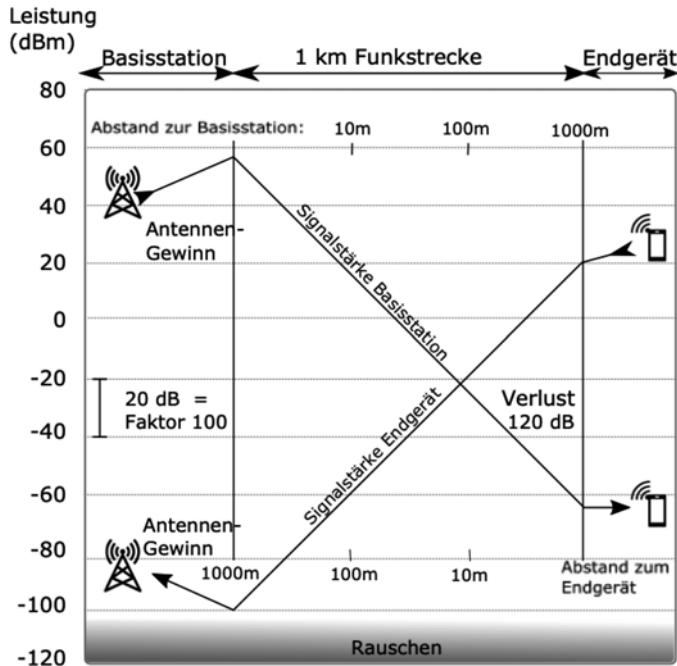


Abb. 3.13 Typischer Leistungsverlauf der Wellen zwischen Basisstation und Endgerät

Ein Polizeifahrzeug oder Krankenwagen fährt auf einen Beobachter zu, passiert ihn und entfernt sich wieder. Während der Anfahrt ist der Ton erhöht; im Augenblick des Passierens fällt die Tonhöhe deutlich ab und der Ton bleibt tief, solange das Fahrzeug sich entfernt. Die akustische Tonhöhe entspricht der Frequenz der Schallwelle. Das gleiche Phänomen tritt bei elektromagnetischen Wellen auf. Bewegt sich die Quelle auf den Empfänger zu, verschiebt sich die beim Empfänger gemessene Frequenz nach oben; entfernt sich die Quelle vom Empfänger, erfolgt eine Verschiebung zu niedrigeren Frequenzen. Der Doppler-Effekt kann anschaulich so erklärt werden, dass durch die relative Bewegung von Sender und Empfänger die Folge der beim Empfänger eintreffenden Wellenberge gestaucht beziehungsweise gedehnt wird. Damit treffen bei Annäherung mehr Wellenberge pro Zeiteinheit am Empfänger ein, bei Entfernung treffen umgekehrt weniger Wellenberge pro Zeiteinheit ein.

Bei hohen Geschwindigkeiten zwischen Sender und Empfänger kann die Frequenzverschiebung durch den Doppler-Effekt so stark sein, dass das empfangene Signal nicht mehr verarbeitet werden kann. Daher gibt es für Mobilfunknetze Grenzen für die unterstützte Geschwindigkeit. Dabei handelt es sich immer um die zulässige Geschwindigkeit der Endgeräte, da die Basisstationen ortsfest sind. Der 2G Standard GSM erlaubte eine Geschwindigkeit des Endgerätes von bis zu 250 km/h. Der neue 5G Standard ist für Endgeräte-Geschwindigkeiten von bis zu 500 km/h definiert.

3.3 Datenübertragung durch elektromagnetische Wellen

Die Übermittlung von Daten über Distanzen war eine der ersten Anwendungen der neu entdeckten elektromagnetischen Wellen. Guglielmo Marconi nutzte im Jahre 1901 die von Heinrich Hertz experimentell bestätigten Wellen zur drahtlosen Übertragung von Morsezeichen über den Atlantik. In der Weiterentwicklung gab es ab 1920 erste Rundfunkstationen und seit den 1930er-Jahren erste Fernseh-Übertragungen. Parallel dazu entwickelte sich auch die drahtlose Telefonie (Kap. 4).

Zur Übertragung von Sprache, Bildern und Daten durch elektromagnetische Wellen sind verschiedene Aufgaben zu bewältigen.

- Modulation: Bei einer Übertragung werden letztlich elektromagnetische Wellen gesendet und empfangen. Mittels Modulation wird das zu übertragende Nutzsignal in eine elektromagnetische Welle verwandelt.
- Kodierung und Fehlerkorrektur: Elektromagnetische Wellen werden auf dem Weg durch Umgebungseinflüsse verändert. Da der Empfänger das Nutzsignal aus der empfangenen Welle interpretieren muss, kommt es hier zu Fehlern. Kodierung verändert das Nutzsignal vor der Aussendung, um die Fehlerwahrscheinlichkeit zu senken; effiziente Fehlerkorrekturalgorithmen sorgen für die Behebung von Fehlern, die dennoch auftreten.
- Netzzugriff: In der Regel werden elektromagnetische Übertragungsressourcen von vielen Geräten gleichzeitig genutzt. Regeln und Verfahren des Netzzugriffs ermöglichen die gleichzeitige Nutzung und sorgen für eine faire Verteilung der vorhandenen Kapazitäten

Das Thema Sicherheit und Vertraulichkeit wird in Kap. 9 angeschnitten.

3.3.1 Modulation

Über einen metallischen Leiter lässt sich ein kontinuierlich verändertes Eingangssignal, wie etwa die über ein Mikrofon in elektrischen Strom verwandelten Schwingungen der menschlichen Stimme direkt und unmittelbar übertragen und auf der Empfangsseite einem Lautsprecher zuführen. Diese Art von *Basisband-Übertragung* funktioniert für Rundfunk, Fernsehen und drahtlose Kommunikation mit vielen Teilnehmern nicht mehr. Die Signale befinden sich alle im selben Frequenzbereich und würden sich bis zur Unkenntlichkeit überlagern und mischen. Datenübertragung wäre so nur äußerst eingeschränkt möglich.

3.3.1.1 Grundprinzipien der Modulation

Zur Lösung dieses Problems wird auf Wellen mit höheren Frequenzen ausgewichen, denen die zu übertragenden Daten (Nutzsignal) aufgeprägt werden: Eine elektromagnetische

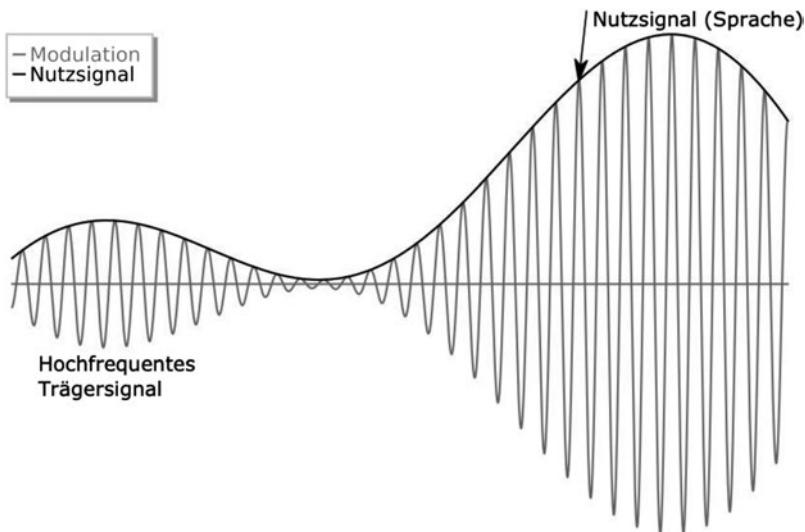


Abb. 3.14 Amplitudenmodulation

Welle gegebener Frequenz (Trägersignal) wird durch das Nutzsignal technisch so verändert, dass der Empfänger das empfangene Signal wieder in Trägersignal und Nutzsignal zerlegen kann. Die Bezeichnung für diesen Vorgang ist *Modulation*. Als Beispiel wird die schon seit über 100 Jahren bekannte *Amplitudenmodulation* betrachtet (Abb. 3.14). Dabei wird die Amplitude einer hochfrequenten Schwingung mit der Amplitude des Nutzsignals multipliziert. Die durch die Antenne ausgesandte Welle erzeugt in der Empfangsan天ne eine gleichartige Welle, die allerdings sehr viel schwächer ist. Auf der Empfangsseite werden durch eine einfache elektronische Filter-Schaltung die hohen von den niedrigen Frequenzen getrennt („Tiefpass“), so dass die ursprüngliche Schwingung als Kurve erhalten wird.

Amplitudenmodulation ist sehr einfach zu realisieren, hat aber gravierende Beschränkungen mit Bezug auf die Übertragungsqualität. So muss aus technischen Gründen die Amplitude des Nutzsignals immer strikt kleiner sein als die Amplitude des nicht modulierten Trägersignals. Für Rundfunkübertragungen wurde die Amplitudenmodulation deshalb abgelöst durch die leistungsfähigere Frequenzmodulation.

Abb. 3.15 stellt das Prinzip der Modulation schematisch dar. Der *Modulator* kombiniert das Nutzsignal mit einem selbst erzeugten oder zugeführten hochfrequenten Signal, dem Träger. Da es sich beim Träger ebenfalls um eine elektromagnetische Welle handelt, wird von der Trägerwelle gesprochen und ihre Frequenz als Trägerfrequenz bezeichnet. Das kombinierte hochfrequente Signal wird als elektromagnetische Welle übertragen. Auf der Empfangsseite trennt der *Demodulator* den hochfrequenten Anteil ab und gewinnt so das Nutzsignal zurück. Aus der Wortpaarung Modulator/Demodulator entstand der heute noch gebräuchliche Begriff *Modem*. In Abb. 3.15 wird noch einmal Bezug auf die oben dargestellte Amplitudenmodulation genommen. Es können aber auch andere Wellenparameter (Abb. 3.3) wie Frequenz oder Phase durch die Modulation beeinflusst werden.

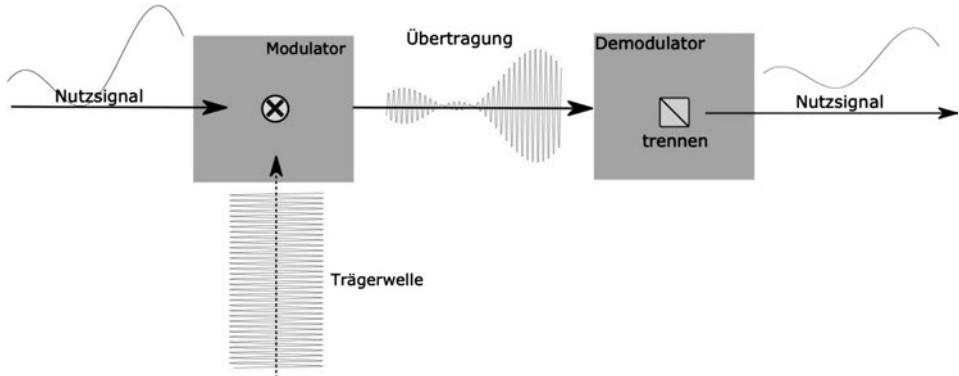


Abb. 3.15 Prinzip-Darstellung der Datenübertragung durch Modulation von Wellen

Im Falle der *analogen Modulation* ist das Nutzsignal ein sich kontinuierlich veränderndes Signal, wie etwa die laufenden Schallpegel bei einer Sprach- oder Musikübertragung. Analoge Modulation wird heute noch verbreitet für die Rundfunkübertragung angewendet.

3.3.1.2 Digitale Modulation

Die *digitale Modulation*, also die Übermittlung von digitalen (binären) Daten, muss den Umstand berücksichtigen, dass die übertragenen Daten als diskrete Werte, also zum Beispiel als Bits vorliegen. Die digitale Modulation ist gleichzeitig *wertdiskret* und *zeitdiskret*. Die Zeit wird in kleine Abschnitte unterteilt. Jedem Abschnitt wird ein zu übertragender Wert aus einem vorgegebenen Wertevorrat zugeordnet. Dabei handelt es sich im einfachsten Fall um ein Bit (Wertevorrat 0 und 1); bei modernen Verfahren allerdings meist um eine Gruppe von Bits. Dieser Wert wird durch eine Wellenform dargestellt. Eine Wellenform wird durch bestimmte Wellenparameter (Frequenz, Amplitude, Phase, ...) festgelegt und wird während des Zeitabschnittes laufend ausgesendet. Die Kombination von Zeitabschnitt, Wert und Wellenform wird als *Symbol* bezeichnet. Es ist von entscheidender Bedeutung, dass das Symbol vom Empfänger aus der empfangenen Wellenform identifiziert werden kann. Die Wellenformen müssen also einen hohen Wiedererkennungswert besitzen. Ihre Optimierung ist seit langem Gegenstand der Forschung. Internationale Telekommunikationsstandards wie GSM oder LTE regeln auf der Basis der wissenschaftlichen Erkenntnisse im Detail, wie die Welle während eines Zeitabschnittes für einen bestimmten Wert auszusehen hat. Nachfolgend werden die wichtigsten Methoden der digitalen Modulation etwas genauer vorgestellt.

3.3.1.3 Digitale Amplitudenmodulation

In Abb. 3.16 wird *Digitale Amplitudenmodulation* zur Darstellung einzelner Bits verwendet. Die Bit-Werte 0 und 1 werden durch verschiedene Werte der Amplitude dargestellt. Einfaches An- und Abschalten als Information der Gegenseite über das gerade übertragene

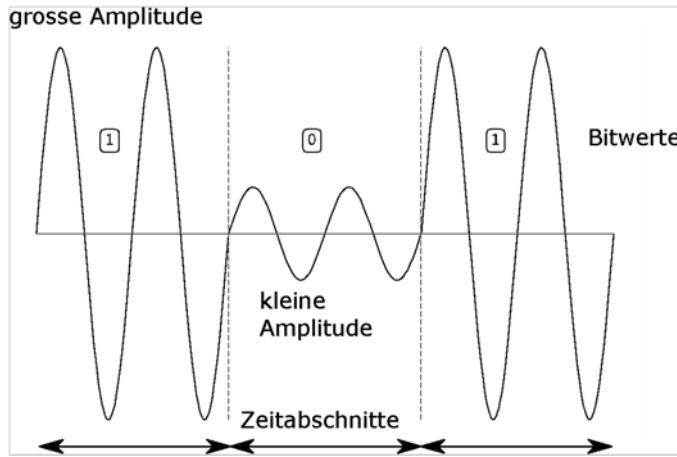


Abb. 3.16 Einfache Digitale Amplitudenmodulation zur Übertragung von Bitwerten

Bit funktioniert aus vielen Gründen bei modernen Systemen nicht. Das Verfahren in der dargestellten einfachen Form findet aber heute auch keine Verwendung mehr, da es wenig performant und darüber hinaus sehr fehleranfällig ist. Als Teil der im Folgenden dargestellten Quadratur-Amplitudenmodulation ist es jedoch weit verbreitet.

3.3.1.4 Digitale Frequenzmodulation

Die Frequenzmodulation ist das bis heute gängige Verfahren zur qualitativ hochwertigen Übertragung von Rundfunkprogrammen (FM Radio). Die Frequenz der Trägerwelle wird durch das Nutzsignal verändert. Da die Amplitude des modulierten Signals keine Information enthält, ist ein frequenzmoduliertes Signal wenig empfindlich gegen Störungen durch Rauschen. Bei der *digitalen Frequenzmodulation* wechseln sich höhere Frequenzen mit niedrigeren Frequenzen entsprechend der kodierten Bit-Werte 0 und 1 ab (Abb. 3.17). Es

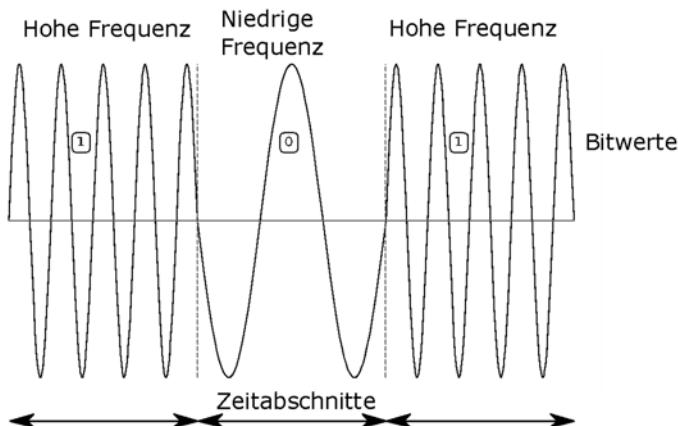


Abb. 3.17 Digitale Frequenzmodulation (Frequency Shift Keying)

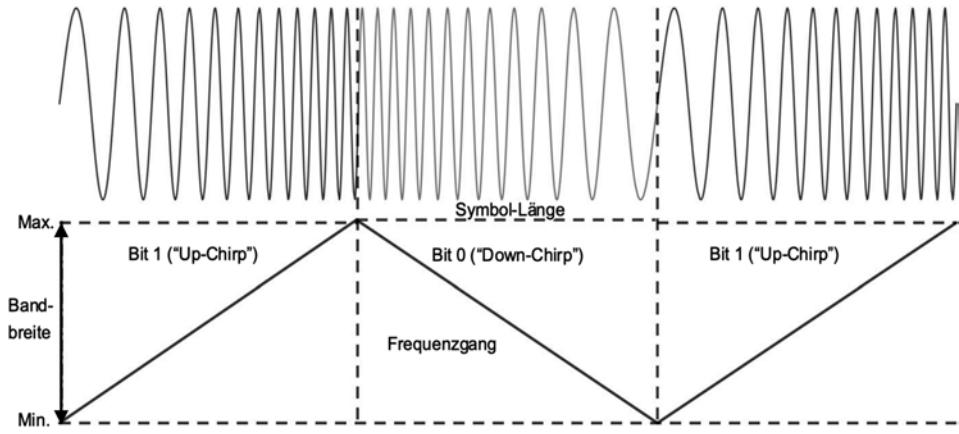


Abb. 3.18 CHIRP-Modulation

wird von Frequenzumtastung (Frequency Shift Keying, FSK) gesprochen. Frequenzumtastung wird in digitalen Mobilfunksystemen (z. B. GSM) eingesetzt.

Eine heute noch gebräuchliche Variante der Frequenzmodulation ist die *Compressed High Intensity Radar Pulse Modulation* (CHIRP). Ursprünglich für die Verwendung in militärischen und zivilen Radarsystemen entwickelt findet sie auch Anwendung in sogenannten Low Power Wide Area (LPWA) Systemen (Abschn. 5.9). CHIRP ist eine sehr robuste Modulation: Sie ist unempfindlich gegen Störungen und erlaubt die Identifikation des Signals noch bei -20 dB Signal-Rauschabstand. Zudem ist sie nicht empfindlich gegen den Doppler-Effekt (Abschn. 3.2.4). Die Bezeichnung CHIRP (englisch für „Zwitschern“) beschreibt den charakteristischen Frequenzverlauf. Während der Dauer eines Symbols wird die gesamte zur Verfügung stehende Bandbreite einmal durchlaufen. Zur Modulation eines Bit-Wertes 1 wird die Frequenz dabei kontinuierlich erhöht (Up-Chirp); für den Bit-Wert 0 wird sie kontinuierlich gesenkt (Down-Chirp). Abb. 3.18 zeigt die Bitfolge 101 in der Chirp-Modulation.

3.3.1.5 Digitale Phasenmodulation

Bei der *Phasenmodulation* (Abb. 3.19) wird die Phase der Trägerwelle durch das Nutzsignal verändert. Die Trägerwelle wird also jeweils in Zeitrichtung um den Wert des Nutzsignals verschoben. Die Phasenmodulation, auch als Phasenumtastung (Phase Shift Keying, PSK) bezeichnet, eignet sich sehr gut zur Übertragung digitaler Daten. Dabei wird die Phase der Trägerwelle bei gleichbleibender Frequenz lediglich jeweils um konstante Werte verschoben, entsprechend den zu übertragenden digitalen Werten. Am Beginn und am Ende jedes Zeitabschnittes kann sich die Phase verändern. Die Bezeichnung Phasenumtastung geht auf diese Veränderungen zurück.

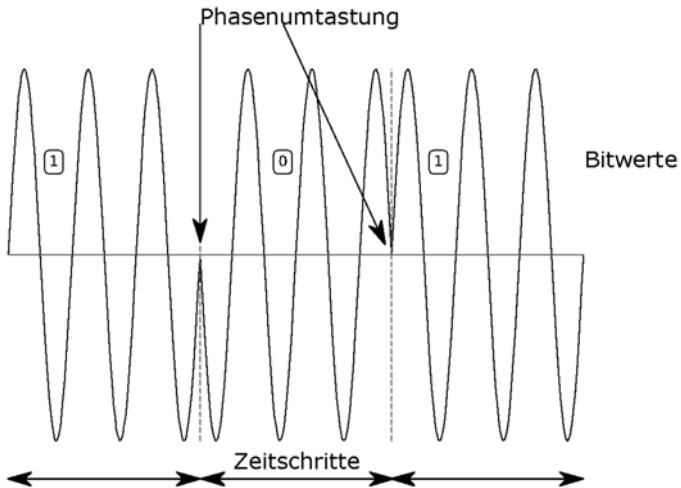


Abb. 3.19 Digitale Phasenmodulation (Phase Shift Keying)

3.3.1.6 Quadratur-Amplitudenmodulation

In Hochleistungs-Digitalsystemen, wie etwa im Mobilfunk, werden zur Erhöhung der erzielbaren Datenraten komplexere Modulationsverfahren eingesetzt. Die im Mobilfunk weit verbreitete Quadratur-Amplitudenmodulation (QAM) beruht auf Konfigurationsdiagrammen, wie in Abb. 3.20 b) und d) dargestellt. Jeder Punkt in einem solchen Diagramm entspricht einem zu übertragenden Symbol. Dabei ist die Entfernung des Punktes vom Nullpunkt gleich der Amplitude und der Winkel, den der Strahl vom Nullpunkt zum Konfigurationspunkt mit der positiven x-Achse bildet, die Phase der zum Symbol gehörigen Welle (Abb. 3.22).

Der Sender zerlegt die zu übertragende Bitfolge in gleich lange Abschnitte von Bits. Jede dieser Bitfolgen repräsentiert einen der diskreten Werte des Wertevorrats. Bei der QAM ist die Länge der Abschnitte stets eine gerade Zahl: 2 Bits entsprechend 4 Werten bei QPSK, 4 Bits entsprechend 16 Werten bei 16QAM, 6 Bits entsprechend 64 Werten bei 64QAM usw. Jeder dieser Werte wird durch ein Symbol übertragen. Er wird dazu in zwei Hälften zerlegt. Die erste Hälfte der Bits definiert die I-Amplitude, die zweite Hälfte die Q-Amplitude.

Abb. 3.21 illustriert das Schema bei 16QAM. Jede Vierergruppe von Bits wird in zwei Bit-Paare zerlegt, denen dann jeweils ein Amplitudenwert zugeordnet wird (Spalte „Wert“ in der Tabelle). Die Trägerwellen für I und Q sind von gleicher Frequenz, sind aber um eine Viertel Wellenlänge (90°) gegeneinander verschoben. Wegen der Begrenzung der Sendenergie werden die Amplituden mit dem in der Tabelle nicht gezeigten gemeinsamen Faktor $1/\sqrt{10}$ multipliziert. Abb. 3.22 zeigt, wie sich Amplitude und Phase der resultierenden Welle aus der Addition von I und Q ergeben. Auf der Empfängerseite misst die elektronische Schaltung die Amplitude und die Phasenverschiebung der einfallenden Welle und liest direkt die zum Symbol gehörigen vier Bits aus einer Tabelle ab.

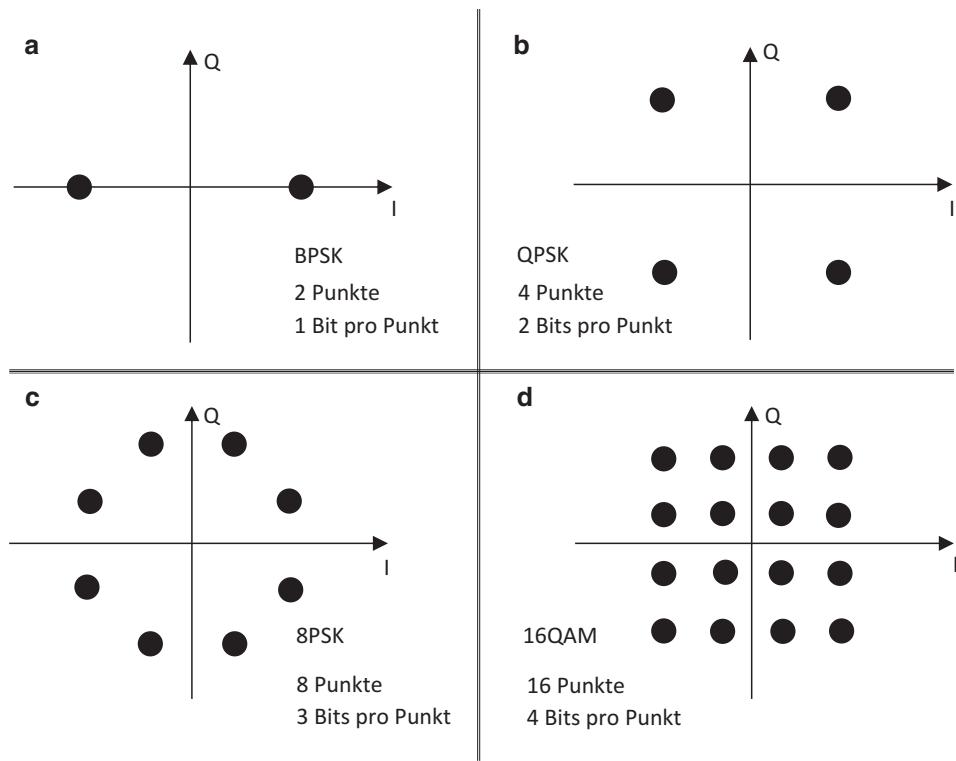
**Abb. 3.20** Konfigurationsdiagramme zur Quadratur-Modulation

Abb. 3.20 zeigt in a) die binäre Phasenmodulation in der Darstellung durch ein Konfigurationsdiagramm (BPSK). Hier entfällt die zweite Trägerwelle, da jedes Symbol nur ein Bit zu übertragen hat. In Abb. 3.20 c) wird als ein weiteres Beispiel die Konfiguration einer 8PSK-Modulation gezeigt. Es handelt sich um eine reine Phasenmodulation, da alle

| Bitfolge | I-Amplitude | | Q-Amplitude | | Bitfolge | I-Amplitude | | Q-Amplitude | |
|----------|-------------|------|-------------|------|----------|-------------|------|-------------|------|
| | Bits | Wert | Bits | Wert | | Bits | Wert | Bits | Wert |
| 0000 | 00 | 1 | 00 | 1 | 1000 | 10 | -1 | 00 | 1 |
| 0001 | 00 | 1 | 01 | 3 | 1001 | 10 | -1 | 01 | 3 |
| 0010 | 00 | 3 | 10 | 1 | 1010 | 10 | -3 | 10 | 1 |
| 0011 | 00 | 3 | 11 | 3 | 1011 | 10 | -3 | 11 | 3 |
| 0100 | 01 | 1 | 00 | -1 | 1100 | 11 | -1 | 00 | -1 |
| 0101 | 01 | 1 | 01 | -3 | 1101 | 11 | -1 | 01 | -3 |
| 0110 | 01 | 3 | 10 | -1 | 1110 | 11 | -3 | 10 | -1 |
| 0111 | 01 | 3 | 11 | -3 | 1111 | 11 | -3 | 11 | -3 |

Abb. 3.21 Konfigurationsschema bei 16QAM

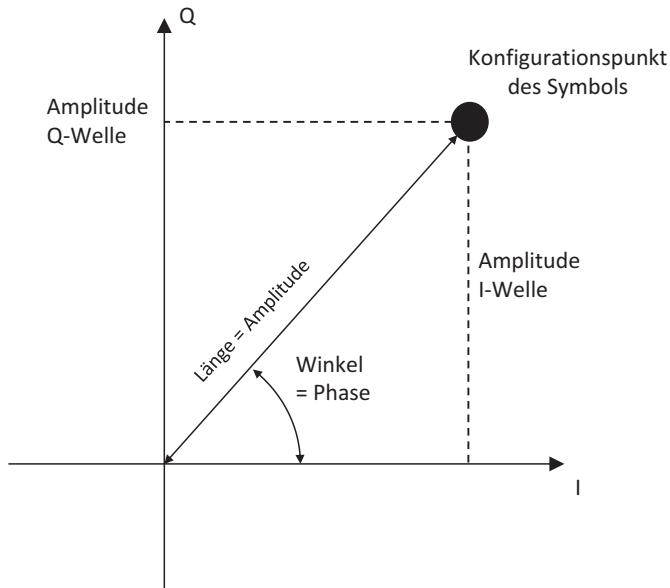


Abb. 3.22 Amplituden und Phase zu einem Konfigurationspunkt bei QAM (European Telecommunications Standards Institute 2017)

Konfigurationspunkte gleichen Abstand zum Nullpunkt haben. BPSK und 8PSK sind von historischer Bedeutung für die Entwicklung des digitalen Mobilfunks in den 2G-Standards GSM und EDGE.

Aus Abb. 3.20 ist auch erkennbar, dass bei wachsender Anzahl der Konfigurationspunkte die Abstände zwischen ihnen immer kleiner werden. Die Trennschärfe des Empfängers zur Unterscheidung verschiedener Amplituden- und Phasenwerte muss mit der Anzahl der Konfigurationspunkte wachsen. Daher werden höhere QAM-Stufen, wie 64QAM oder gar 256QAM nur bei ausgezeichneten Übertragungsbedingungen eingesetzt. Genaueres wird dazu in den Erläuterungen zu den Mobilfunkgenerationen (Kap. 4) ausgeführt.

3.3.1.7 Modulation und Frequenzbänder

Die Modulation einer Trägerfrequenz erzeugt Variationen und weitere Frequenzen durch die vielfältigen Kombinationen periodischer Ereignisse, wie der schnellen Abfolge der Symbole und der Veränderungen der Welle innerhalb der Symbole. Ausgehend von der Trägerfrequenz liegen die zusätzlichen Frequenzen nach oben und unten verschoben im Spektrum. Die übertragenen Daten sind wesentlich in den Nachbarfrequenzen enthalten. Ihre vollständige Unterdrückung ist daher nicht erwünscht und technisch auch nicht mög-

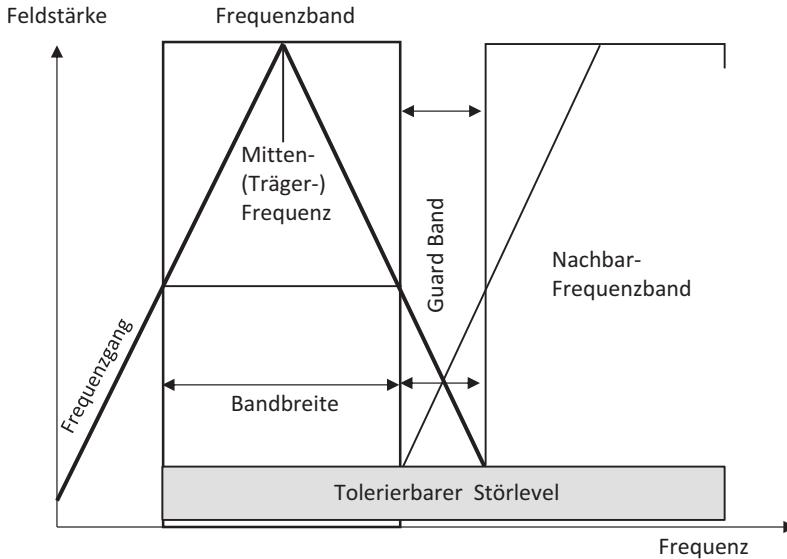


Abb. 3.23 Frequenzband und Guard-Band bei modulierten Signalen

lich. Die Leistung der durch die Modulation erzeugten Frequenzen nimmt mit wachsendem Abstand von der Trägerfrequenz ab. Zusätzlich verstärken spezielle Schaltkreise, sogenannte Filter, die Absenkung der Leistung. Die Abhängigkeit der Leistung von der Frequenz wird in einer Kurve, dem Frequenzgang, dargestellt. Abb. 3.23 zeigt das Prinzip: Der Frequenzgang ist eine von der Trägerfrequenz nach beiden Seiten abnehmende Kurve. Trotzdem erzeugt jede modulierte Trägerfrequenz Störungen anderer übertragenen Frequenzen. Deshalb wird für jede Funkübertragung ein ganzer Frequenzbereich, ein sogenanntes Frequenzband, reserviert. Die Breite des Frequenzbandes ist so definiert, dass die empfangenen Wellen der eingeschlossenen Frequenzen die Demodulation ermöglichen. Je höher die Frequenz der Symbole (also die Anzahl der Symbole pro Zeiteinheit), desto breiter ist das für eine Übertragung benötigte Frequenzband. Umgekehrt kann ein breiteres zur Verfügung stehendes Frequenzband nur durch sehr hohe Symbolfrequenzen und damit sehr kurze Symbolzeiten effektiv genutzt werden. Zusätzlich wird eine Schutzzone (Guard Band) zwischen benachbarten Frequenzbändern eingefügt, die verhindert, dass die Übertragungen in den benachbarten Bändern sich gegenseitig stören.

3.3.2 Fehlerquellen und Fehlerkorrektur

Datenübertragung mittels Funkverbindung ist grundsätzlich sehr fehleranfällig. Der Übertragungsweg ist nicht abgeschirmt, so dass viele Störungen von außen einwirken können. Störungen können einen einzelnen Empfänger betreffen, aber auch ganze Regionen. Die wichtigsten Effekte, die zu Übertragungsfehlern führen sind

- Hochfrequente Signale aus defekten oder nicht zugelassenen Geräten überlagern und stören das ohnehin sehr schwache Funksignal; beispielhaft: Alte, nicht demontierte Antennenverstärker, defekte Koaxial-Hausverkabelung, nicht-konforme Schnurlosetelefone, Babyphones oder WiFi Access Points im nicht-lizenzierten Funkbereich.
- Zeitweilige oder dauernde Abschattung des Übertragungsweges: Vorbeifahrende Lkw, neue Häuser oder Baumwuchs schwächen das Signal ab.
- Regenschauer oder Nebel dämpfen oder streuen das Signal und können kurzfristig auftreten.
- Die Längen der Übertragungswege ändern sich kurzfristig durch zusätzliche Reflexionen an Hindernissen. Die veränderten Laufzeiten unterschiedlicher Übertragungswege können durch den Empfänger nicht mehr ausgeglichen werden.
- Ein Endgerät bewegt sich und erzeugt dadurch eine Verschiebung der Frequenz (Doppler-Effekt, Abschn. 3.2.4). Bei schneller Bewegung kann das zum Ausfall von empfangenen Bits führen.

Ein großer und dauerhaft vorhandener Störparameter ist jedoch das schon in Abschn. 3.2.3 angesprochene Rauschen in Kombination mit dem Abfall der Leistung über die Entfernung zur Quelle. Rauschen wirkt als statistisch verteilte Leistung auf das Signal ein. Je schwächer das Signal ist, desto stärker ist die Verfälschung durch Rauschen. Ein durch Rauschen verfälschtes Signal kann durch den Empfänger falsch interpretiert werden.

Die Erkennung eines Übertragungsfehlers erfolgt durch die in der gesamten Nachrichtentechnik verbreiteten Zyklischen Redundanzprüfung (Cyclic Redundancy Check, CRC). Der CRC dividiert den Datenblock durch die gegebene CRC-Bitfolge. Dabei wird die Binär-Addition durch die bitweise XOR-Operation ersetzt. XOR vergleicht zwei Bit-Werte. Stimmen sie überein, ist das Ergebnis 0, sind sie verschieden, ist das Ergebnis 1. Der Rest dieser Division wird vor dem Senden an den Block angehängt. Beim Empfänger wird die Division inklusive der angefügten Bits wiederholt; ergibt die Division hier den Rest Null, wird der Block als fehlerfrei akzeptiert. Abb. 3.24 zeigt beispielhaft einen 4 Bit CRC und die Reaktion auf einen einfachen Bit-Fehler. In der Funkübertragung wird häufig ein 24 Bit CRC verwendet. Er erkennt sicher gebündelte Fehler von bis zu 24 Bits, und darüber hinaus auch längere Folgen fehlerhafter Bits mit hoher Wahrscheinlichkeit (Kurose und Ross 2014).

Die Fehlerrate bei drahtlosen Datenübertragungen durch Funkwellen liegt um Größenordnungen über derjenigen bei leitungsgebundenen Übertragungen. Es ist davon auszugehen, dass etwa jedes zehnte Bit falsch beim Empfänger ankommt. Eine einfache Neusendung eines als nicht korrekt empfangen deklarierten Datenblocks von mehreren Hundert Bits würde dann zu einer andauernden Wiederholung dieses einen Blocks führen. Ohne effiziente Fehlerkorrekturverfahren ist eine mobile Datenkommunikation daher nicht möglich.

Wiederholungen von fehlerhaften Datenpaketen lassen sich nur vermeiden, wenn der Sender den übertragenen Daten „Selbstheilungskräfte“ mitgibt. Entsprechende Verfahren werden als Vorwärts-Fehlerkorrektur (Forward Error Correction, FEC) bezeichnet: Jedem

| Ermittlung des CRC-Wertes zu den Nutzdaten | | | | | | | | Überprüfung des CRC nach korrekter Übertragung | | | | | | | |
|--|--|--|--|--|--------------------|---|---|--|--|--|--|--|--|--|--|
| Nutzdaten | | | | | Platz für CRC-Wert | | | Nutzdaten mit angehängtem CRC | | | | | | | |
| 1 1 0 0 1 1 | | | | | 0 | 0 | 0 | 1 1 0 0 1 1 1 1 0 1 0 | | | | | | | |
| 1 0 0 1 1 | | | | | 1 | 0 | 0 | 1 0 0 1 1 1 1 0 1 0 | | | | | | | |
| 0 1 0 1 0 | | | | | 1 | 0 | 0 | 1 0 0 1 1 1 1 0 1 0 | | | | | | | |
| 1 0 0 1 1 | | | | | 0 | 0 | 0 | 1 0 0 1 1 1 1 0 1 0 | | | | | | | |
| 0 0 1 1 0 | | | | | 0 | 0 | 0 | 1 0 0 1 1 1 1 0 1 0 | | | | | | | |
| 1 0 0 1 1 | | | | | 1 | 0 | 0 | 1 0 0 1 1 1 1 0 1 0 | | | | | | | |
| 1 0 1 1 0 | | | | | 1 | 0 | 0 | 1 0 0 1 1 1 1 0 1 0 | | | | | | | |
| 0 0 1 0 0 | | | | | 0 | 0 | 0 | 1 0 0 1 1 1 1 0 1 0 | | | | | | | |
| 1 0 0 1 1 | | | | | 1 | 0 | 0 | 1 0 0 1 1 1 1 0 1 0 | | | | | | | |
| 0 0 1 0 0 | | | | | 0 | 0 | 0 | 1 0 0 1 1 1 1 0 1 0 | | | | | | | |
| 1 0 1 0 0 | | | | | 1 | 0 | 0 | 1 0 0 1 1 1 1 0 1 0 | | | | | | | |
| 0 0 1 0 0 | | | | | 0 | 0 | 0 | 1 0 0 1 1 1 1 0 1 0 | | | | | | | |
| 1 0 1 0 0 | | | | | 1 | 0 | 0 | 1 0 0 1 1 1 1 0 1 0 | | | | | | | |
| 0 0 1 0 0 | | | | | 0 | 0 | 0 | 1 0 0 1 1 1 1 0 1 0 | | | | | | | |
| 1 0 1 0 0 | | | | | 1 | 0 | 0 | 1 0 0 1 1 1 1 0 1 0 | | | | | | | |
| 0 0 1 0 0 | | | | | 0 | 0 | 0 | 1 0 0 1 1 1 1 0 1 0 | | | | | | | |
| 1 0 1 0 0 | | | | | 1 | 0 | 0 | 1 0 0 1 1 1 1 0 1 0 | | | | | | | |
| 0 0 1 0 0 | | | | | 0 | 0 | 0 | 1 0 0 1 1 1 1 0 1 0 | | | | | | | |
| 1 0 1 0 0 | | | | | 1 | 0 | 0 | 1 0 0 1 1 1 1 0 1 0 | | | | | | | |
| 0 0 1 0 0 | | | | | 0 | 0 | 0 | 1 0 0 1 1 1 1 0 1 0 | | | | | | | |
| 1 0 1 0 0 | | | | | 1 | 0 | 0 | 1 0 0 1 1 1 1 0 1 0 | | | | | | | |
| 0 0 1 0 0 | | | | | 0 | 0 | 0 | 1 0 0 1 1 1 1 0 1 0 | | | | | | | |
| 1 0 1 0 0 | | | | | 1 | 0 | 0 | 1 0 0 1 1 1 1 0 1 0 | | | | | | | |
| 0 0 1 0 0 | | | | | 0 | 0 | 0 | 1 0 0 1 1 1 1 0 1 0 | | | | | | | |
| 1 0 1 0 0 | | | | | 1 | 0 | 0 | 1 0 0 1 1 1 1 0 1 0 | | | | | | | |
| 0 0 1 0 0 | | | | | 0 | 0 | 0 | 1 0 0 1 1 1 1 0 1 0 | | | | | | | |
| 1 0 1 0 0 | | | | | 1 | 0 | 0 | 1 0 0 1 1 1 1 0 1 0 | | | | | | | |
| 0 0 1 0 0 | | | | | 0 | 0 | 0 | 1 0 0 1 1 1 1 0 1 0 | | | | | | | |
| 1 0 1 0 0 | | | | | 1 | 0 | 0 | 1 0 0 1 1 1 1 0 1 0 | | | | | | | |
| 0 0 1 0 0 | | | | | 0 | 0 | 0 | 1 0 0 1 1 1 1 0 1 0 | | | | | | | |
| 1 0 1 0 0 | | | | | 1 | 0 | 0 | 1 0 0 1 1 1 1 0 1 0 | | | | | | | |
| 0 0 1 0 0 | | | | | 0 | 0 | 0 | 1 0 0 1 1 1 1 0 1 0 | | | | | | | |
| 1 0 1 0 0 | | | | | 1 | 0 | 0 | 1 0 0 1 1 1 1 0 1 0 | | | | | | | |
| 0 0 1 0 0 | | | | | 0 | 0 | 0 | 1 0 0 1 1 1 1 0 1 0 | | | | | | | |
| 1 0 1 0 0 | | | | | 1 | 0 | 0 | 1 0 0 1 1 1 1 0 1 0 | | | | | | | |
| 0 0 1 0 0 | | | | | 0 | 0 | 0 | 1 0 0 1 1 1 1 0 1 0 | | | | | | | |
| 1 0 1 0 0 | | | | | 1 | 0 | 0 | 1 0 0 1 1 1 1 0 1 0 | | | | | | | |
| 0 0 1 0 0 | | | | | 0 | 0 | 0 | 1 0 0 1 1 1 1 0 1 0 | | | | | | | |
| 1 0 1 0 0 | | | | | 1 | 0 | 0 | 1 0 0 1 1 1 1 0 1 0 | | | | | | | |
| 0 0 1 0 0 | | | | | 0 | 0 | 0 | 1 0 0 1 1 1 1 0 1 0 | | | | | | | |
| 1 0 1 0 0 | | | | | 1 | 0 | 0 | 1 0 0 1 1 1 1 0 1 0 | | | | | | | |
| 0 0 1 0 0 | | | | | 0 | 0 | 0 | 1 0 0 1 1 1 1 0 1 0 | | | | | | | |
| 1 0 1 0 0 | | | | | 1 | 0 | 0 | 1 0 0 1 1 1 1 0 1 0 | | | | | | | |
| 0 0 1 0 0 | | | | | 0 | 0 | 0 | 1 0 0 1 1 1 1 0 1 0 | | | | | | | |
| 1 0 1 0 0 | | | | | 1 | 0 | 0 | 1 0 0 1 1 1 1 0 1 0 | | | | | | | |
| 0 0 1 0 0 | | | | | 0 | 0 | 0 | 1 0 0 1 1 1 1 0 1 0 | | | | | | | |
| 1 0 1 0 0 | | | | | 1 | 0 | 0 | 1 0 0 1 1 1 1 0 1 0 | | | | | | | |
| 0 0 1 0 0 | | | | | 0 | 0 | 0 | 1 0 0 1 1 1 1 0 1 0 | | | | | | | |
| 1 0 1 0 0 | | | | | 1 | 0 | 0 | 1 0 0 1 1 1 1 0 1 0 | | | | | | | |
| 0 0 1 0 0 | | | | | 0 | 0 | 0 | 1 0 0 1 1 1 1 0 1 0 | | | | | | | |
| 1 0 1 0 0 | | | | | 1 | 0 | 0 | 1 0 0 1 1 1 1 0 1 0 | | | | | | | |
| 0 0 1 0 0 | | | | | 0 | 0 | 0 | 1 0 0 1 1 1 1 0 1 0 | | | | | | | |
| 1 0 1 0 0 | | | | | 1 | 0 | 0 | 1 0 0 1 1 1 1 0 1 0 | | | | | | | |
| 0 0 1 0 0 | | | | | 0 | 0 | 0 | 1 0 0 1 1 1 1 0 1 0 | | | | | | | |
| 1 0 1 0 0 | | | | | 1 | 0 | 0 | 1 0 0 1 1 1 1 0 1 0 | | | | | | | |
| 0 0 1 0 0 | | | | | 0 | 0 | 0 | 1 0 0 1 1 1 1 0 1 0 | | | | | | | |
| 1 0 1 0 0 | | | | | 1 | 0 | 0 | 1 0 0 1 1 1 1 0 1 0 | | | | | | | |
| 0 0 1 0 0 | | | | | 0 | 0 | 0 | 1 0 0 1 1 1 1 0 1 0 | | | | | | | |
| 1 0 1 0 0 | | | | | 1 | 0 | 0 | 1 0 0 1 1 1 1 0 1 0 | | | | | | | |
| 0 0 1 0 0 | | | | | 0 | 0 | 0 | 1 0 0 1 1 1 1 0 1 0 | | | | | | | |
| 1 0 1 0 0 | | | | | 1 | 0 | 0 | 1 0 0 1 1 1 1 0 1 0 | | | | | | | |
| 0 0 1 0 0 | | | | | 0 | 0 | 0 | 1 0 0 1 1 1 1 0 1 0 | | | | | | | |
| 1 0 1 0 0 | | | | | 1 | 0 | 0 | 1 0 0 1 1 1 1 0 1 0 | | | | | | | |
| 0 0 1 0 0 | | | | | 0 | 0 | 0 | 1 0 0 1 1 1 1 0 1 0 | | | | | | | |

dekodiert werden, und nur 10 % Neuübertragung erforderlich sind. Nach dem ersten Korrekturpaket sind dann bereits 99 % der Pakete korrekt dekodiert.

3.3.3 Vielfach-Nutzung: Medienzugriffsverfahren und Multiplexverfahren

Die drei Mobilfunknetze in Deutschland besitzen insgesamt ca. 90.000 Standorte mit Sendeanlagen. Bei mehr als 130 Millionen Mobilfunkverträgen entfallen auf jeden Sendestandort im Mittel bis zu 1700 Nutzer. Im Berliner Olympiastadion sind 72 Antennen installiert: Entlang der Überdachung, im Tribünenbereich und an den Flutlichtmasten. Ausgehend davon, dass praktisch jeder Stadionbesucher ein Smartphone mit sich führt, sind hier pro Mobilfunkzelle bis zu 1000 Endgeräte eingebucht, von denen jedes die Wahl aus bis zu 70 Funkzellen hat. Die Regelung des Zugriffs auf die Basisstation ist für einen funktionierenden Mobilfunkverkehr also von allerhöchster Priorität. Die Auswahl einer Basisstation und die Herstellung der Verbindung sind in Abschn. 2.5 bereits dargestellt worden. In diesem Kapitel geht es um die gleichzeitige und parallele Nutzung eines Frequenzbandes und der Kapazität einer Basisstation und eines Frequenzbandes durch eine große Zahl von verbundenen Endgeräten.

3.3.3.1 Medienzugriffsverfahren in Mobilfunknetzen und leitungsgebundenen Netzen

Medienzugriffsverfahren (Medium Access Control, MAC) umfassen alle Mechanismen, um Nutzern den Zugriff auf ein Medium zu gewähren. Die Funkübertragung weist einige Besonderheiten auf, die zu Unterschieden im Vergleich zu leitergebundenen Übertragungstechniken führt. Wird das ISO/OSI-Referenzmodell für Datenübertragungssysteme als Grundlage gewählt, dann sind die grundsätzlichen Multiplex-Verfahren der Bitübertragungsschicht zuzuordnen (erste Schicht). Die Medienzugriffsverfahren sind der Sicherungsschicht (zweite Schicht) zuzuordnen und werden in modernen Kommunikationssystemen typischerweise miteinander kombiniert.

Aus leitergebundenen Kommunikationssystemen sind Verfahren bekannt, die den Medienzugriff effektiv und effizient regeln. Das wohl bekannteste Verfahren ist CSMA/CD (Carrier Sense Multiple Access with *Collision Detection*). CSMA/CD wird bei Übertragungsverfahren wie dem Ethernet mit einer paketorientierten Datenübertragung auf einem gemeinsam genutzten Medium (Shared Medium) genutzt. Daher ist es möglich, dass mehrere Kommunikationskanäle über dasselbe Medium (z. B. Koaxialkabel) zeitgleich Daten austauschen wollen. Hierdurch können Kollisionen entstehen, welche die übertragenen Signale unbrauchbar machen. Von einer Kollision wird gesprochen, wenn sich zwei oder mehr Signale zeitgleich auf einem gemeinsamen Medium überlagern, so dass eine Identifikation der einzelnen Signalanteile nicht mehr möglich ist. Das CSMA/CD-Verfahren erkennt auftretende Kollisionen, löst sie auf und verhindert weitgehend, dass sie sich wiederholen. Wenn ein Gerät Daten senden möchte, wird folgender Ablauf durchlaufen:

1. Abtasten des Mediums: Das Medium wird überwacht, ob es belegt ist, also bereits eine Datenübertragung stattfindet.
 - a. Frei: Wenn das Medium eine bestimmte Zeit lang frei ist, weiter mit Schritt 2.
 - b. Belegt: Wiederholung von Schritt 1
2. Senden: Datenübertragung, zugleich wird das Medium fortwährend weiter abgehört
 - a. Erfolg: Die Übertragung wird erfolgreich abgeschlossen und an höhere Netzwerkschichten gemeldet, weiter mit Schritt 4.
 - b. Kollision: Der Sender überwacht während der Übertragung das Medium kontinuierlich. Eine Kollision äußert sich dadurch, dass das Gesamtsignal auf dem Medium nicht seiner eigenen Übertragung entspricht. Wird eine Kollision entdeckt, wird die Datenübertragung abgebrochen und ein definiertes Störsignal in das Medium abgegeben (Jamming), um alle anderen Sender/Empfänger über die Kollision zu informieren. Dann weiter mit Schritt 3.
3. Die Anzahl der Übertragungsversuche ist begrenzt. Wird die maximal zulässige Anzahl erreicht, wird die Übertragung abgebrochen (Schritt 4), ansonsten wird eine weitere Wiederholung in Schritt 1 gestartet.
4. Ende: Übertragungsmodus verlassen.

In der drahtlosen Datenkommunikation ist das CSMA/CD Verfahren in dieser Form nicht einsetzbar. Die grundlegende Voraussetzung, dass jedes der beteiligten Geräte Sendever suchen aller anderen Geräte auf dem Medium bemerken kann, ist hier nicht gegeben.

Folgendes Szenario soll zur Beschreibung der vorliegenden Problematik im Medienzugriff bei funkbasierten Kommunikationsnetzwerken zur Illustration dienen (Abb. 3.25): Es befinden sich zwei mobile Endgeräte A und B in einer Funkzelle. Beide Endgeräte haben den gleichen Abstand zur versorgenden Antenne Z. Endgerät A ist jedoch in westlicher Richtung von der Antenne Z, Endgerät B in östlicher Richtung von der Antenne Z lokalisiert. Der Übertragungsbereich von Endgerät A reicht dabei noch bis zur Antenne Z, jedoch nicht bis zum Endgerät B. Auch der Erkennungsbereich von A reicht nicht bis zum Endgerät B. Gleichermaßen gilt in die andere Richtung (Z liegt im Übertragungsbereich von B, A liegt nicht im Erkennungsbereich von B). In diesem anschaulichen Beispiel kann also Endgerät A nicht erkennen, dass Endgerät B Daten überträgt. Bereits der erste Schritt des CSMA/CD-Verfahrens würde nicht funktionieren. Genauso würde die Überwachung des Kanals die Signale des jeweils anderen mobilen Endgeräts nicht erkennen. Daher wird hier von versteckten Endgeräten (*hidden terminals*) gesprochen: Endgerät A und Endgerät B sind für den jeweils anderen nicht erkennbar.

Für die Anwendung in lokalen funkbasierten Netzwerken (Kap. 5) beim Netzzugriff in Situationen mit versteckten Endgeräten wird das CSMA/CD Verfahren zu CSMA/CA modifiziert. CA steht dabei für *Collision Avoidance*. Jedes Endgerät beobachtet den Funkverkehr wie beim CSMA/CD Verfahren. Wird das Medium als frei erkannt, beginnt zunächst eine Wartezeit von zufälliger Dauer. Dadurch wird die Wahrscheinlichkeit verringert, dass zwei Geräte direkt nach Ende der Belegung des Mediums gleichzeitig mit der Sendung beginnen. Eine Kollision zeigt sich aber erst durch die ausbleibende Quittung vom Emp-

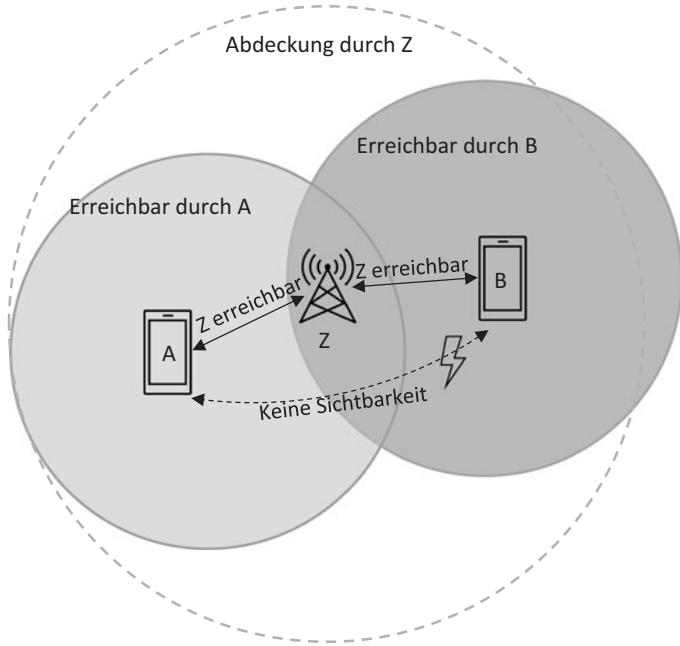


Abb. 3.25 Versteckte Endgeräte

fänger. Für kleine Pakete ist das Verfahren unproblematisch, da die notwendige Wiederholung keine starke Belastung des Netzes darstellt. Bei diesem Verfahren werden aber auch lange Pakete trotz Kollision immer vollständig gesendet. Zur Vermeidung von Kollisionen kann ein Endgerät daher vor Aussendung eines langen Paketes einen optionalen Request-to-send (RTS)/ Clear-to-send (CTS) Handshake durchführen. Bei freiem Medium wird RTS nach zufälliger Wartezeit als kurzes Datenpaket gesendet. Die CTS-Antwort des zentralen Knotens wird von allen Endgeräten empfangen und dient als Anzeige für die Reservierung des Mediums für die Sendung des langen Paketes. Um die Ressourcen (Funkkanäle) von Mobilfunknetzwerken effizient zu nutzen und eine Vielzahl von Nutzern in den Netzen zu ermöglichen, kommen Multiplexverfahren zum Einsatz. Diese werden im Folgenden erläutert.

3.3.3.2 Raummultiplex

Die unmittelbarste Zugriffsregelung erfolgt über die Aufteilung der Fläche in Mobilfunkzellen durch den Raummultiplex (Space Division Multiplexing, SDM). Ein mobiles Endgerät kommuniziert zu jeder Zeit mit genau einer Basisstation über genau eine der zu dieser Basisstation gehörenden Antennen. Wie bereits erläutert, wird diese Aufteilung erzwungen durch die begrenzten Reichweiten der ausgesendeten Signale. Zusätzlich hat eine Basisstation nur eine begrenzte Kapazität für die Kommunikation mit Endgeräten, daher werden Zellen auch räumlich verdichtet, so dass ein Endgerät mehrere Basisstatio-

nen funktionsmäßig erreichbar ist. Trotzdem wird es immer nur einer Funkzelle zugeordnet.

Ein weitergehendes Verständnis und eine bedeutende Nutzung von Raummultiplex haben sich mit der MIMO-Technologie entwickelt (Abschn. 4.5.3.1). Hier wird das von der Basisstation ausgehende Signal sehr viel stärker gebündelt als in Abschn. 3.2.3 beschrieben. Der so entstehende Signalstrahl überstreicht wie ein Scheinwerferkegel in schneller Folge den der Antenne zugeordneten Zellsektor. Jedes Endgerät ist abhängig von der Position immer nur für Bruchteile eines Zyklus in der Lage, Signale mit der Basisstation auszutauschen. In diesen kurzen Zeitintervallen steht allerdings eine hohe Bandbreite zur Verfügung.

3.3.3.3 Zeitmultiplex

Zeitmultiplex (Time Division Multiplexing, TDM) basiert auf dem Ansatz, dass in einem bestimmten Zeitintervall der gesamte nutzbare Frequenzbereich einem Teilnehmer zur Verfügung steht (Abb. 3.26). Dies bedeutet, dass zwar alle Teilnehmer den gleichen Frequenzbereich nutzen, dieses jedoch zu unterschiedlichen Zeiten. In der Praxis laufen alle beteiligten Sende- und Empfangsgeräte in einem festen Takt. Die Zeit wird in feste Abschnitte unterteilt, die als Zeitschlitz bezeichnet werden. Eine bestimmte Anzahl von Zeitschlitzten wird zu einer Gruppe zusammengefasst, den sogenannten Rahmen. Ein Rahmen wird, vergleichbar mit dem Takt eines Musikstückes, laufend wiederholt. Der Beginn eines Rahmens wird vom Sender stets durch ein festes Signal angezeigt. Der Empfänger zählt die Zeitschlitzte ab Rahmenbeginn und identifiziert so den für sich bestimmten Zeitschlitz.

Im Mobilfunk wird die Belegung der Zeitschlitzte nicht dauerhaft festgelegt, sondern vom zentralen Knoten (Basisstation) dynamisch vergeben. Damit können Endgeräte Zu-

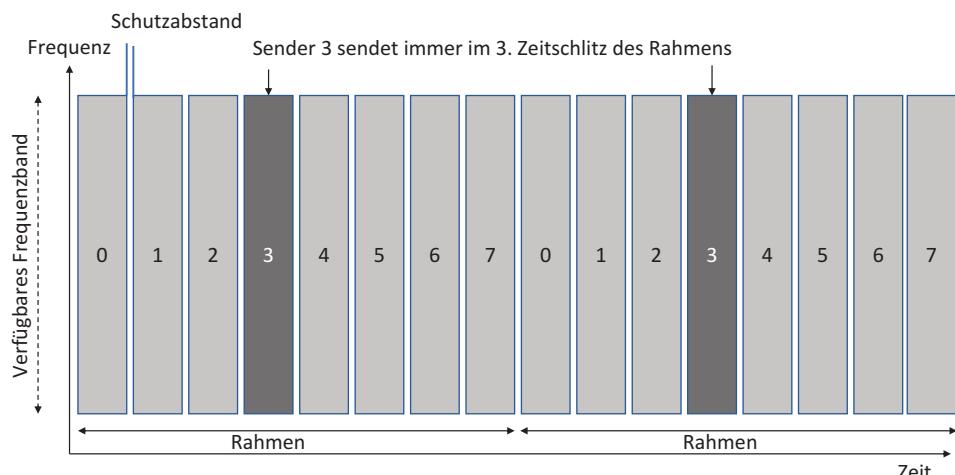


Abb. 3.26 Zeitmultiplex mit Rahmen und Zeitschlitzten

griff auf das vorhandene Frequenzband beantragen und erhalten. Es wird dann von Time Division Multiple Access (TDMA) gesprochen. Durch unterschiedliche Entfernung und Mobilität der Endgeräte kann es zu Laufzeitunterschieden und geringfügigen Verschiebungen der Zeitschlitz kommen. Daher sind zwischen den Zeitschlitz beim Mobilfunk immer kurze zeitliche Schutzabstände vorgesehen.

3.3.3.4 Frequenzmultiplex

Frequenzmultiplex (Frequency Division Multiplexing, FDM) ist jedem Radiohörer aus der täglichen Erfahrung mit diesem Medium bekannt: Sendestationen sind bestimmte Frequenzbänder zugeordnet. Im Radioempfänger wird eine Frequenz eingestellt und der gewünschte Sender wird wiedergegeben. Durch Veränderung der Frequenz kann zwischen einzelnen Radiosendern hin und her geschaltet werden. Bezogen auf die zur Verfügung stehende Ressource zur Funkübertragung erfolgt also eine Aufteilung des Frequenzspektrums auf einzelne Sender. Jedem Sender wird ein Teil des Frequenzbandes zugewiesen (Abb. 3.27).

Wie in Abschn. 3.3.1 und Abb. 3.22 dargestellt können die Frequenzbänder beim Frequenzmultiplex nicht unmittelbar nebeneinander liegen. Zur Vermeidung von gegenseitigen Störungen wird zwischen benachbarten Frequenzbändern immer ein Schutzabstand (Guard Band) freigehalten. Guard Bands führen damit zu einer schlechten Nutzung des vergebenen Frequenzbereiches im Frequenzmultiplex.

Bei einer dynamischen, nicht fest vorgegebenen Zuteilung der Frequenzbänder als Zu griffsregelung für Endgeräte wird analog zum Zeitmultiplex von Frequency Division Multiple Access (FDMA) gesprochen.

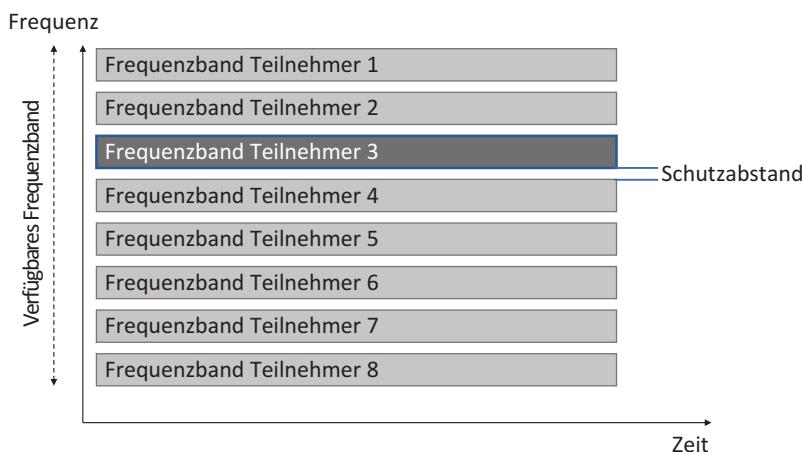


Abb. 3.27 Frequenzmultiplex, jeder Teilnehmer erhält ein eigenes Frequenzband

3.3.3.5 Frequency Division Duplex und Time Division Duplex

Mit den beiden vorgestellten Multiplex-Verfahren TDM und FDM kann ein wichtiges Unterscheidungsmerkmal von Mobilfunknetzen erläutert werden. Die Kommunikation zwischen Endgerät und Mobilfunkstation beinhaltet bereits eine Mehrfachnutzung vorhandener Ressourcen. Da es sich um zwei Parteien handelt, wird von Duplex anstelle des allgemeineren Begriffs Multiplex gesprochen. Traditionell nutzen Mobilfunknetze dafür meist ein Paar von Frequenzbändern: Ein Band für den Downlink, also die Übertragung von der Basisstation zu den verbundenen mobilen Endgeräten, und ein Band für den Uplink, also die Übertragung von mobilen Endgeräten zur Basisstation. Die Übertragungsrichtungen sind also in einer FDM-Lage. Diese Situation wird als *Frequency Division Duplex (FDD)* bezeichnet.

Da sowohl die Basisstation als auch die Endgeräte dieselbe Antenne zum Senden und zum Empfangen nutzen, muss sich zwischen Uplink-Band und Downlink-Band genügend Abstand befinden. Andernfalls würden die um 100 dB stärkeren eigenen Sendesignale die schwachen empfangenen Signale der Gegenstelle überdecken. In der Regel ist diese *Duplexlücke* mindestens 10 MHz breit. Abb. 3.28 zeigt die Zuordnung von Frequenzblöcken im 700 MHz Frequenzbereich, der von der Bundesnetzagentur von TV auf Mobilfunk umgewidmet worden ist. Die Duplexlücke beträgt hier jeweils 50 MHz. Die Frequenzen der Duplexlücke werden durch andere Netze belegt: das Problem der Beeinflussung der Wellen entsteht in den Sende- und Empfangseinrichtungen, nicht bei der Ausbreitung im Raum.

In neuerer Zeit hat sich ein anderes Verfahren zur Trennung von Uplink und Downlink in den Vordergrund geschoben: Time Division Duplex (TDD). Hierbei benutzen Basisstation und Endgerät für ihren Signalaustausch dasselbe Frequenzband. Getrennt werden Uplink und Downlink durch unterschiedliche Sendezeiten. Innerhalb des festen Rahmens senden zunächst die Endgeräte (Uplink), und die Basisstation empfängt die Signale. Zu einem festgelegten Zeitpunkt innerhalb des Rahmens erfolgt die Umschaltung, und die Basisstation sendet an die Endgeräte. Aus dem gleichen Grund wie für den Schutzabstand bei TDM gibt es hier eine Umschaltpause.

Durch die Möglichkeit, die Längen von Uplink- und Downlink-Übertragungen zu variieren erweist sich als ein klarer Vorteil des TDD. Zur Vermeidung von gegenseitigen Störungen müssen Netzbetreiber, die benachbarte Bänder verwenden, sich hierbei allerdings

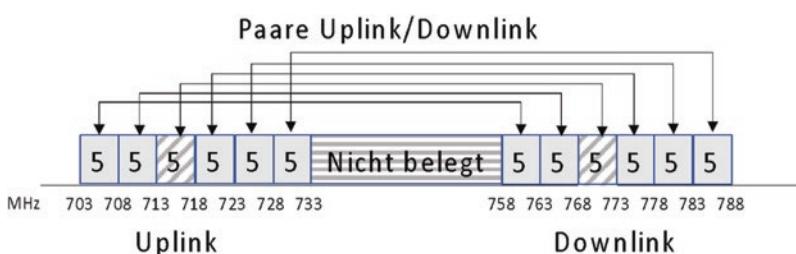


Abb. 3.28 FDD Belegung mit 5 MHz Frequenzblöcken und Duplexlücke (Bundesnetzagentur 2015)

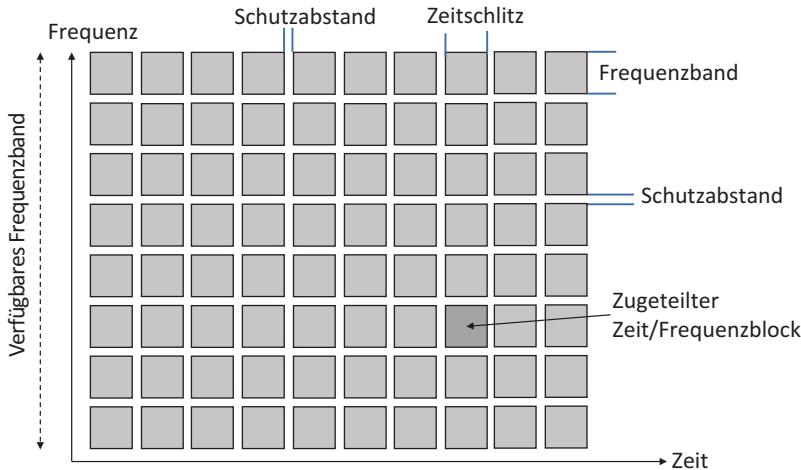


Abb. 3.29 Kombiniertes Frequenz- und Zeitmultiplex

abstimmen. Ein weiterer Vorteil ist die Möglichkeit, sehr schnell Reaktionen auf abgesetzte Kommandos zu erhalten. Dies ist die Basis, um im Mobilfunk sehr kurze Latenzzeiten zu ermöglichen.

3.3.3.6 Kombiniertes Zeit- und Frequenzmultiplex

In modernen Mobilfunknetzwerken werden Multiplex-Verfahren kombiniert eingesetzt. Besonders deutlich ist dies bei der Kombination von Frequenz- und Zeitmultiplex. Hier wird einem Kommunikationskanal für eine gewisse Zeitspanne ein gewisses Frequenzband koordiniert zur Signalübertragung zur Verfügung gestellt. Abb. 3.29 zeigt die Grundidee. Zeitlich schnell wechselnde Anforderungen durch Endgeräte können flexibel beantwortet werden. Zusätzlich können kurzfristige Störungen im Bereich einzelner Frequenzen dadurch vermieden werden, dass die betreffenden Blöcke zeitweilig nicht mehr verwendet werden. Der Nachteil des kombinierten Zeit- und Frequenzmultiplex liegt in der doppelten Reservierung von Schutzabständen sowohl in der Zeit- als auch in der Frequenzdimension.

Eine Variante des Netzzugriffs, die die TDMA/FDMA Kombination aktiv ausnutzt, ist das Frequenzsprungverfahren (Frequency-Hopping, FHSS). Es wird zum Beispiel beim Bluetooth-Standard (Kap. 5) angewendet. Die kommunizierenden Geräte wechseln in schneller zeitlicher Folge die genutzten Frequenzbänder. Der Wechsel geschieht adaptiv auf Anweisung eines Network Masters oder algorithmisch gesteuert. Bei Algorithmischem Frequency-Hopping wird zu Beginn der Verbindung eine Sprungsequenz vereinbart. Es kann sich um einen festen Offset der Band-Nummer oder um eine vereinbarte Sequenz handeln. Bei adaptivem Frequency-Hopping misst der Master laufend die empfangene Signalstärke pro Kanal und gibt periodisch neue Sprungsequenzen heraus, die die belasteten Kanäle auslassen.

3.3.3.7 Orthogonal Frequency Division Multiplex und Multiple Access (OFDM und OFDMA)

Eine Erhöhung der Datenrate im Mobilfunk ist verbunden mit einer Erhöhung der zur Verfügung stehenden Bandbreite. Die Nutzung immer breiterer Frequenzbänder zur Erhöhung der Übertragungsraten führt zu einer starken Verkürzung der für jedes Symbol zur Verfügung stehenden Zeit (Abschn. 3.3.1). Damit verstärkt sich der Einfluss von Laufzeitunterschieden, wie zum Beispiel als Folge von Reflektionen, und es sinkt die Erkennungswahrscheinlichkeit des Symbols beim Empfänger. Ein Ausweg aus diesem Dilemma bietet das Orthogonale Frequenzmultiplex Verfahren (OFDM). Das zur Verfügung stehende Frequenzband wird in eine große Zahl von schmalen Bändern unterteilt. Jedem dieser Bänder werden Teile des zu übertragenden Datenstroms zugeordnet, die mit einer reduzierten Datenrate zu übertragen sind. Entsprechend kann die Symboldauer auf den Teilbändern verlängert werden. Damit wird eine robustere Übertragung erzielt. Im Übertragungsstandard LTE wird ein 5 MHz Band in 300 schmale Bänder zerlegt. Gegenüber der Nutzung des Bandes für UMTS wird die Symboldauer um den Faktor 300 verlängert.

Die zahlreichen eng beieinander liegenden Bänder benötigen nach dem „klassischen“ Frequenzmultiplex (Abb. 3.27) jeweils Schutzabstände zur Verhinderung von gegenseitiger Störung oder Beeinflussung. Dies würde zu einer schlechten Ausnutzung des Frequenzspektrums führen. Unter der Voraussetzung einer gemeinsamen synchronisierten Symbolrate kann allerdings auf einen Schutzabstand zwischen den Bändern verzichtet werden. Der Grund liegt im speziellen Frequenzgang wie in Abb. 3.30 dargestellt.

Eine genaue Untersuchung der Leistungsverteilung über die Frequenzen ergibt, dass in diesen Fällen bei einer Symboldauer T der Frequenzgang in den regelmäßigen Abständen mit Frequenzabstand $1/T$ von der Mittenfrequenz auf null sinkt. In Abb. 3.29 führt die Symboldauer (z. B. bei LTE) von 66,67 μs zu den Abständen von 15 kHz:

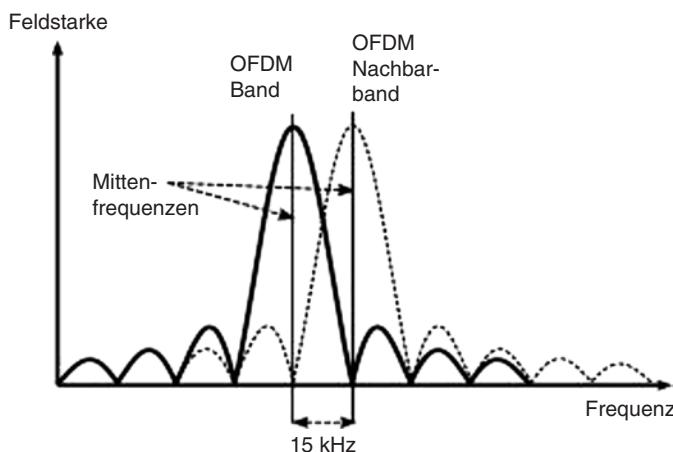


Abb. 3.30 Frequenzverlauf und Positionierung der Bänder

$\frac{1}{(66,67 \cdot 10^{-6})s} = 15.000 \text{ Hz}$. Wenn die Mittenfrequenzen der benachbarten Unterbänder auf jeweils diese Frequenzen gelegt werden, ist die gegenseitige Störung der Bänder minimal. Gleichzeitig wird durch die enge Gruppierung und teilweise Überlappung der Unterbänder eine sehr effiziente Nutzung des vorhandenen Spektralbereichs ermöglicht (Abb. 3.31).

Seit seiner Entdeckung in den 1960er-Jahren hat das OFDM-Verfahren immer stärkere Anwendung gefunden. Im Festnetz-Bereich wird es zum Beispiel unter der Bezeichnung Discrete Multitone (DMT) für den DSL-Zugang verwendet. Im Mobilfunk werden die schmalen Unterbänder von den Basisstationen dynamisch an verschiedene Endgeräte vergeben. Dabei kann ein Endgerät in der Regel mehrere Unterbänder gleichzeitig empfangen. Das entsprechende Verfahren wird dann als Orthogonal Frequency Multiple Access bezeichnet.

Weitere Vorteile von OFDM und OFDMA im Funkbetrieb sind die Vermeidung von gestörten Frequenzen und der mögliche parallele Empfang der Signale von verschiedenen Basisstationen. Beides ergibt sich unmittelbar aus der kontrollierten Vergabe bzw. Vermeidung von Unterbändern.

3.3.3.8 Code Division Multiple Access (CDMA)

In den bisher dargestellten Multiplex-Verfahren wurden die Übertragungen verschiedener Teilnehmer über die Zuteilung von Zeitpunkten oder Frequenzen unterschieden. Mit Code Division Multiple Access (CDMA) wird ein vollständig anderer Weg beschritten. Alle Teilnehmer benutzen das gesamte zur Verfügung stehende Frequenzband. Es gibt auch kein festes Zeitschema, welches den Zugriff regelt. Es wird für jede Übertragung ein eindeutiger Code verwendet, mit dem die gesendeten Daten multipliziert werden (Abb. 3.32).

Die Codes sind Folgen (Vektoren) von binären Werten. Multiplikation bedeutet, dass jedes Bit des binär vorliegenden Nutzsignals durch XOR mit dem gesamten Vektor ver-

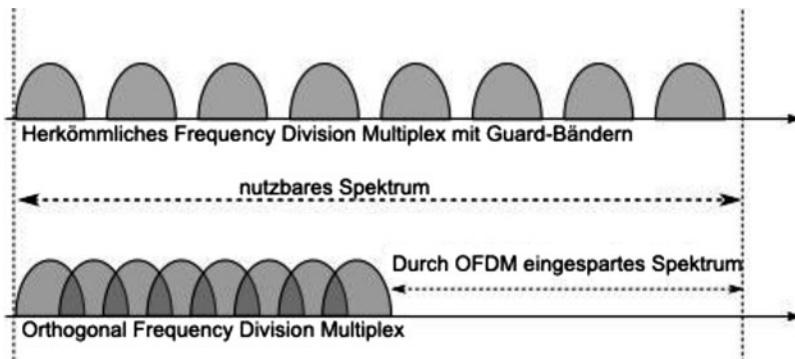
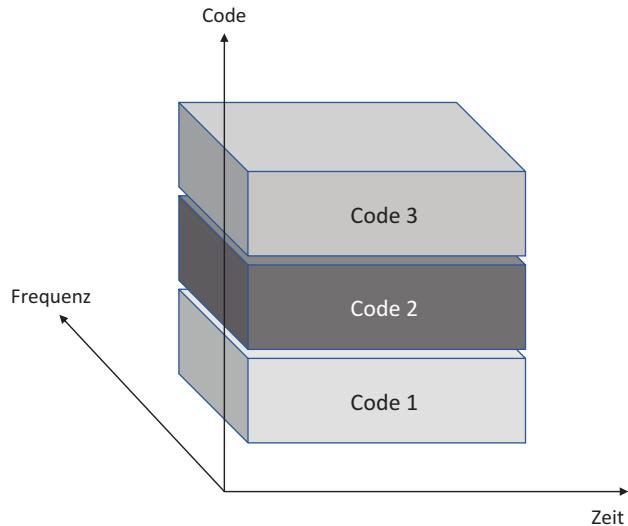


Abb. 3.31 Effektive Spektrum-Nutzung durch OFDM

Abb. 3.32 Code Division Multiple Access



CDMA Code: (0 1 0 0 1)

Zu übertragende Nutzdaten: 1 0 1

Jedes Bit der Nutzdaten wird mit dem CDMA-Code XOR-multipliziert

CDMA codierte Nutzdaten:

| | | |
|------------|-------------|-------------|
| (1 0 1 1 0 | 0 1 0 0 1 | 1 0 1 1 0 |
| Erstes Bit | Zweites Bit | Drittes Bit |

Korrekte Übertragung

XOR-Multiplikation des CDMA-Codes durch Empfänger auf jede Fünfer-Gruppe von empfangenen Bits

Korrektes Resultat mit Prozessgewinn

| | | |
|------------|-------------|-------------|
| (1 1 1 1 1 | 0 0 0 0 1 | 1 1 1 1 1 |
| Erstes Bit | Zweites Bit | Drittes Bit |

Beispiel einer fehlerhaften Übertragung

| | |
|------------|-------------|
| (1 0 1 0 0 | 0 1 1 0 1 |
| Erstes Bit | Zweites Bit |

Anwendung des Schlüssels

| | |
|------------|-------------|
| (1 1 1 0 1 | 0 0 1 0 1 |
| Erstes Bit | Zweites Bit |

Das Resultat der XOR-Multiplikation mit dem CDMA-Code zeigt immer noch eine Majorität korrekter Bits an (Toleranz)

Ein Empfänger mit dem Code (1 0 1 1 0) kann die übertragenen Daten nicht lesen.

Resultat der Anwendung dieses Schlüssels

| | |
|------------|-------------|
| (0 0 0 0 0 | 0 0 0 0 0 |
| Erstes Bit | Zweites Bit |

Abb. 3.33 CDMA Beispiel

knüpft wird. Jedes Bit wird also durch eine längere Bitfolge ersetzt. Durch diese Spiegelung wird mehr Bandbreite für die Übertragung benötigt, jedoch kann die vorhandene Bandbreite durch mehrere codierte Nutzsignale gleichzeitig genutzt werden. Hierzu sind die Codes so beschaffen, dass sie sich gegenseitig annullieren: Die Multiplikation eines Codes mit sich selbst ist von Null verschieden; die Multiplikation dieser Codes mit anderen Codes ergibt dagegen immer Null. Diese Eigenschaft wird *Orthogonalität* genannt. Der Adressat eines Nutzsignals wendet den Code des Absenders auf das Gemisch der verschiedenen Signale an, und erhält genau den für ihn bestimmten Code zurück. Abb. 3.33 zeigt die CDMA-Codierung im Beispiel.

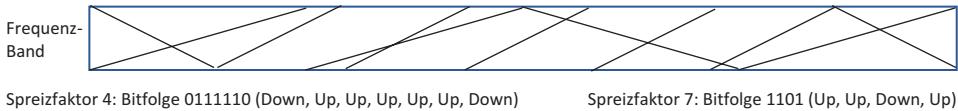


Abb. 3.34 Multiplex bei CHIRP Modulation durch Spreizfaktoren. Darstellung der Frequenzverläufe

Das CDMA-Verfahren bringt eine zusätzliche Redundanz ins Spiel: Durch Multiplikation mit längeren Codes wird die Redundanz des ursprünglichen Nutzsignals immer weiter erhöht (sogenannter Prozess-Gewinn). Damit kann ein Signal unter sehr schlechten Bedingungen noch empfangen werden, um den Preis einer geringeren nutzbaren Datenrate. CDMA gilt daher als besonders robust und wurde wohl aus diesem Grund ursprünglich für militärische Datenübertragungsanwendungen entwickelt.

3.3.3.9 CHIRP Spreizfaktoren

Low Power Wide Area Kommunikationssysteme mit CHIRP-Modulation (Abb. 3.18) verwenden ein dem CDMA verwandtes System für Netzzugriff und den Multiplex-Betrieb. Gleichzeitig liefert auch dieses Verfahren einen Prozessgewinn für Endgeräte in schlechter Abdeckung. Aufgrund der Verwendung von schmalen Frequenzbändern für CHIRP bietet sich eine Spektrum-Spreizung hier nicht an. Stattdessen wird die Zeitachse gespreizt. Endgeräte verwenden ein von der empfangenen Leistung abhängiges System von Spreizfaktoren für die Symbollänge. Ist die Basissymbollänge wie in Abb. 3.18 etwa 1 ms, so wird ein Endgerät mit einem Spreizfaktor von 7 eine Symbollänge von 7 ms anwenden. Der unmittelbare Effekt ist eine gesteigerte Erkennbarkeit aufgrund der langsameren Veränderung der Frequenz. So werden Endgeräte in der Nähe der Basisstation einen niedrigen Spreizfaktor, und Endgeräte in großer Entfernung einen hohen Spreizfaktor verwenden. Die Größe der Spreizfaktoren ist in der Regel technisch beschränkt, da sonst die Übertragungszeiten zu lang würden.

Gleichzeitig erlaubt die Verwendung unterschiedlicher Spreizfaktoren einen Multiplex-Betrieb auf dem schmalen Frequenzband. Parallel gesendete CHIRP-Signale verschiedener Endgeräte lassen sich vom Empfänger bei Verwendung unterschiedlicher Spreizfaktoren unterscheiden (Abb. 3.34). Ein Endgerät kann der Basisstation zum Beispiel bei jedem Netzzugriff über eine feste Folge von CHIRPs den verwendeten Spreizfaktor mitteilen.

3.4 Fragen

1. Recherchieren Sie die reservierten Frequenzbereiche für FM Rundfunk, für Fernseh-Übertragungen nach DVBT, für digitalen Rundfunk DAB, für GPS-Signale, für schnurlose Telefone nach DECT und Wireless LAN.
2. Welcher Wellenlängenbereich elektromagnetischer Wellen wird für den Mobilfunk genutzt? Geben Sie zwei Werte an (von – bis).

3. Welche Frequenzen korrespondieren mit den von Ihnen genannten Wellenlängen?
4. Durch welche Effekte wird die von einem Mobilfunk-Sender ausgehende Strahlung abgeschwächt?
5. Angenommen, Sie stehen in der Nähe eines Mobilfunkturmes (500 m Entfernung) und messen die bei Ihnen ankommende Leistungsdichte mit dem Ergebnis 1 mW/m^2 . Sie begeben sich jetzt in der gleichen Richtung zu einem Punkt, der 1 km entfernt vom Turm liegt. Was für eine Leistungsanzeige erhalten Sie nach der Friis Formel.
6. Sie wiederholen die Messungen aus Aufgabe 5 mit der doppelten Frequenz. Was sind die erwarteten Werte?
7. Sie stehen in der Nähe eines Gebäudes mit Sicht auf einen Mobilfunksender. Ihr Smartphone zeigt (mit einer passenden App) einen Empfangspegel von -70 dBm an. Die Signaldämpfung durch die Außenwand des Gebäudes sei 9 dB (typischer Wert). Wenn Sie in das Gebäude eintreten, und die Messung wiederholen: Welchen Wert werden Sie vermutlich erhalten?
8. Eine Stabantenne bestehe aus 3 Segmenten der Länge $\lambda/2$, die in eine Kunststoffröhre eingebaut sind. Mit welchem Antennengewinn ist in der horizontalen Richtung (Hauptrichtung) zu rechnen?
9. Warum besitzt ein Smartphone in der Regel nur eine einfache Dipol-Antenne?
10. Eine Mobilfunk-Antenne erzeugt ihren Antennengewinn in der Regel durch die Kombination von Dipolen in einem Array. Warum sind hier mehr Dipole übereinander als nebeneinander angeordnet?
11. Welche Eigenschaften zeichnen die digitale Modulation aus? Vorgegeben sind drei Kombinationen von Eigenschaften.
 - a. Übertragene Informationen sind wertdiskret
 - b. Übertragene Werte werden durch Symbole dargestellt
 - c. Jede Welle (Berg & Tal) kann ein Bit übertragen
 - d. Symbole haben ein zum übertragenen Wert proportionale Dauer
12. Was wird unter der Modulation von Wellen verstanden? Nennen Sie mindestens zwei Modulationsverfahren.
13. Richtig oder Falsch?
 - a. Ein Frequenzband erstreckt sich von der Mittenfrequenz symmetrisch zu beiden Seiten
 - b. Das Band enthält alle Frequenzen, die vom Sender erzeugt werden
 - c. Das Band ist so breit, dass alle Störungen für das Nachbarband unterhalb des tolerierbaren Rauschniveaus liegen.
 - d. Der Schutzabstand (Guard Band) dient zum Ausgleich von Sender-Ungenaugkeiten.
14. Mit welchem Verfahren prüft ein Mobilfunk-Empfänger, ob ein empfangener Block von Daten korrekt ist?
15. Nennen Sie Gründe für die hohe Bitfehlerrate bei Mobilfunk-Übertragungen.
16. Welche Maßnahmen werden im Mobilfunk ergriffen, um die anfallenden Übertragungsfehler zu korrigieren? Nennen Sie zwei Verfahren.
17. Was wird unter Vorwärts-Fehlerkorrektur verstanden?

18. Beschreiben Sie das Konzept eines „Rahmens“ im Zeitmultiplex
19. Wie viele Frequenzbänder werden beim Frequency Division Duplex (FDD) Verfahren mindestens eingesetzt?
20. Weshalb nutzen Zeit- und Frequenzmultiplex die vorhandenen Ressourcen nicht vollständig aus?
21. Orthogonales Frequenzmultiplex (OFDM) nutzt das vorhandene Spektrum besser aus als FDM. Begründen Sie diese Aussage.
22. Was ist Halb-Duplex? Wie verhalten sich die kommunizierenden Partner?
23. Ist TDD ein Halb-Duplex oder ein Duplex-Verfahren

Literatur

- Berrou C, Glavieux A, Thitimajshima P (1993) Near Shannon limit error-correcting coding and decoding: Turbo-codes. In: Proceedings of ICC '93 – IEEE International Conference on Communications (Band 2). IEEE, Geneva, S 1064–1070. <https://doi.org/10.1109/ICC.1993.397441>
- Bundesnetzagentur (2015) Entscheidung der Präsidentenkammer vom 28. Januar, Aktenzeichen: BKI-11/003 2015. Bundesnetzagentur. Bonn: Bundesnetzagentur. https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Frequenzen/OffentlicheNetze/Mobilfunk/DrahtloserNetzzugang/Projekt2016/PräsidentenkammerentscheidungProjekt2016_pdf.pdf?__blob=publicationFile&v=3. Zugriffen am 24.08.2021.
- European Commission (1999) COST Action 231: Digital mobile radio towards future generation systems: Final Report. Brussels. <https://op.europa.eu/de/publication-detail/-/publication/f2f42003-4028-4496-af95-beaa38fd475f>. Zugriffen am 24.08.2021.
- European Telecommunications Standards Institute (2017) LTE; Evolved Universal Terrestrial Radio Accees (E-UTRA); Physical Channels and Modulation (3GPP TS 36.211 version 14.2.0 Release 14). Sophia Antipolis Cedex. https://www.etsi.org/deliver/etsi_ts/136200_136299/136211/14.0.2.00_60/ts_136211v140200p.pdf. Zugriffen am 24.08.2021.
- Friedrichs B (1996) Kanalcodierung. Kanalcodierung. Springer, Berlin. <https://doi.org/10.1007/978-3-642-60985-5>
- Friis HT (1946) A note on a simple transmission formula. Proceedings of the IRE. IEEE, S 254–256. <https://doi.org/10.1109/JPROC.1946.234568>
- Kurose J, Ross K (2014) Computernetzwerke, 6. Aufl. Pearson, München. 978-3-868-94237-8
- Wiesbeck W (2005) Antennen und Antennensysteme, 2. Aufl. Universität Karlsruhe, Institut für Höchstfrequenztechnik und Elektronik, Karlsruhe



Lizenzierte Mobilfunksysteme

4

4.1 Einführung und Lernziele

Die in diesem Kapitel vorgestellten Mobilfunksysteme werden von staatlich lizenzierten Netzbetreibern auf exklusiv genutzten Frequenzen betrieben. Die Netzbetreiber sind kommerzielle Anbieter von Sprach- und Datenkommunikation, die das Recht zur Nutzung eines bestimmten Frequenzbandes über eine staatliche Ausschreibung oder Auktion erwerben. Der Betrieb der Netze folgt heute offenen internationalen Standards, die nach einem Generationen-Prinzip entwickelt werden (Kap. 7). Der Schwerpunkt liegt hier auf den Systemen der 4. Generation, die ab dem Jahr 2010 installiert und in Betrieb genommen wurden. Sie bilden das „Rückgrat“ der heutigen mobilen Datenkommunikation, und sie sind auch die Grundlage für die neueste Generation nach dem Standard „5G“. Die GSM-Systeme, die den Beginn des digitalen Mobilfunks Anfang der 1990er-Jahre bildeten, finden ebenfalls Berücksichtigung. Sie sind, obwohl technisch längst überholt, weltweit immer noch weit verbreitet. Hierzulande laufen noch viele technische und industrielle Anwendungen über sie. Die Systeme der 3. Generation („UMTS“, „HSPA“) werden mit der Einführung von 5G außer Betrieb genommen. Daher ist ihnen hier nur ein kurzer Abriss mit einigen technischen Erläuterungen gewidmet. Eine kurze Einführung in den viel diskutierten Mobilfunkstandard 5G schließt dieses Kapitel ab.

► **Lernziele**

- Sie verstehen die Entwicklung der Mobilfunkstandards
 - Sie wissen, wie die allgemeinen technischen Grundlagen aus Kap. 2 und 3 in konkreten Netzen umgesetzt werden
 - Sie haben ein genaueres Verständnis der Technik der Netze der zweiten und vierten Mobilfunkgeneration
 - Sie können die Technik der dritten Generation überblicksartig beschreiben
 - Sie kennen die wesentlichen Anforderungen an den neuesten Standard „5G“ und verstehen seine Grundelemente
-

4.2 Die Entwicklung der Standards der digitalen Mobilkommunikation

Die Anfänge der Entwicklung der mobilen Kommunikation wurden in Kap. 1 dargestellt. Der Erfolg von NMT bewog die skandinavischen Post- und Telekommunikationsverwaltungen, der EU die gemeinsame Entwicklung eines einheitlichen, offenen *digitalen* Mobilfunkstandards vorzuschlagen. Es wurde bei der Europäischen Konferenz der Post- und Telekommunikationsverwaltungen CEPT eine Arbeitsgruppe unter dem Titel *Groupe Spéciale Mobile* (GSM) eingerichtet, die später in das neu gegründete European Telecommunications Study Institute (ETSI) eingegliedert wurde. Europaweit wurden Netze nach dem GSM-Standard Anfang der 1990er-Jahre in Betrieb genommen. Die ursprüngliche Kapazität von 13 Millionen Teilnehmern reichte schon bald nicht mehr aus, so dass weitere Frequenzblöcke, sowohl im ursprünglichen 900 MHz-Spektrum als auch im 1800 MHz-Spektrum, zur Verfügung gestellt wurden. GSM wurde weltweit zum führenden Standard des digitalen Mobilfunks, so dass der Name unter Beibehaltung des Kürzels in *Global System for Mobile Communication* verändert wurde. Ab Mitte der 1990er-Jahre wurde – parallel zur Ausdehnung des Internets – die Möglichkeit geschaffen, über GSM-Netze auch Daten auszutauschen (Abschn. 4.3.1 und 4.3.2).

Gleichzeitig wurde auch international über einen Nachfolgestandard diskutiert, der dem ständig wachsenden Datenvolumen und der steigenden Teilnehmerzahl gewachsen war. Für die Entwicklung dieser sogenannten dritten Generation wurde mit dem *Third Generation Partnership Project* (3GPP) eine internationale Organisation aus 6 regionalen Gesellschaften geschaffen, der das European Telecommunications Study Institute (ETSI) als Europäische Vertretung angehörte. Das 3GPP lieferte – aufgrund regionaler Differenzen – zwei verschiedene, aber eng verwandte Standards ab: UMTS und CDMA2000, die ab dem Jahr 2000 weltweit in Betrieb genommen wurden. In der Weiterentwicklung wurde vom 3GPP auch der 4G/LTE-Standard (ab 2008) und neue 5G-Standard (ab 2018) veröffentlicht. Bei beiden handelt es sich zu guter Letzt um echte globale Standards, die weltweit einheitlich gehandhabt werden. Die von der 3GPP entwickelten Mobilfunkstandards sind offene Standards und stehen allen Interessenten ohne Kosten zum Download zur Verfügung (www.3gpp.org).

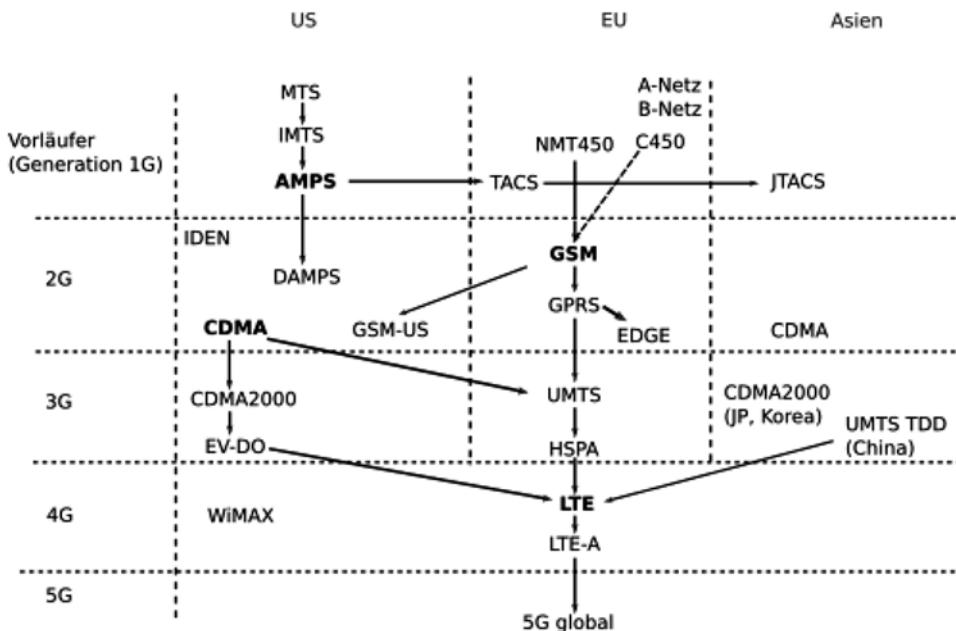


Abb. 4.1 Die Entwicklung der Mobilfunkstandards

Das Zusammenwachsen der unterschiedlichen Standards des Mobilfunks wird in der Abb. 4.1 veranschaulicht.

4.3 GSM Überblick

Das GSM-Netz hat sich in mehreren Stufen entwickelt. Das ursprünglich als reines Telefonnetz konzipierte GSM wurde sehr schnell auch zur Datenübertragung per Datenmodem genutzt. Mit der Erweiterung GPRS fügten die Hersteller und Betreiber die Möglichkeit zur paketvermittelten Übertragung von Daten hinzu. Die anfänglichen Datenraten waren mit praktisch erreichten ca. 50 kbit/s allerdings recht bescheiden, so dass mit dem Feature Enhanced Data Rates for GSM Evolution (EDGE) der Datenübertragung ein deutlicher Schub verliehen wurde. EDGE ist mit dem Symbol „E“ auf dem Smartphone heute den meisten Smartphone-Nutzern in Gebieten mit schwacher Netzabdeckung noch vertraut.

4.3.1 GSM-Systemarchitektur

Die Systemarchitektur eines GSM-Netzes ist in Abb. 4.2 dargestellt. Sie stellt einige Details zu der Übersicht in Abb. 2.1 dar. Dabei ist zu beachten, dass alle gezeigten Knoten mehrfach vorhanden sind. Die Sprachvermittlung wird mittels *Mobile Switching Centers*

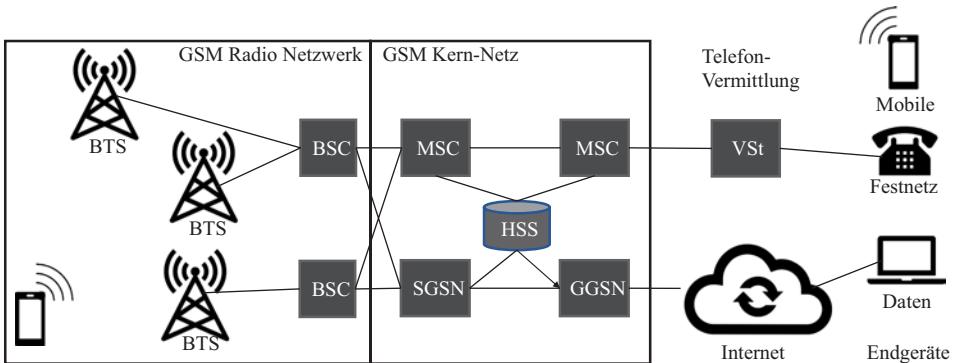


Abb. 4.2 Netzstruktur eines GSM-Netzwerkes für Sprache und Daten (GPRS)

(MSC) durchgeführt. *Gateway MSC* übernehmen die Vermittlung in andere Netze. Die MSC sind auch verantwortlich für den Kurznachrichtenverkehr. Die Schnittstelle zwischen Radio- und Kern-Netz wird durch die *Base Station Controller* (BSC) als Radio-Netz-Controller gebildet. Ein BSC steuert den Radio-Betrieb der angeschlossenen Basisstationen (Base Transceiver Station, BTS, Abb. 4.3), und ist in gewisser Weise das Gehirn dieser Basisstationen. Es herrscht eine strikte Hierarchie: Jede BTS ist eindeutig einem BSC zugeordnet, jeder BSC wiederum eindeutig einem MSC. Umgekehrt wird eine MSC für zahlreiche BSC, und eine BSC für zahlreiche BTS verantwortlich sein. Entsprechendes gilt für die Relation zu den *Serving GPRS Support Nodes* (SGSN), die für Datendienste die Rolle der MSC übernehmen.

Der BSC steuert den Handover eines Endgerätes von einer Zelle zu einer benachbarten Zelle, wenn beide betroffenen Basisstationen an diesem BSC angeschlossen sind. Ansonsten fällt diese Aufgabe an das übergeordnete MSC zurück; möglicherweise auch an das betroffene Paar von MSC, wenn das Endgerät den Anschlussbereich eines MSC verlässt. Der BSC hat auch die zusätzliche Funktion, die Datenpakete für die Übertragung per Funk vorzubereiten bzw. über Funk empfangene Datenpakete auszuwerten. Wie in Abb. 4.3 dargestellt, wird die Datenübertragung im GPRS Dienst durch die beiden Knoten *Serving GPRS Support Node* (SGSN) und *Gateway GPRS Support Node* (GGSN) geleistet. Ein mobiles Endgerät kann im Laufe einer Datensitzung zum Handover von Zelle zu Zelle mit mehreren SGSN verbunden sein; dabei bleibt der Übergangspunkt zum Internet oder externen Datennetz am GGSN unverändert.

Aufgrund des vom Endgerät angeforderten APN (Abschn. 2.3) identifiziert der SGSN den für das Zielnetz und den Aufenthaltsort des Endgerätes verantwortlichen GGSN und baut einen Datentunnel dorthin auf. Der GGSN vergibt die externe IP-Adresse für das Mobiltelefon und führt die Übersetzung von internen Netzadressen zu externen IP-Adressen durch. Zusätzlich ist der GGSN auch verantwortlich für die „Policy Control“ Funktion, durch die die tariflichen Beschränkungen des Teilnehmers durchgesetzt werden (Daten-Volumen, maximale Datenrate). Bestimmte Netzbetreiber-eigene Datennetze, wie

Abb. 4.3 Mobilfunk-Basisstation BTS-4, D1-Netz (GSM), 1993, Deutsches Technikmuseum Berlin



etwa das interne Multimedia Messaging Netz (MMS) haben dedizierte GGSN Knoten oder GGSN-Schnittstellen. Auch die Mitarbeiter eines Enterprise Großkunden können z. B. über eine dedizierte GGSN Schnittstelle an das eigene Unternehmensnetz durchgeschaltet werden.

4.3.2 GSM-Funkschnittstelle

Das GSM-Frequenzspektrum wird in schmale Bänder von jeweils 200 kHz Breite unterteilt. Die Zuteilung der Ressourcen an ein Endgerät zum Empfang oder zur Sendung von Daten erfolgt nach dem kombinierten FDMA/TDMA Verfahren (Abschn. 3.3.3 und Abb. 3.29). Es werden getrennte 200 kHz-Bänder für Uplink und Downlink Übertragung verwendet (FDD-Modus). Abb. 4.4 zeigt die Schnittstellen-interne Organisation der Daten. Im Zentrum steht der Rahmen (Frame) des Zeitmultiplex (Abschn. 3.3.3). Jedes verbundene Endgerät erhält einen der 8 Slots dieses Rahmens zugeteilt. Innerhalb dieses Slots werden 114 Datenbits in Symbole übersetzt übertragen, wie in Abb. 4.4 dargestellt. Jedes Symbol transportiert nach einem modifizierten BPSK-Verfahren genau ein Bit. Zur

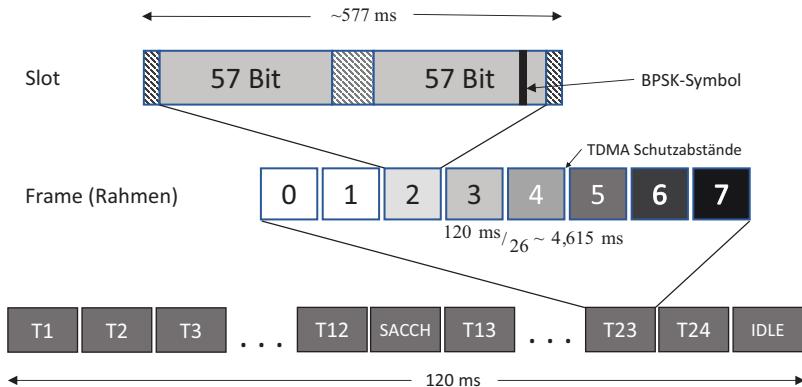


Abb. 4.4 GSM Rahmenstruktur für den Zeitmultiplex

zeitlichen Organisation werden je 24 Rahmen mit einem Kontrollrahmen und einem „Idle“-Rahmen zu einer übergeordneten Struktur von 120 ms Dauer zusammengefasst. Über den Kontrollrahmen (Slow Associated Control Channel, SACCH) tauschen Basisstation und Endgerät Informationen aus, wie zum Beispiel Laufzeit oder Sende- und Empfangsstärke. Mit dem „Idle“ Rahmen wird den sich anmeldenden Endgeräten der Beginn eines neuen Abschnittes angezeigt.

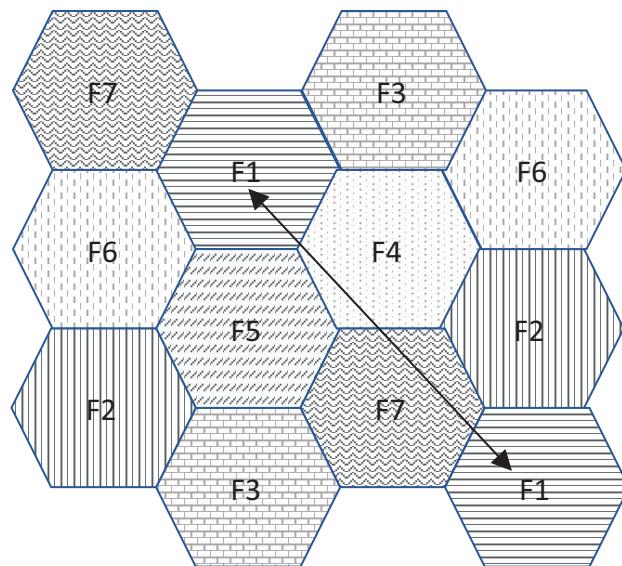
Die Slots 0 und 1 jedes Rahmens werden in der Regel für die Übertragung von Kontrollinformationen genutzt. Pro 200 kHz-Band sind an einem BTS-Standort daher maximal 6 parallele Telefongespräche möglich. Diese Kapazität reicht lediglich in sehr dünn besiedelten Gegenden aus. In der Regel wird daher eine sogenannte 3 x 3 Konfiguration eingesetzt: 3 Antennen mit um 120 Grad versetzten Abstrahlrichtungen senden und empfangen jeweils 3 verschiedene 200 kHz-Bänder. Das ergibt 9 Frequenzbänder und ermöglicht bis zu 54 parallele Sprachverbindungen pro Standort. In Stadtzentren und dicht besiedelten Gebieten werden noch deutlich größere Konfigurationen gewählt oder Standorte werden mit reduzierter Sendeleistung nahe beieinander gebaut, um die Kapazität weiter zu erhöhen.

In einem GSM-Netz muss streng darauf geachtet werden, dass sich die Signale benachbarter Basisstationen nicht gegenseitig stören. Es wird daher das einer Basisstation zugeordnete Frequenzband erst in einem größeren Abstand erneut verwendet. Abb. 4.5 zeigt eine einfache Netzplanungs-Konfiguration. Es werden dabei sieben Gruppen von Frequenzbändern F1 bis F7 definiert. Gleiche Bezeichnungen und Schattierungen der Basisstations-Sechsecke entsprechen gleichen Frequenzplänen. Der Doppelpfeil zeigt den Mindestabstand zweier Basisstationen mit gleichen Frequenzbändern.

4.3.2.1 Datenübertragung über die Funkschnittstelle im GSM

Ursprünglich wurde GSM als reines Sprach-Netz entwickelt und geplant. Für Datenübertragungen wird mit den beschriebenen 114 Bit pro $577 \mu\text{s}$ eine Datenrate von ca. 200 kbit/s über die gesamte Schnittstelle erreicht. Pro Kanal ergibt sich unter Berücksichtigung der nicht für den Nutzer verfügbaren Kapazität eine Rate von 20 kbit/s. Es wurde deshalb eine

Abb. 4.5 Frequenzplanung bei GSM-Netzen
(schematisches Beispiel)



leitungsvermittelte Datenübertragung mit bis zu drei gebündelten Kanälen im GSM technisch ermöglicht. Unter der Bezeichnung *High Speed Circuit Switched Data* (HSCSD) ergaben sich Datenraten von bis zu 60 Kbit/s. Da dies pro Teilnehmer schon 50 % eines Frequenzbandes belegte, handelte es sich um einen recht exklusiven Dienst für wenige Nutzer. Die Erweiterung GPRS (General Packet Radio System oder GSM Packet Radio System) stellte die gleiche Datenrate von 60 kBit/s pro Nutzer im paketvermittelten Modus für viele Teilnehmer gleichzeitig zur Verfügung. Das Netz (hier der BSC) stellt dabei angemeldeten Endgeräten dynamisch bis zu drei Slots pro Frame zur Verfügung. Drei weitere Slots wurden weiter für die Übertragung von Sprache benötigt.

4.3.2.2 Frequenzzuteilung

Insgesamt sind in Deutschland 175 Frequenzbänder in Bündeln für den Betrieb von GSM lizenziert worden. Das entspricht einer Gesamtallokation von 2 x 35 MHz (jeweils gepaart für Uplink und für Downlink) für GSM im 900 MHz-Frequenzbereich. Dazu kommen noch 225 Frequenzbänder im 1800 MHz-Bereich, die ursprünglich für die „neuen“ Netzbetreiber E-Plus und Viag Interkom (inzwischen beide Telefónica O2) lizenziert wurden, inzwischen aber wie die 900 MHz-Frequenzen gemischt lizenziert und genutzt werden.

4.3.2.3 Handover von Endgeräten bei GSM

Der Handover eines Endgerätes zwischen zwei Basisstationen wird bei GSM unterbrechungsfrei durchgeführt (Abschn. 2.5.4). Die Struktur des Netzes (Abb. 4.5) hilft bei der Durchführung, da benachbarte Zellen auf verschiedenen Frequenzen senden. Nach der Handover-Entscheidung durch das Kern-Netz baut das Endgerät eine neue parallele Ver-

bindung in der neuen Funkzelle auf. Die beiden Verbindungen stören sich nicht gegenseitig. Das Kern-Netz sorgt für parallele Datenströme zum Endgerät über beide Verbindungen. Zur Komplettierung des Handover wird einfach die Verbindung zur abgebenden Basisstation abgebaut.

4.3.2.4 EDGE

Die Einführung von GPRS im GSM hatte in erster Linie das Ziel, Datendienste für viele Teilnehmer zur Verfügung zu stellen. Gegen Ende der 1990er-Jahre konnten aber auch die Datenraten von bis zu 60 Kbit/s pro Teilnehmer nicht mehr befriedigen. Mit der Erweiterung *Enhanced Data Rates for GSM Evolution* (EDGE) wurde vor der Einführung von 3G versucht, den gestiegenen Bedürfnissen der Nutzer kurzfristig zu entsprechen. Es wurden dazu eine ganze Reihe von technischen Verbesserungen eingeführt. Wesentlich verantwortlich für die Steigerung der Datenraten war eine Veränderung des Modulationsschemas. Statt der BPSK-Modulation wie bei GSM wurde die 8PSK-Modulation eingeführt (Kap. 3, Abb. 3.20c), mit der die dreifache Übertragungsrate von bis zu 180 Kbit/s über das gleiche Frequenzband möglich wurde. EDGE nutzte dabei die gleichen Slots wie GSM und konnte so auf einer Schnittstelle kombiniert mit GSM Sprache und GPRS genutzt werden. EDGE ist bis heute als Rückfall-Option bei schlechter Abdeckung durch die neueren Standards flächendeckend verfügbar. Im Smartphone-Display wird die Nutzung von EDGE vom Netzbetreiber in der Regel durch den Buchstaben E angezeigt.

4.3.3 GSM Besonderheiten und Ausblick

Der GSM-Standard besteht seit mehr als 30 Jahren. Drei Nachfolge-Generationen sind in der Zwischenzeit entwickelt worden. Dennoch ist er nicht nur historisch relevant. Weltweit sind heute immer noch etwa 20 % der Endgeräte reine GSM-Telefone (Ericsson 2020). In Deutschland ist es bis heute die einzige digitale Mobilfunk-Technologie, die flächendeckend zur Verfügung steht. Das liegt vor allem an der großen Reichweite der Mobilfunksignale im 900 MHz-Bereich und an dem flächendeckenden Netzausbau in den 1990er-Jahren. Wie im übrigen Westeuropa ist in Deutschland der Anteil der „nur GSM“-Mobilfunkverträge allerdings auf unter 5 % gesunken, wobei es sich es sich meist um Maschine-zu-Maschine-Anwendungen (M2M) handelt. Das seit 2018 für Neuwagen in der EU vorgeschriebene eCall für automatische Notrufe bei Autounfällen wird über GSM abgewickelt. Der Verband der Automobilindustrie verlangt deshalb eine Bestandsgarantie für GSM bis 2035 (Verband der Automobilindustrie 2019).

Dank der langen Entwicklungs- und Optimierungserfahrung und der Beschränkung auf nur zwei Frequenzbänder (900 MHz und 1800 MHz; 1900 MHz in den USA) liegen die Kosten für ein komplettes M2M Radiomodul heute bei deutlich unter 10 € (Liberg et al. 2018, Abschn. 3.1.2.4). Das macht GSM derzeit zur Technologie der Wahl für viele M2M-Anwendungen, insbesondere wenn Laufzeiten, Datenraten und Zahl der zu vernetzenden Endgeräte noch keine herausragende Rolle spielen. Beispiele hier sind mobile

Kreditkartenterminals, intelligente vernetzte Stromzähler (Smart Metering) sowie eHealth Anwendungen im Bereich der Haus-Versorgung.

In der fortlaufenden GSM-Standardisierung sind zahlreiche Neuerungen vor allem bezüglich der Reichweite und des Stromverbrauchs (Power Saving Mode) aus der modernen Entwicklung übernommen worden. In dem auf klassischem GSM basierenden IoT-Standard Enhanced Coverage GSM (EC-GSM) wurden Elemente aus der dritten und vierten Generation zur Verbesserung der Reichweite und zur Energieeinsparung eingeführt (Liberg et al. 2018). Die Endgeräte der meisten M2M-Anwendungen wie Kreditkartenterminals oder Stromzähler sind in der Regel nicht oder nur geringfügig mobil, was die Erfordernisse an das Handover zwischen Basisstationen reduziert. Daher ist auch die Möglichkeit einer Reduktion der verfügbaren GSM-Frequenzbänder untersucht worden. Ein M2M-Netzwerk auf GSM-Basis lässt sich mit nur 600 kHz verfügbarem Spektrum betreiben (Liberg et al. 2018). Mit dieser Beschränkung kann GSM in Europa als M2M-Medium für geraume Zeit weiter existieren, auch wenn der größte Teil des ursprünglich lizenzierten Spektrums mittlerweile für Nachfolge-Systeme genutzt wird.

4.4 Systeme der dritten Generation

Wie schon weiter oben angekündigt, werden die 3G-Systeme lediglich überblicksartig behandelt. 3G wurde weltweit in zwei Varianten unter der Bezeichnung *Universal Mobile Telecommunication System* (UMTS) standardisiert: Die europäische Variante nach dem Standard Wideband CDMA (W-CDMA) und das nordamerikanische CDMA2000 wurden weltweit von den Mobilfunkbetreibern implementiert. Die 3G-Technologie nutzt im Vergleich zu GSM das zugeteilte Spektrum deutlich besser aus. Weltweit sind im Jahr 2020 noch 20 % aller Endgeräte auf dem 3G-Standard, allerdings mit abnehmender Tendenz. Weil die Nachfolgesysteme 4G und 5G für den Ausbau in der Fläche, insbesondere in ländlichen Gebieten, die von 3G belegten Frequenzbänder benötigen, werden die 3G-Systeme in Europa und den USA bis 2022 abgeschaltet

4.4.1 Die Architektur von W-CDMA-Netzen

Die Architektur eines W-CDMA-Netzes (Abb. 4.6) ist auf den ersten Blick fast identisch mit der Architektur eines 2G-Netzes, wie in Abschn. 4.3.1 beschrieben. Der einzige in der Übersicht erkennbare Unterschied besteht in der Vernetzung der Radio Network Controller (RNC), die die Base Station Controller (BSC) bei GSM ersetzen, und die das 3G-Radio-Netz (UTRAN) unabhängig vom Kern-Netz steuern. Die neuen 3G-Basisstationen mit der Bezeichnung NodeB sind jeweils genau einem RNC zugeordnet. Das Kern-Netz beauftragt das Radio-Netz durch die Knoten MSC bzw. SGSN mit der Einrichtung einer mobilen Verbindung zu einem Teilnehmer oder Endgerät mit Qualitätsparametern wie Datenrate oder erlaubte Laufzeitverzögerung. Der RNC stellt gemeinsam mit der NodeB

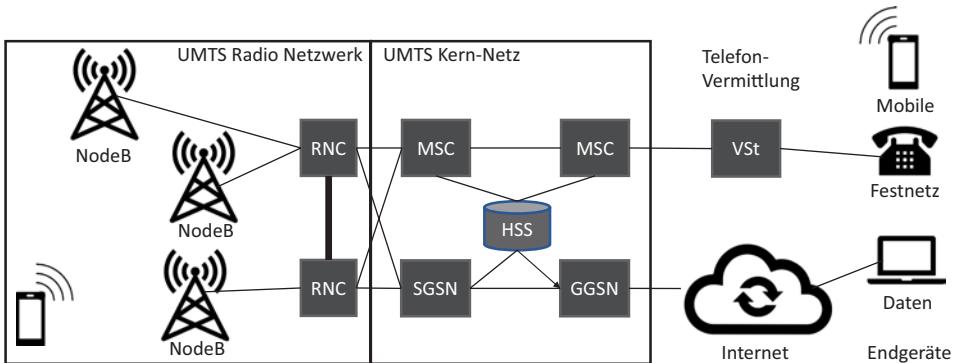


Abb. 4.6 UMTS W-CDMA-Netzarchitektur mit RNC-Vernetzung

die gewünschte Verbindung zum Endgerät her und steuert und überwacht sie. Insbesondere die Steuerung des Handover zu einer Nachbarzelle, die an eine andere NodeB angeschlossen ist, erfolgt durch den RNC.

4.4.2 Die 3G-Radioschnittstelle

Mit der Einführung des Mobilfunks der dritten Generation haben sich einige Anpassungen ergeben, die im Folgenden kurz erläutert werden sollen.

4.4.2.1 Qualitätsparameter von Verbindungen

In 3G sind Sprache und Datenverkehr gleichberechtigte Formen der Nutzung und werden bei der Zuweisung durch ein gemeinsames Protokoll und gemeinsame Vergabeverfahren gleichbehandelt. Daten werden also nicht durch Bündelung von Sprach-Ressourcen wie bei GPRS übertragen. Stattdessen wird für jede Nutzungsart eine Verbindung mit einer definierten Qualitätsklasse vom Kern-Netz angefordert und vom UMTS Radio-Netz bereitgestellt. Die möglichen Qualitätsklassen einer Verbindung sind

- Conversational (typisch für Sprachverbindung, Übertragung in Echtzeit mit minimalen Verzögerungen, konstante Bitrate)
- Streaming (typisch für Video-Streaming, Übertragung nahe Echtzeit, Erhalt der zeitlichen Ordnung der Pakete, begrenzte Laufzeitverzögerungen, garantierte minimale Bitrate)
- Interactive (typisch für Web Browsing, keine Echtzeit-Anforderung, korrekte Übertragung der Nutzdaten, variable Bitrate)
- Background (typisch für Telemetrie oder E-Mail, Übertragung nach Verfügbarkeit von Ressourcen, keine Anforderungen an Verzögerungen, korrekte Übertragung der Nutzdaten)

Die Qualitätsklassen werden im UMTS Radio-Netz in eine Liste von technischen Attributen der Verbindung übersetzt, die dann vom NodeB umgesetzt werden.

4.4.2.2 Frequenzen, Modulation und Codierung

Im Gegensatz zur kleinteiligen Frequenzverteilung durch 200 KHz-Bänder bei GSM erhält ein 3G-Netzwerk nach dem UMTS-Standard ein Frequenzband von 2 x 5 MHz zugewiesen. Alle Basisstationen dieses Netzes nutzen das gleiche Frequenzband. Gleichfalls senden alle Endgeräte im Netz im gemeinsamen 5 MHz-Frequenzband für die Uplink-Richtung. Die übertragenen Daten werden durch Codes in zwei Stufen unterschieden: Jedes sendende Gerät signiert seine Daten mit einem sogenannten Scrambling Code, der vom NodeB zugewiesen wird. Jeder Verbindung wird zusätzlich ein CDMA-Code (Abschn. 3.3.3) zugeordnet. Sprachverbindungen benötigen nur eine geringe Bandbreite und erhalten zur Qualitätssicherung einen langen Code. Mit dem verbundenen hohen Prozessgewinn sind sie nur wenig anfällig für Störungen. Der Breitbandverbindungen zugewiesene kurze CDMA-Code ergibt nur einen geringen Prozessgewinn und die Verbindung ist stärker anfällig für Fehler (Tab. 4.1).

4.4.2.3 Handover bei UMTS

Der Handover eines Endgerätes von einer Funkzelle zu einer benachbarten muss auch bei UMTS unterbrechungsfrei erfolgen, da Sprachverbindungen betroffen sein können. Ein einfacher Aufbau von parallelen Verbindungen ist jedoch problematisch, da in allen Zellen sowohl im Uplink als auch im Downlink die jeweils selben Funkfrequenzen genutzt werden. Die parallelen Verbindungen würden sich also massiv stören. Aus diesem Grunde wurde mit dem sogenannten „Soft Handover“ ein anderer Ablauf gewählt.

Wenn das Netz durch die übertragenen Daten feststellt, dass die Verbindungsqualität unter eine definierte Schranke fällt, wird das Endgerät in einen Handover-Zustand versetzt. In diesem Zustand empfängt und sendet es simultan und synchron identische Daten von und zu bis zu drei Funkzellen, dem *Aktiven Set*, die im Empfänger überlagert werden. Die Qualität der Übertragung von jeder der Basisstationen wird separat registriert. Fällt eine dieser Basisstationen unter eine definierte Schwelle, wird sie aus dem Aktiven Set entfernt. Am Ende bleibt nur eine Funkzelle übrig und der Handover-Zustand wird wieder verlassen.

4.4.2.4 HSPA Erweiterung

Schon kurz nach Einführung von 3G wurde klar, dass die ursprünglich geplanten Datenraten mit der Entwicklung des leitergebundenen Internets nicht Schritt halten würden.

Tab. 4.1 Mögliche Datenraten bei UMTS

| CDMA-Code Spreizfaktor | 8 | 16 | 32 | 64 | 128 | 256 |
|---------------------------|-------|-------------|-------------|-------|-------------------|-------------------|
| Nutzer-Datenrate (kbit/s) | 384 | 128 | 64 | 32 | 12 | 5 |
| Anwendung | Daten | Daten/Video | Daten/Video | Daten | Sprache Kontrolle | Sprache Kontrolle |

High Speed Packet Access HSPA ist eine Erweiterung, die diesem Umstand Rechnung trägt. HSPA baut auf der Radio-Schnittstelle von UMTS auf. Es ist mit W-CDMA innerhalb der Zelle kompatibel. Für Sprachverbindungen und den Austausch von Kontrollnachrichten zwischen Endgerät und NodeB bleibt immer ein Teil der Kapazität für W-CDMA reserviert. Der HSPA-Anteil wird über einen festen Satz von CDMA-Codes realisiert, die allen Teilnehmern im Multiplex zur Verfügung stehen und dynamisch auf Anforderung vergeben werden. Es handelt sich um beim HSPA-Anteil um einen reinen Datendienst. Mittels höherer Modulationsverfahren (16QAM anstelle QPSK), Nutzung von mehreren 5 MHz-Bändern, sowie der sogenannten MIMO Technik, übernommen aus der LTE-Entwicklung (Abschn. 4.5.3.1), können theoretisch bis zu 84 Mbit/s pro Zelle übertragen werden.

4.5 Systeme der vierten Generation nach dem LTE-Standard

Die vierte Generation des digitalen Mobilfunks 4G löste die dritte Generation seit 2010 ab. W-CDMA konnte mit den wachsenden Ansprüchen an Datenraten und an Teilnehmerzahlen nicht Schritt halten. *Long Term Evolution* (LTE) als technische Grundlage der Systeme der vierten Generation erlaubt eine bis dahin nicht erreichte Effizienz in der Nutzung von verfügbarem Spektrum. Gleichzeitig ist LTE flexibler als 3G durch die Nutzung von vielen Frequenzbändern unterschiedlicher Breite. Schließlich ermöglicht LTE die Einbettung von Speziallösungen zur M2M-Kommunikation.

Zentrale Design-Ziele bei LTE waren

- Signifikante Erhöhung der Datenraten auf 100 Mbit/s im Downlink und bis zu 50 Mbit/s im Uplink mit Bezug auf 20 MHz Bandbreite
- Weniger als 10 ms Laufzeitverzögerung zwischen Endgerät und Basisstation
- Unterstützung von Frequenzbändern von 1,4 MHz, 3 MHz, 5 MHz, 10 MHz, 15 MHz, 20 MHz statt einer einheitlichen 5 MHz Bandbreite wie bei 3G
- Unterstützung mobiler Geräte bis 500 km/h, z. B. für Hochgeschwindigkeitszüge
- Reduktion von Übertragungskosten und Energieverbrauch am Endgerät
- Vereinfachung der Netz-Architektur

4.5.1 LTE-Netzwerk Architektur

Ein Netzwerk nach dem LTE-Standard ist ein reines IP-Datennetzwerk, Ende-zu-Ende vom mobilen Endgerät bis zum Internet Server. Die für die vorhergehenden Generationen fundamentalen Sprachdienste werden in der Architektur oberhalb der IP-Schicht als Applikationen angesiedelt.

Abb. 4.8 zeigt die im Vergleich zur 3G-Architektur (Abb. 4.6) flache Netzstruktur eines LTE-Netzes. Der neue LTE-Radio-Knoten wird als *evolved NodeB* (eNodeB oder kurz

eNB) bezeichnet. Die Radio-Netzwerk Controller (2G: BSC, 3G: RNC) entfallen; damit entfällt eine ganze Netzwerkebene. Die Aufgaben des 3G-RNC gehen teilweise auf den eNodeB über. Der übrige Teil wird vom Kern-Netz übernommen. Die vernetzten eNodeB werden damit zu komplexen Steuerungsknoten. Sie regeln selbstständig den Datenverkehr zum mobilen Endgerät: Sie vergeben Übertragungsrechte, kontrollieren die Qualität der Verbindung, sie messen und steuern die Ausgangsleistung des Endgerätes und sind verantwortlich für die Fehlerkorrektur. Ein eNodeB stößt aufgrund der vom mobilen Endgerät empfangenen Rückmeldung einer schlechten Signalqualität auch eigenständig einen Handover zu einem besser positionierten Nachbar-eNodeB an, und führt sie in der Regel auch mit diesem durch. Abb. 4.7 zeigt eine moderne eNodeB in modularer Bauweise, bei der die Aufbereitung und Analyse von übertragenen Daten in einem Hochleistungsrechner, der Baseband-Unit (BBU), konzentriert ist. Die BBU ist verantwortlich für die Formatierung der Sendesignale und die Decodierung der Empfangssignale. Die sogenannten Radio-Heads erzeugen das hochfrequente Sendesignal und transformieren das empfangene Signal zurück auf das Baseband. Sie sind zur Vermeidung von Verlusten nahe bei den Antennen untergebracht und mit der BBU durch Datenkabel verbunden. Die BBU muss sich auch nicht am selben Standort befinden, und kann in einer geschützten Umgebung installiert sein. Der Schrank in der Bildmitte enthält Batterien zur Notstromversorgung und neben der BBU die Elektronik der Übertragungstechnik sowie IP-Netztechnik.



Abb. 4.7 Moderne eNodeB in modularer Bauweise von Ericsson

Im Kern-Netz entfallen alle ausschließlich mit dem Sprachverkehr befassten Knoten, also in erster Linie das MSC. Im Datenzweig erfolgt eine Aufteilung der Aufgaben des SGSN auf zwei Knoten. Das *Serving-Gateway* (S-GW) bildet zusammen mit dem aus dem GGSN hervorgegangenen Packet Data Network Gateway (PDN-GW) die Daten-Pipeline, über die der Datenverkehr ins Internet fließt. Die gesamte Steuerintelligenz wird in die Mobility Management Entity (MME) verlagert. Die MME ist das „Gehirn“ des Netzwerkes und übernimmt die gesamte Steuerung der Datenverbindungen. MME und S-GW stehen nicht in einer 1:1 Beziehung; die MME deckt in der Regel einen sehr viel größeren Einzugsbereich ab.

Die MME regelt den Verbindungsaufbau, überprüft die Identität des Teilnehmers und identifiziert das zu einem APN gehörende Gateway. Sie fordert die Vergabe von IP-Adressen an, kontrolliert die Mobilität des Teilnehmers, und routet den Datenverkehr nach einem Handover gegebenenfalls zu einem neuen Serving-Gateway, unter Beibehaltung des anfänglich bestimmten Packet Data Network Gateway. Nach dem Wegfall des MSC geht die Abwicklung des Messaging-Betriebs (SMS) auf die MME über.

Das PDN-GW entspricht im Prinzip dem GGSN bei 2G und 3G. In seiner Grundfunktion ist es ein IP-Router, der zwischen dem Kern-Netz des Mobilfunkes und dem Internet bzw. anderen Datennetzen vermittelt. Es vergibt die öffentliche IP-Adresse des Mobiltelefons und speichert sie für den Datenverkehr ins Internet. Es ist zuständig für die Policy-Überwachung bezüglich Datenraten, Datenvolumina und Firewall-Richtlinien für jedes angeschlossene Endgerät. Die entsprechenden Informationen werden allerdings nicht im PDN-GW selbst gespeichert, sondern von Verwaltungs-Servern (Policy Server) beim Verbindungsaufbau abgerufen (Abb. 4.8).

4.5.2 Die LTE-Funkschnittstelle

Im Folgenden werden die Charakteristika der LTE-Funkschnittstelle erläutert.

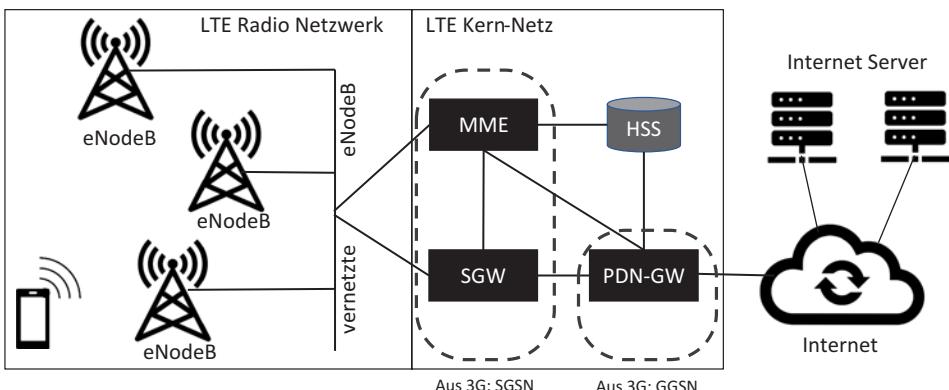


Abb. 4.8 Architektur des LTE-Netzes

4.5.2.1 LTE-Frequenzspektrum

Der LTE-Standard unterstützte von Beginn an eine Reihe von Bandbreiten: 1,4 MHz, 3 MHz, 5 MHz, 10 MHz, 15 MHz und 20 MHz. Die für die internationale Frequenzregulierung verantwortliche ITU-R reservierte international mehr als 80 Frequenzbänder im Bereich zwischen 450 MHz und 2,6 GHz für die Nutzung durch LTE. Nicht alle diese Bänder sind bereits in nationales Recht überführt; in einigen Fällen besteht noch eine staatliche oder anderweitig vertraglich verbrieft alternative Nutzung. Einige dieser Frequenzen werden auch bereits im Hinblick auf den 5G-Standard diskutiert. Die liberale Handhabung der Frequenzen wird durch die Struktur der LTE-Radio-Schnittstelle ermöglicht. Die Hersteller von Netzwerk-Komponenten und Endgeräten konzentrieren sich aber in der Hauptsache auf die Entwicklung von Komponenten für die Frequenzbänder, für die die größten Volumina am Weltmarkt zu erwarten sind, so dass nicht für alle reservierten Frequenzen Netzausrüstung und Endgeräte zur Verfügung stehen. Ein weltweit kompatibles GSM-Mobiltelefon benötigte für die vier international vergebenen Frequenzbereiche 800, 900, 1800 und 1900 MHz lediglich eine Antenne. Ein weltweit kompatibles LTE-Endgerät müsste Dutzende von Antennen für die genutzten Frequenzen besitzen. Zum Beispiel gibt es daher das im Jahr 2020 veröffentlichte Apple iPhone 12 in vier nationalen bzw. regionalen Varianten, die sich durch die Unterstützung verschiedener LTE-Frequenzkombinationen unterscheiden.

4.5.2.2 LTE-Frequenzen in Deutschland

In Deutschland wurden im Jahre 2010 und 2015 Frequenzblöcke in den Bereichen 1800 MHz und 2600 MHz versteigert. Genutzt werden diese Frequenzblöcke von den drei Netzbetreibern in der Regel für LTE 2x10 MHz und LTE 2x5 MHz. Die heute insgesamt für LTE in Deutschland zur Verfügung stehenden Frequenzen sind in der nachstehenden Tabelle aufgeführt (Tab. 4.2). Die Bezeichnung der Bänder entspricht der durch die ITU-R vorgegebenen Numerierung.

Jedem LTE-Netz ist ein festes Frequenzband in einer der in Abschn. 4.5.2 angegebenen Bandbreiten zugeordnet. Da in Europa das FDD Verfahren für LTE genutzt wird (Abschn. 3.3.3), ist dieses Band als Paar vergeben. Ein Frequenzband ist für den Downlink reserviert; mit einem ausreichenden Duplex-Abstand davon getrennt gibt es ein gleich breites Band für den Uplink. Alle eNodeB senden auf demselben Downlink-Frequenzband, alle Endgeräte des Netzes senden auf demselben Uplink-Frequenzband.

4.5.2.3 Die LTE-Rahmenstruktur

LTE verwendet verschiedene Stufen des QAM-Modulationsverfahrens (Abb. 3.20) und OFDMA als Zugriffs- und Multiplexverfahren. Die Symbolfrequenz wurde mit 15 kHz festgelegt; damit liegt die Breite der OFDMA-Streifen ebenfalls bei 15 kHz. Durch Ausgleichs- und Schutzabstände werden 14.000 Symbole pro Sekunde gesendet. Der Zugriff auf das LTE-Frequenzband erfolgt jeweils durch Allokation einer Gruppe benachbarter OFDM-Unterbänder von je 15 kHz Breite. Die zugrunde liegende Struktur ist in Tab. 4.3 für eine 3 MHz-Schnittstelle dargestellt. In der Senkrechten werden Frequenzen in Form

Tab. 4.2 In Deutschland zugeteilte LTE-/4G-Frequenzen

| Bezeichnung/ Nummerierung | Frequenzbereich | Totaler Bandbreite (Uplink+Downlink) | Ehemalige Verwendung |
|------------------------------|-----------------|---|--|
| Band 1 | 2100 MHz | 2x60 MHz | UMTS, noch bis 2021 genutzt |
| Band 2 | 1800 MHz | 2x60 MHz | GSM „E-Netz“ Frequenzen |
| Band 7 | 2600 MHz | 2x70 MHz | Bisher nicht genutzte Frequenzen |
| Band 8 | 900 MHz | 2x35 MHz | GSM „D-Netz“ Frequenzen, teilweise genutzt |
| Band 20 | 800 MHz | 2x30 MHz | „Digitale Dividende I“, Fernsehsender |
| Band 28 | 700 MHz | 2x45 MHz | „Digitale Dividende II“, Fernsehsender |
| Band 32 | 1500 MHz | 40 MHz | Nur Downlink, gebündelt mit einem anderen Band (Carrier Aggregation) |
| Band 72 | 450 MHz | 2x5 MHz | Nicht öffentlich, für „kritische Kommunikation“ |

Tab. 4.3 Tabelle der maximal erzielbaren Datenraten in Mbit/s im Downlink über LTE (Johnson 2012)

| | 1,4 MHz | 3 MHz | 5 MHz | 10 MHz | 15 MHz | 20 MHz |
|-------|---------|-------|-------|--------|--------|--------|
| QPSK | 1,0 | 2,6 | 4,4 | 8,8 | 13,2 | 17,6 |
| 16QAM | 2,0 | 5,2 | 8,7 | 17,6 | 26,4 | 35,3 |
| 64QAM | 2,9 | 7,8 | 13,1 | 26,4 | 39,6 | 52,9 |

von nebeneinander liegenden 15 kHz-Streifen abgetragen, und in der waagerechten Richtung läuft die Zeit. Immer 12 der 15 kHz-Streifen werden zu einer Gruppe von $12 \times 15 \text{ kHz} = 180 \text{ kHz}$ Bandbreite zusammengefasst. Diese Gruppe wird *Physikalischer Ressource-Block* (PRB) genannt. Der PRB ist die kleinste Frequenz-Einheit, auf den ein Endgerät Zugriff hat.

In der Zeit-Dimension ist die Basiseinheit der Rahmen von 10 ms Dauer. Jeder Rahmen ist unterteilt in 10 *Subframes* von je einer Millisekunde Dauer. Jeder Subframe ist unterteilt in 2 *Slots*, die je 7 Symbole enthalten. Insgesamt enthält ein Subframe damit 14 Symbole. Das dunkel schattierte Rechteck in Tab. 4.3 zeigt ein Subframe in der Zeitdimension und 1 PRB in der Frequenzdimension. In der Detaildarstellung zeigen sich die $12 \times 14 = 168$ enthaltenen QAM-Symbole. Je nach Modulationsvorschrift lassen sich dort 336 Bits (QPSK), 672 Bits (16QAM) oder 1008 Bits (64QAM) unterbringen. Die kleinste Einheit, die einem Endgerät vom eNodeB zum Senden oder Empfangen von Daten zugewiesen werden kann, ist 1 Slot x 1 PRB.

Die innere Struktur des LTE-Rahmens wird beispielhaft für die Downlink-Richtung im FDD-Verfahren betrachtet. In dieser Betrachtung werden nur die wichtigsten Elemente, wie sie in Abb. 4.9 gezeigt sind, diskutiert. Zahlreiche weitere Elemente in Uplink- und in

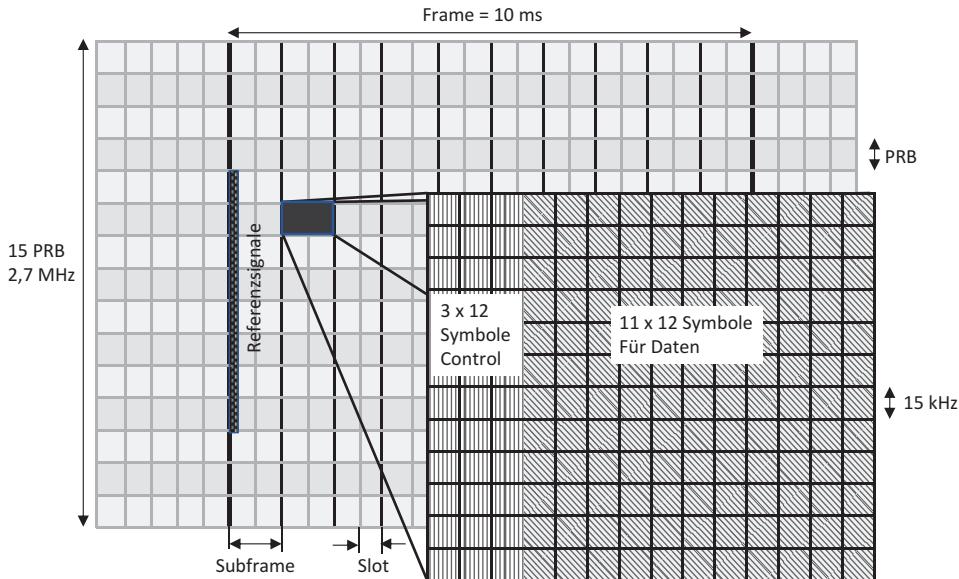


Abb. 4.9 LTE-Rahmen-Struktur Downlink 3 MHz

Downlink-Richtung dienen der Feinkontrolle des Ablaufs an der Schnittstelle. In jedem Subframe sind die ersten bis zu drei der 14 Symbole der Übermittlung von Kontrollnachrichten an das Endgerät reserviert. Die Kontrollnachrichten dienen zum Beispiel dazu, dem Endgerät anzukündigen, welche PRB seine Daten enthalten oder dem Endgerät Sendeberechtigung für bestimmte PRB einzuräumen. Mit jedem Datenblock kommen Demodulations-Anweisungen mit der Information über das verwendete Modulationsverfahren an das Endgerät. Es können aber auch Statusabfragen an das Endgerät erfolgen. Im schattierten Streifen zu Beginn des Rahmens und in der Mitte des Frequenzbereiches teilt der eNodeB seine Referenzinformationen für die Anmeldung mit. Dies sind zum Beispiel die Identität des Netzes und des eNodeB, Muster zur Synchronisation, sowie die Zeitpunkte für die Übersendung zur Anmeldung.

Beim TDD-Verfahren wird der gezeigte Rahmen zwischen der Uplink- und der Downlink-Richtung geteilt. Die Kommunikation beginnt mit dem Downlink-Teil; nach einer kurzen Sicherheitsperiode folgt dann der Uplink-Teil. Der Teilungspunkt zwischen Uplink und Downlink ist in jeder Zelle konfigurierbar. Ein Vorteil liegt darin, dass das Verhältnis zwischen Uplink- und Downlink-Datenvolumen flexibel asymmetrisch gestaltet werden kann. Auch können Downlink gesendete Anweisungen an das Endgerät bereits im selben Rahmen, also binnen 10 ms, beantwortet werden.

Die in Tab. 4.3 gezeigte Schnittstellenstruktur eines 3 MHz-LTE-Bandes umfasst 15 PRB. Da die Breite eines PRB $12 \times 15 \text{ kHz} = 180 \text{ kHz}$ beträgt, ist die tatsächliche Bandbreite von 15 PRB, wie auch in der Abbildung dargestellt 2,7 MHz. Die fehlenden 300 kHz sind als Guard-Band gegenüber dem nächsten Frequenzband vorgesehen. Grundsätzlich

wird bei jeder LTE-Bandzuweisung 10 % der Bandbreite als Guard Band reserviert. Mit den 15 PRB und 1000 Frames pro Sekunde ergibt sich die Brutto-Transportrate der 3 MHz-Schnittstelle zu $15 \times 1000 \times 336 \text{ Bit/s} = 5 \text{ Mbit/s}$, wenn die Daten QPSK-moduliert sind. Mit 64 QAM erreicht die 3 MHz-Schnittstelle dann schon das Dreifache, nämlich 15 Mbit/s.

Allerdings steht diese Leistung dem Teilnehmer an seinem mobilen Endgerät nicht exklusiv zur Verfügung. Grundsätzlich handelt es sich bei LTE wie bei allen Mobilfunk-Systemen um ein Multiplex-System. Die Bandbreite wird zwischen allen eingebuchten Teilnehmern verteilt. Ein Teil der Kapazität wird für Kontrolle, Referenz und Signalisierung verwendet. Bei nicht optimalen Radio-Bedingungen werden zusätzlich Modulations-Schema und Fehlerrichtigung angepasst. Die Tabelle Tab. 4.3 zeigt die in der Praxis insgesamt maximal erreichbaren Werte pro Zelle in Abhängigkeit von der Bandbreite und dem Modulations-Schema.

Der eNodeB legt für jede Verbindung dynamisch das Modulations-Schema und die Fehlerrichtigung-Rate (Coding Rate) fest. Die Coding Rate ist das Verhältnis von Nutzdaten zu den gesamten übertragenen Daten. Bei einer niedrigen Coding Rate von 0,35 sind 65 % der übertragenen Datenmenge Vorräts-Fehlerkorrekturdaten. Bei einer hohen Coding Rate von 0,75 werden lediglich 25 % durch Korrekturdaten belegt. Durch diese Prozedur wird die den meisten Smartphone-Nutzern bekannte Abhängigkeit der eigenen Datenrate von der Empfangsstärke („Anzahl der Balken im Display“) und anderen Faktoren erklärt. In Abb. 4.10 ist das Schema grafisch dargestellt. Für eine beispielhafte Anwendung wird angenommen, dass das Netz eine 10 MHz-Bandbreite verwendet. Befindet sich der Nutzer mit seinem mobilen Endgerät in unmittelbarer Nähe des eNodeB, sind die Empfangsbedingungen optimal. Der eNodeB und das Endgerät setzen die 64QAM Modulation ein. Da die Fehlerrate gering ist, werden nur sehr wenige Korrektur-Bits benötigt (Forward Error Correction, FEC). Die Coding-Rate ist 0,85. Die Datenrate wird

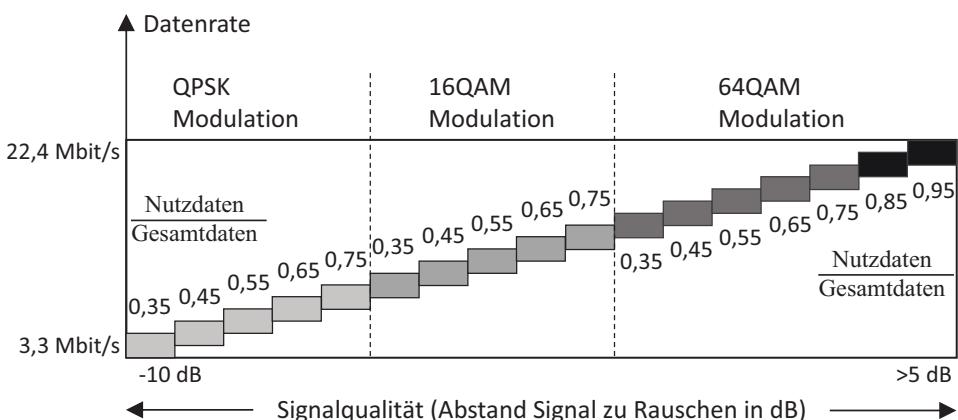


Abb. 4.10 Modulationsschema und Coding Rate in Abhängigkeit von der Signalqualität (nach Johnson 2012)

ca. 22,4 Mbit/s betragen. Bei wachsender Entfernung vom eNodeB wird das Signal schwächer und der eNodeB wird die Verwendung von immer höheren Fehlerkorrektur-Anteilen festlegen, bis die Coding Rate auf 0,35 abgesunken ist (65 % Korrektur-Bits). Die erreichbare Datenrate ist auf unter 10 Mbit/s gesunken. Entfernt sich der Nutzer weiter, können eNodeB und Endgerät die 64QAM Modulation aufgrund der ansteigenden Fehlerhäufigkeit nicht mehr aufrechterhalten und wechseln auf 16QAM, das mit 13 Mbit/s eine bessere Datenrate verspricht. Bei noch weiterer Entfernung oder dem Auftreten von Störungen sinkt die Datenrate auf etwa 6 Mbit/s, bevor auf die Modulation QPSK umgeschaltet wird. Die über LTE erreichbare Datenrate kann dann noch auf 3,3 Mbit/s absinken, bevor der eNodeB versucht, das mobile Endgerät auf eine andere Technologie (2G/EDGE oder 3G) zu übergeben. Die Werte dieses Beispiels gelten nur, wenn der Nutzer mit seinem Endgerät allein in der Zelle ist; in der Regel werden die Datenraten nach einem „Fair-Usage“ Prinzip aufgeteilt und die erreichten Datenraten sind geringer.

4.5.2.4 Mobile Verbindungen

Wie bei 3G wird auch im 4G-System die Einrichtung und der Betrieb einer Funkverbindung autonom durch das Radio-Netz (auf Anforderung vom Kern-Netz) durchgeführt. Das Kern-Netz fordert für die Verbindung Qualitätsparameter an, die bei 4G durch *Quality of Service Class Identifiers* (QCI) repräsentiert werden. Die QCI regeln grundsätzlich, ob die geforderte Bitrate garantiert werden muss, oder ob sie abweichen darf. Gleichzeitig wird die erlaubte Verzögerung von Daten (Packet Delay) und die gestattete Verlustrate für Pakete festgelegt. Die Priorität erlaubt dem Radio-Netz niedriger priorisierte Verbindungen bei Überlastsituationen zu verdrängen. Abb. 4.11 zeigt QCI-Werte und beispielhafte Anwendungsklassen. Für spezielle Anwendungen sind zusätzliche QCI definiert worden, die in dieser allgemeinen Tabelle nicht auftauchen. Netzbetreiber können auch einzelne Werte in ihren Systemen neu setzen, und sogar dynamisch verändern, wenn die Bedürfnisse ihrer Kunden von den allgemeinen Annahmen abweichen (Tab. 4.4).

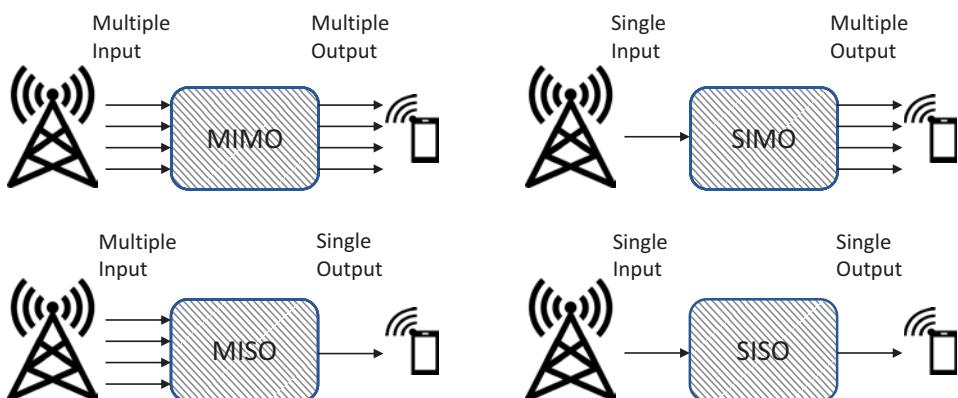


Abb. 4.11 Multiple Input – Multiple Output (MIMO)

Tab. 4.4 QCI-Parameter bei LTE

| QCI | Ressource Type | Priorität | Packet Delay | Paket-Verlust | Beispiele |
|-----|---------------------------|-----------|--------------|---------------|-------------------------------|
| 1 | Garantierte Bitrate | 2 | 100 ms | 10^{-2} | Sprache |
| 2 | (GBR) | 3 | 150 ms | 10^{-3} | Video-Konferenz |
| 3 | | 4 | 50 ms | | Gaming |
| 4 | | 5 | 300 ms | 10^{-6} | Streaming |
| 5 | Nicht-Garantierte Bitrate | 1 | 100 ms | | IMS Signal |
| 6 | (non GBR) | 6 | 300 ms | | Buffered Video |
| 7 | | 7 | 100 ms | 10^{-3} | Sprache, Video Live Streaming |
| 8 | | 8 | 300 ms | 10^{-6} | Video buffered Streaming |
| 9 | | 9 | | | |

4.5.3 LTE-Besonderheiten

4.5.3.1 Multiple Input – Multiple Output (MIMO)

Multiple Input – Multiple Output (MIMO) ist das Verfahren, mit dem die größten Steigerungen von Datenrate und Empfangsqualität bei LTE erreicht wurden. MIMO verwendet mehrere Antennen auf der Sende- und der Empfangsseite zur Verbesserung der Empfangsleistung oder zur Erhöhung der Datenrate. Die verschiedenen Möglichkeiten zeigt Abb. 4.11.

Durch MIMO kann der Sender (hier: LTE-Basisstation) auf einem Frequenzband mehrere unabhängige Datenströme an ein Endgerät senden und damit die Datenrate vervielfachen. Durch Multiple Input – Single Output (MISO) kann der Sender auf einem Frequenzband verschiedene Kopien desselben Datenstroms parallel an das Endgerät übertragen und damit die Empfangsqualität verbessern. Das Endgerät empfängt einen Datenstrom über eine Antenne. Hier ist eine hohe Koordination erforderlich, da sich durch Laufzeitunterschiede die empfangenen Wellen auslöschen können. Bei der Variante Single Input – Multiple Output (SIMO) empfängt das Endgerät den von der eNodeB ausgesandten Datenstrom über verschiedene Antennen. Mit Single Input – Single Output (SISO) ist schließlich die herkömmliche Übertragung von Antenne zu Antenne gemeint.

Eine Anwendung von MIMO zeigt Abb. 4.12. Es handelt sich dabei um „Transmit Diversity“. Die blockierte direkte Sichtverbindung zwischen Basisstation und Endgerät wird mittels MIMO genutzt, unabhängige Datenströme zum Endgerät zu senden. Damit kann der Empfang gegen Abschattungen oder Störungen unempfindlicher gemacht werden (*Diversity Gain*). Bei guten Empfangsbedingungen können auch unabhängige Datenströme gesendet und so die Datenrate erhöht werden.

Synchrone Datenströme, die von verschiedenen Antennen ausgehen, können zu einem sehr engen, auf das mobile Endgerät gerichteten Funkfeld (umgangssprachlich: Keule, englisch: beam) fokussiert werden (Abb. 4.13). Diese so genannte *Beamforming*-Technologie wird genutzt, um die Datenübertragungsrate zu maximieren. Der von dieser Keule erreichte Bereich hat durch die enge Fokussierung eine hohe Energie und garantiert damit eine exzellente Empfangsqualität. Das Funkfeld ändert dynamisch die Richtung und

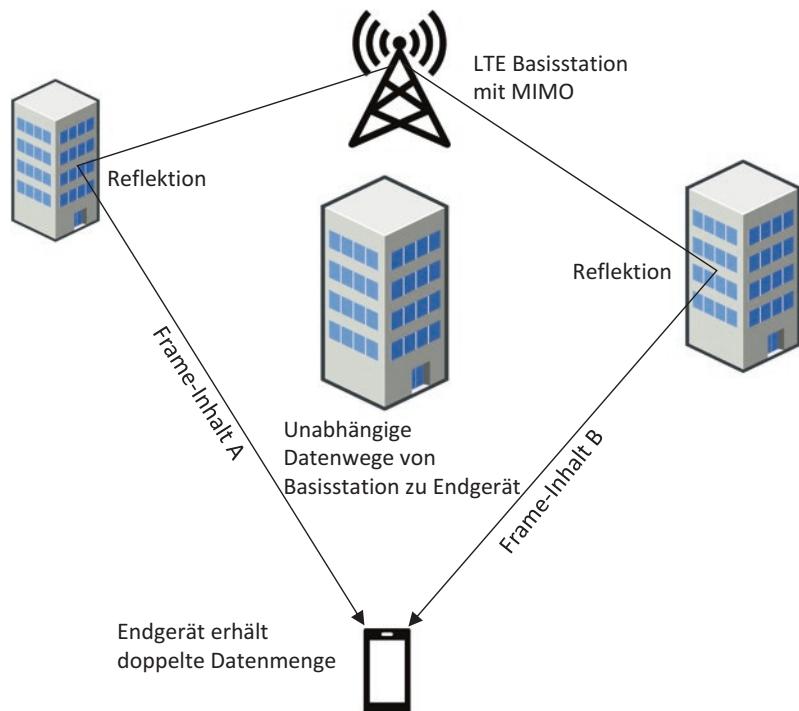


Abb. 4.12 Transmit Diversity – Unabhängige Übertragungswege zum Endgerät

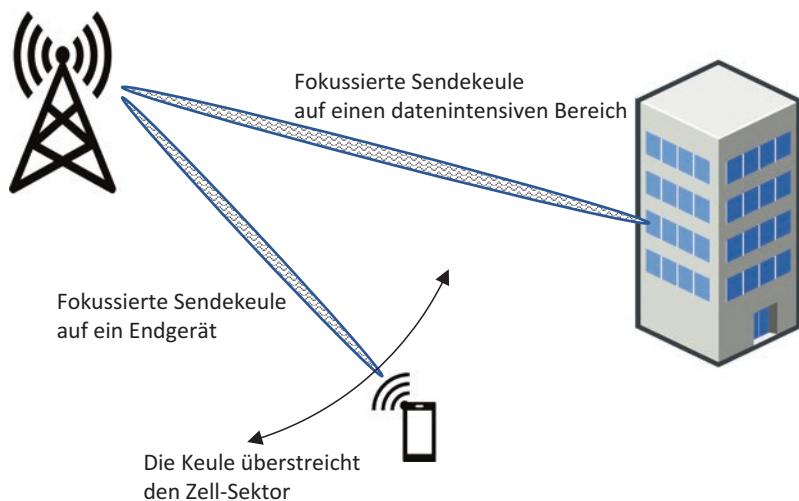


Abb. 4.13 Beamforming

überstreicht in regelmäßigen Abständen den gesamten Sektor. Auf diese Weise wird sichergestellt, dass alle Nutzer in den Genuss des guten Datenempfangs kommen, und dass sich neu anmeldende Endgeräte registriert werden, auch wenn sie sich gerade außerhalb des Zielbereichs befinden.

Für eine kurze Erläuterung der MIMO-Technik wird auf die Grundlagen für die Richtwirkung von Mobilfunk-Antennen in Abschn. 3.2.3 zurückgegriffen. Bei herkömmlichen Mobilfunk-Antennen beruht die Richtwirkung auf den unterschiedlichen Weglängen und Laufzeiten, die zwischen der Antenne und dem Empfänger bei verschiedenen Winkeln auftreten. Die beim mobilen Endgerät eintreffenden Wellen der beiden Antennen sind durch die Laufzeitveränderung gegeneinander verschoben. Dies äußert sich beim Empfänger als *Phasenverschiebung*. Im Extremfall liegen die Wellenberge eines Wellenzuges genau über den Wellentälern des Wellenzuges, der vom benachbarten Sende-Element ausgeht, so dass die beiden Wellen sich sogar auslöschen. MIMO beruht auf der gleichen Idee. Der Unterschied besteht darin, dass die Phasenverschiebung mathematisch durch komplexe Faktoren in das zu sendende Signal eingearbeitet wird. Endgeräte-spezifische Referenzsignale teilen dem Empfänger pro PRB mit, welche Phasenfaktoren verwendet wurden. Das Endgerät kann so diese Phasen wieder herausdividieren und die empfangene Information dekodieren.

In LTE wird bis zu 8x8 MIMO verwendet. Das bedeutet, dass Signale und Faktoren für bis zu 8 unabhängige Sendeantennen und bis zu 8 unabhängige Empfangsantennen vordefiniert sind und implementiert werden können.

4.5.3.2 Carrier Aggregation

Der Bedarf an immer höherer Datenkapazität konnte mit der Bandbreitenbeschränkung auf 20 MHz nicht gedeckt werden. Im Rahmen des erweiterten Standards *LTE-Advanced* wurde die parallele Nutzung von mehreren Frequenzbändern innerhalb eines Netzes und durch ein Endgerät unter dem Namen *Carrier Aggregation* eingeführt. Dabei wurde für Endgeräte die Möglichkeit der Nutzung von bis zu 5 parallelen Frequenzbändern mit einer maximalen Gesamtbandbreite von 100 MHz vorgesehen. Auf der Netzseite wurden drei Carrier Aggregation-Optionen von je zwei Bändern definiert: 10 MHz + 10 MHz, 15 MHz + 15 MHz und 20 MHz + 20 MHz mit den Bandbreiten 20 MHz, 30 MHz und 40 MHz. Für kleinere kombinierte Bandbreiten bestand kein Bedarf. Die möglichen Kombinationen bis 20 MHz können weitgehend durch die bereits vorhandenen LTE-Standard-Bandbreiten dargestellt werden. Die zu den Kombinationsfähigkeiten eines Endgerätes passende Carrier Aggregation muss vom Netzbetreiber konfiguriert werden. Für den Fall, dass genau diese Konfiguration hergestellt ist, kann das Feature von Endgeräten genutzt werden, die die Fähigkeit besitzen und dies dem Netz durch die Anmelde-Nachricht mitgeteilt haben.

4.5.3.3 Kategorien von LTE-Endgeräten

Der LTE-Standard sah von vornherein eine Klassifikation und Festlegung von Leistungsmerkmalen der Endgeräte vor. Damit sollte sichergestellt werden, dass beim Start der Netztechnologie leistungsfähige Endgeräte zur Verfügung standen. Die ursprüngliche

Klassifikation von Kategorie 1 (Cat-1) bis Kategorie 5 (Cat-5) wurde als Reaktion auf das steigende Leistungsniveau zunächst um Cat-6 bis Cat-10 und inzwischen bis auf Cat-21 erweitert. Tab. 4.5 zeigt beispielhaft einige Kategorien mit wesentlichen technischen Spezifikationen und einigen Gerätebeispielen.

Alle Geräte der Kategorien oberhalb von Cat-6 können die maximalen Bandbreiten nur mittels Carrier Aggregation erreichen. Es gibt allerdings kaum Netzwerke, die diese Werte ermöglichen. Wie an Cat-21 zu sehen, bedeutet eine höhere Kategorie nicht notwendigerweise höhere Bitraten. Kategorien sind häufig auf Initiative von Herstellern eingeführt worden und stellen auch ein Marketing-Instrument dar. Für Endgeräte vom Einsteigersegment bis zur Mittelklasse ist nach wie vor die Kategorie Cat-4 interessant. Hier gibt es neben den in Tab. 4.5 genannten Geräten zahlreiche weitere. Mit Cat-4 und Cat-6 kann der Nutzer die Performance eines durchschnittlichen LTE-Netzwerkes vollständig nutzen. Die Geräte höherer Kategorien können in entsprechend konfigurierten Netzen ihre überlegenen Bitraten realisieren; im alltäglichen Gebrauch müssen sie sich mit den angebotenen Datenraten begnügen. Sie entsprechen in gewisser Weise Sportwagen, die auf präparierten Strecken hohe Geschwindigkeiten erreichen können, ohne dies im Alltag auf viel befahrenen Straßen jemals nutzen zu können.

Für die Nutzung im Bereich „Internet der Dinge“ werden die hohen Bitraten oft nicht benötigt. Dafür sind Eigenschaften wie geringer Energieverbrauch wichtig, die in Kap. 6 dargestellt werden. Deshalb wurden die zusätzlichen Kategorien Cat-0 und Cat-M1 eingeführt, die mit niedrigen Datenraten, hoher Reichweite und Eindringtiefe geeignet für

Tab. 4.5 Beispielhafte Gerät-Kategorien und Endgeräte

| Kategorie | Cat-3 | Cat-4 | Cat-6 | Cat-9 | Cat-12 | Cat-16 | Cat-18 | Cat-20 | Cat-21 |
|---------------------|----------|-------------------|----------------|--------------|--------------------|----------------|----------------|-------------------------|------------|
| Max DL | 100 | 150 | 300 | 450 | 600 | 1000 | 1200 | 2000 | 1400 |
| Max UL | 50 | 50 | 50 | 50 | 50 | 50 | 150 | 300 | 300 |
| MIMO | 2x2 | 2x2 | 4x4 | 4x4 | 4x4 | 4x4 | 4x4 | 8x8 | 8x8 |
| Modulation DL | 64 | 64 | 64 | 64 | 256 | 256 | 256 | 256 | 256 |
| Modulation UL | 16 | 16 | 16 | 16 | 16 | 16 | 64 | 64 | 64 |
| Carrier Aggregation | Nein | Nein | Ja | Ja | Ja | Ja | Ja | Ja | Ja |
| Beispiele | iPhone5s | Honor 8A | LG G3 | Google Pixel | Sony Xperia 10Plus | Huawei P20 Pro | ZTE Nubia Z20 | Samsung Galaxy S10, S20 | Huawei P30 |
| | | Samsung Galaxy S5 | Sony Xperia L3 | LG S5Pro | iPhone8 | iPhone XS | Google Pixel 4 | Xiaomi Mi Mix 3 | |
| | | iPhone6 | | | | | | | |

Erläuterungen:

UL = Uplink, DL = Downlink

Die Modulationsschemata UL und DL sind als QAMxyz zu lesen, mit der zwei- bis dreistelligen Zahl xyz aus der Tabellenzeile

M2M-Kommunikation sind. Sie haben jeweils 1 Mbit/s maximale Datenrate im Uplink und im Downlink und unterstützen die Modulationen QAM16 und QPSK.

4.5.3.4 Mobilität bei LTE

Als Mobilfunknetz benötigt LTE effektive Methoden, um die Mobilität der Teilnehmer und Endgeräte zu unterstützen. Insbesondere der Handover von einer Zelle zu einer benachbarten Zelle bei Ortsveränderung des Endgerätes oder Veränderung der Sende- und Empfangsbedingungen ist zu regeln.

Hilfreich ist dabei natürlich die Definition als reines Datennetz. Betroffen ist maximal die Schicht 3 des OSI-Modells (bzw. IP). Damit liegt die Verantwortung für einen unterbrechungsfreien Datenverkehr nicht mehr im LTE-Netzwerk, sondern bei der Ende-zu-Ende-Sicherung in der Transportschicht beziehungsweise den Applikationen. Bei vorherigen Generationen wurden Sprachverbindungen leitungsvermittelt auf gleicher Ebene geführt. Damit ergab sich automatisch die Notwendigkeit, unterbrechungsfreien Übergang von einer Mobilfunkzelle zur nächsten zu gewährleisten. Der Handover bei LTE ist dagegen immer ein harter Handover.

LTE sorgt im Sinne einer Schicht 2-Übertragung aber für eine verlustfreie Übermittlung der Datenblöcke innerhalb des LTE-Netzes. Die eNodeB regeln den Handover mit gewissen Einschränkungen autonom, und sorgen dafür, dass Datenblöcke, die sich während des Handover an einen andere eNodeB bereits in der Übertragung befinden, an den Ziel-eNodeB übertragen werden.

Der Handover erfolgt in drei Phasen:

1. Handover Vorbereitung: Das Endgerät sendet periodisch oder nach Aufforderung die Stärke der empfangenen Pilotkanäle und Referenzkanäle des aktuellen eNodeB und der erreichbaren Ziel-eNodeB. Es gibt verschiedene Kriterien für ein Handover:
 - Das vom Endgerät empfangene Signal der aktuellen Zelle ist schlechter als ein unterer Grenzwert
 - Das vom Endgerät empfangene Referenzsignal einer Nachbarzelle ist besser als das der aktuellen Zelle oder als ein Schwellwert
 - Die aktuelle Zelle ist überlastet
 - Ohne unmittelbaren Handover droht die Verbindung zum Endgerät abzubrechen.Die aktuelle eNodeB fällt die Handover-Entscheidung und informiert die Ziel-eNodeB. Mit dieser Information werden alle Daten übertragen, die für den Aufbau der neuen Verbindung erforderlich sind. Dazu gehören
 - Die Qualitätsparameter der bestehenden Verbindungen zum Endgerät
 - Die ID der verantwortlichen MME und die Daten für den bestehenden PDP-KontextIn ihrer Bestätigungs-Nachricht gibt die Ziel-eNodeB die Details für eine schnelle und kollisionsfreie Anmeldung des Endgeräts bekannt. Darunter ist ein reservierter, kollisionsfreier Access-Code.
2. Handover Durchführung: Die aktuelle eNodeB informiert jetzt das Endgerät über den bevorstehenden Handover und übergibt die Identität der Ziel-eNodeB sowie den reser-

vierten Access Code. An die Ziel-eNodeB überträgt sie ab diesem Zeitpunkt alle für das Endgerät bestimmten Datenpakete, die dort zwischengespeichert werden.

Das Endgerät benutzt den reservierten Access-Code zum Aufbau einer Verbindung mit der Ziel-eNodeB. Die zwischengespeicherten Daten werden zum Endgerät übertragen. Die weiteren Daten fließen jetzt vom S-GW über die abgebende (aktuelle) eNodeB und die Ziel-eNodeB zum Endgerät.

3. Handover Komplettierung: Die Ziel-eNodeB beantragt und erhält vom MME einen neuen Datentunnel. Die Daten fließen jetzt direkt zum Endgerät. Die Verbindung mit der abgebenden eNodeB wird beendet.

Ein weiterer Aspekt neben dem Intra-LTE-Handover ist der Handover an 2G oder 3G, so lange LTE nicht flächendeckend ausgebaut ist. In diesen Fällen nimmt die MME Kontakt zum verantwortlichen SGSN Knoten im verfügbaren 2G oder 3G auf, deren Adresse und Zugangsdaten sie dauerhaft gespeichert hat. Dabei nimmt sie selbst die Rolle eines SGSN ein. Das Handover erfolgt dann gemäß den Regeln der Ziel-Technologie als 2G- oder 3G-Handover.

4.5.4 Erweiterungen und Anwendungen von LTE

Grundsätzlich stellt LTE ein reines Datennetz mit Übergängen in das Internet bereit. Damit ist die gleiche Dienste-Vielfalt wie über einen Internet Service Provider Zugang im Festnetz möglich. Mittels Ortung, Kamera oder NFC-Chip werden sogar sehr viel weitergehende Applikationen realisiert. Für eine Reihe von Anwendungen ist aber in den Augen des Kunden selbstverständlich der Netzbetreiber verantwortlich. Dazu gehören in erster Linie die Sprachdienste. Zusätzlich entstanden schnell nach Einführung von LTE zusätzliche Anforderungen, die nicht effizient über eine IP-Plattform abgewickelt werden können. In den folgenden Kapiteln erfolgt eine kurze Betrachtung der Themen Sprache, Breitband-Verteidienste (Streaming) und Internet der Dinge (IoT) im Zusammenhang mit LTE.

4.5.4.1 Sprache über LTE (VoLTE)

Die wichtigste Einzelapplikation der mobilen Netze der Generationen 1G bis 3G war immer die Telefonie. Die Definition von LTE als reines IP-Datennetzwerk lässt hier Fragen offen, die im Folgenden kurz beantwortet werden sollen. Die Lösung für Telefonie im LTE-Netz ist ein Sprachdienst über das IP-Netz, also im allgemeisten Sinne „Voice over IP“. Voice over IP wird von einer Reihe von Service-Providern auch über Mobilnetze angeboten, wie etwa Skype, WhatsApp, Google oder Facebook. Sie sind oftmals sogar kostenfrei. Allerdings entsprechen sowohl die Komfort-Features als auch die Sprach- oder Bildqualität bei Videotelefonie häufig nicht den Ansprüchen an ein modernes Kommunikationsmedium. Die fehlende Einbindung in das Mobilfunknetz zeigt sich auch bei Problemen mit der Netzabdeckung. Bewegt sich der Nutzer aus der LTE-Abdeckung

hinaus, bricht in der Regel der Telefonkontakt ab. Die Datenraten der Generationen vor LTE reichen oft nicht aus, um die VoIP-Verbindung aufrecht zu erhalten.

Voice over LTE (VoLTE) ist ein Standard, der vom 3GPP, der Industrie und den Netzbetreibern entwickelt wurde, um einen qualitativ hochwertigen Sprach- und Videotelefon-dienst auf der Basis von Voice over IP anzubieten. Die Integration von VoLTE im Mobilfunknetz wird durch einen *Internet Multimedia Server* (IMS) im Operator-Netz hergestellt (Abb. 4.14), der über einen eigenen APN adressiert wird. Der IMS implementiert einen vollwertigen VoIP-Server nach dem Session Initiation Standard (SIP) der IETF und ist verantwortlich für Auf- und Abbau sowie die Kontrolle der laufenden Verbindungen. Zusätzliche Komponenten sorgen für eine Berücksichtigung der Besonderheiten des Mobilfunks und eine enge Integration in das Mobilfunknetz.

- Bei ankommenden Gesprächen wird der Aufenthalt des angerufenen Endgerätes und die Adresse des zugehörigen IMS Servers identifiziert. Dazu besteht eine Verbindung mit der HSS-Datenbank.
- Eine Proxy-Funktion schließt die Verbindung zum Kern-Netz ab, falls die Netzwerk-Verbindung zum Endgerät nicht mehr zur Verfügung stehen sollte. Bei schlechten Empfangs- und Sendebedingungen werden Datenraten angepasst und das Funksignal durch sogenannte TTI-Bündelung verbessert.

Die Anbindung an das weltweite Telefonnetz erfolgt durch Media-Gateways, die die VoIP-Signale in leitungsvermittelte Verbindungen übersetzen oder durch Session Border Gateways, die die IP-Domäne des Netzbetreibers gegenüber dem Internet abschließen. Im Telefonverkehr gebräuchliche Funktionen wie Rufnummern-Analyse, Ermittlung von Gesprächszeiten und -gebühren, Halten und Makeln, Rufumleitung, Rückruf bei Besetzt, Anzeigen oder Unterdrücken von Rufnummern, sowie Konferenzgespräche werden durch einen Applikationsserver nach dem MMTEL-Standard gesteuert.

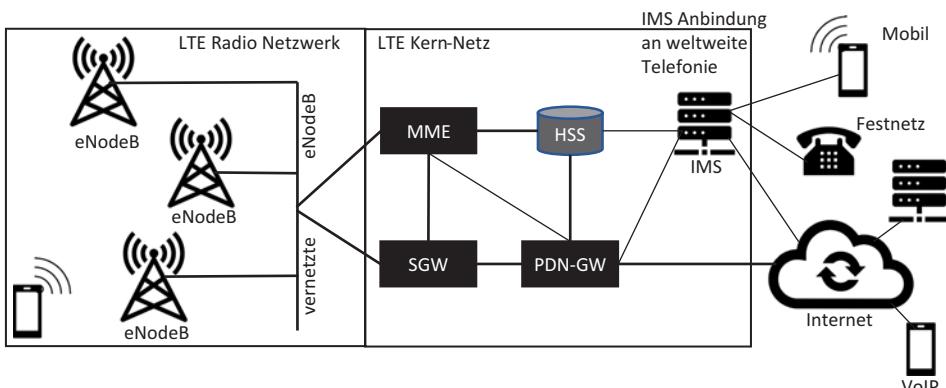


Abb. 4.14 Internet Multimedia Server (IMS) und VoLTE im LTE-Netzwerk

VoLTE wird mit den QCI-Parametern 1 (für die Sprache) und 5 (für die Signalisierung) durchgeführt. Damit hat VoLTE-Signalisierung die höchste Priorität 1 im LTE-Netz; die Priorität 2 für die VoLTE-Sprache ist die nächsthöhere Stufe. Die kontrastiert mit der Einordnung der externen VoIP-Dienste, wie etwa Skype oder WhatsApp-Calling, die über den HTTP-Port 80 als Daten vermittelt werden und damit vom Radio-Netz mit der niedrigen Priorität 7 versehen sind. Die Entscheidung, über den allgemeinen HTTP-Port zu gehen, liegt auf der Seite der VoIP-Anbieter, die damit sicherstellen, dass ihr Dienst auch im WLAN und in privaten, durch Firewalls abgesicherten Netzen erreicht werden kann.

4.5.4.2 WiFi Calling

Bei Verlassen des Abdeckungsbereiches von LTE wird ein über VoLTE geführtes Mobilfunkgespräch durch das IMS-System und die Netzwerk-Knoten an ein anderes vorhandenes Netz des gleichen Netzbetreibers übergeben. Als Ergänzung von VoLTE, speziell in Bereichen mit schwacher LTE-Abdeckung, wurde auch der Service WLAN Calling bzw. WiFi Calling eingeführt. Dabei kann bei kompatiblem Endgerät ein Mobilfunk-Telefonat ankommend oder abgehend aus einem WLAN-Netzwerk geführt werden. Wenn ein entsprechend konfiguriertes Endgerät in einem WLAN angemeldet ist, beantragt es mit seinen Mobilfunk-Zulassungsdaten Zugriff auf das Kern-Netz über ein spezielles *enhanced Packet Data Gateway* (ePDG, Abb. 4.15). Es wird ein VPN-Tunnel Ende-zu-Ende vom Endgerät zum ePDG eingerichtet, über das eine Verbindung direkt zum PD-GW unter Umgehung des LTE-Radio-Netzes hergestellt wird. Abgehende und ankommende VoLTE-Gespräche werden so über einen Internet-Zugang durchgeführt. Damit können Anrufe mit allen Qualitätsmerkmalen getätigt und angenommen werden, ohne dass eine entsprechende Mobilfunkabdeckung vorhanden ist. Der unmittelbare Gewinn für den Kunden besteht in der Möglichkeit, auch unter schwacher Netzarbeitung, zum Beispiel in Kellerräumen, Mobilfunkgespräche zu empfangen oder zu führen. Bei Aufenthalten im nicht-europäischen Ausland eröffnet WiFi Calling auch die Option von qualitativ hochwertigen Verbindungen

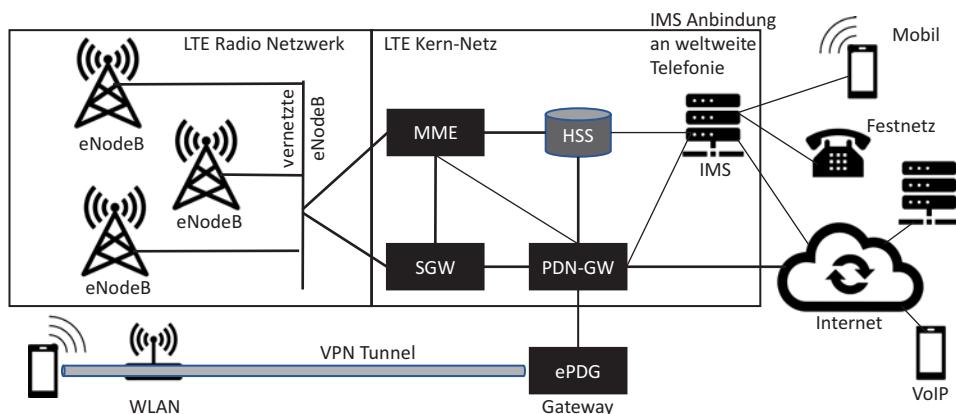


Abb. 4.15 WiFi Calling in LTE

zum Heimattarif, denn für das Netz befindet sich der Nutzer „virtuell“ immer im Heimatnetz. Eine damit verbundene Kostenfalle ist allerdings, dass ein Anruf innerhalb des Gastnetzes mittels WiFi Calling vom Heimatnetz als ein möglicherweise kostenpflichtiger Anruf aus dem Heimatland ins Ausland gewertet wird. WiFi Calling wird von aktuellen Smartphones unterstützt und kann in den Telefon-Einstellungen aktiviert und deaktiviert werden.

4.5.4.3 Mission Critical Push to Talk

Push to Talk (PTT) ist ein im Betriebsfunk verbreitetes Kommunikationsverfahren. Wörtlich fordert die Bezeichnung den Benutzer dazu auf, einen Knopf zu drücken, bevor etwas über das Gerät mitgeteilt wird („Walkie-Talkie-Funktion“). PTT wird auch verbreitet in den Netzen der Rettungs- und Sicherheitskräfte bei Einsätzen genutzt. In der Regel erfolgen dort Mitteilungen und Ansagen der Einsatzleitung über einen Gruppenruf; einzelne Kräfte können nach Knopfdruck antworten.

Speziell für den Einsatz bei Rettungs- und Sicherheitsorganisationen hat das 3GPP die Funktion Mission Critical Push to Talk (MCPTT) auf der Basis von LTE standardisiert. Durch die Verwendung von VoLTE als grundlegendem Sprach-Codec wird eine hohe Sprachqualität gesichert. Die Bandbreite von LTE erlaubt auch das Übertragen von Video-Streams und die Übermittlung von Dateien und Bildern. Zusätzlich wurde die Möglichkeit geschaffen, innerhalb des MCPTT-Systems auch „private“ Gespräche von Person zu Person zu führen. Entsprechend der Geschwindigkeit des Gesprächsaufbaus bei VoLTE werden auch die MCPTT-Verbindungen äußerst schnell hergestellt (typisch: unter 1 Sekunde). Wenn MCPTT in einem LTE-Netz eingesetzt wird, handelt es sich in der Regel um eine wichtige Dienstleistung des Netzbetreibers. Entsprechend wird die Priorität von MCPTT sehr hoch angesetzt; in der Regel sogar höher als die von VoLTE als Sprachdienst.

Wie die VoLTE-Implementierung basiert auch MCPTT auf IMS. Als Applikationsserver kommt hier allerdings nicht MMTEL zum Einsatz, weil keine spezifischen Telefondienste genutzt werden. Stattdessen wurde die IMS-Schnittstelle zu einem MCPTT Applikationsserver standardisiert. Einzelne Hersteller können hier unterschiedliche Leistungsmerkmale und Funktionen entwickeln. In der Regel wird der MCPTT-Server eine Schnittstelle zu einem Applikations-Desk besitzen, von dem aus steuernd in die Kommunikation eingegriffen werden kann. Es können Rechte einzelner Teilnehmer verändert werden, Gruppen geteilt oder zusammengeführt, oder einzelne Mitglieder von einer Gruppe zu einer anderen übertragen werden.

4.5.4.4 Breitband-Verteididienste über LTE

Breitband-Verteididienste (Multimedia Broadcast Multicast Services, MBMS) wurden als ein vereinfachtes LTE-System zur Übertragung von Multimedia-Inhalten, wie etwa der Übertragung von mobilen TV-Programmen definiert. Es handelt sich um Verteilsysteme, bei denen alle für den Dienst registrierten Geräte in der Zelle das Programm erhalten, das dafür nur einmal ausgesendet werden muss. Der Dienst ist ein unidirektonaler Dienst, ohne Fehlerkorrektur und Empfangs-Quittung durch die Endgeräte. Damit wird das

Mobilfunknetz erheblich entlastet. Über ein 5 MHz-LTE-Frequenzband können mit dieser Technologie ca. 20 HD-Fernsehkanäle übertragen werden.

Die erfolgreiche kommerzielle Nutzung von MBMS verlangt neben der Sendetechnologie auch geeignete Angebote und angepasste Endgeräte. Mögliche Anwendungen sind nach (LTE Broadcast Alliance 2016)

- Live HD Streaming Video, als Ergänzung zu HDTV in Innenräumen, und dort wo HDTV schlecht zu empfangen ist
- Ausstrahlung von TV-Inhalten an Mobilgeräte
- Sport, Musik- und Event-Angebote: Replay aus verschiedenen Blickwinkeln, zusätzliche Daten
- Sicherheits-Dienste mit lokalen Warnhinweisen, etwa bei Naturkatastrophen
- Verteilen von Software und Inhalten auf Bahnhöfen, Flughäfen und in Hotels

Es gab und gibt einige vielversprechende Versuche mit dem lokalen Einsatz von MBMS Diensten. Dabei wurden zum Beispiel bei lokalen Großereignissen mit verteilten Schauplätzen (Autorennen, Skirennen, Festivals) vor Ort die Aufnahmen von Kamerateams an verschiedenen Standorten zu mehreren Kanälen zusammengestellt und per MBMS an die Besucher als Stream übermittelt. Der Bayrische Rundfunk hat in einem Großversuch eine reguläre TV-Programmausstrahlung für den Großraum München über zwei LTE-Sendestationen durchgeführt. Damit sollte die Möglichkeit demonstriert werden, reguläre TV-Programme terrestrisch über LTE anstelle des DVBT-Standards auszustrahlen, und so weitere Frequenzen für LTE freizumachen. Die Installation wird derzeit auf den 5G-Standard umgerüstet (Institut für Rundfunktechnik 2019).

4.5.4.5 Internet der Dinge und LTE (LTE-M und NB-IoT)

Das „Internet der Dinge“ (Internet of Things, IoT) nahm nach 2010 in allen Bereichen von Industrie und Gesellschaft Fahrt auf. Es geht dabei im Wesentlichen darum, Geräte zu vernetzen, damit korrekte und vollständige Informationen, z. B. von Messgeräten oder Sensoren, an der richtigen Stelle zusammenkommen und Kontroll- und Steueranweisungen an intelligente Einheiten gegeben werden können. Ein großer Teil dieser Vernetzung ist zwangsläufig drahtlos und mobil, weil Sensoren häufig Teil einer mobilen Installation sind. Beispielsweise seien etwa Automobile, aber auch Sensoren in Kleidungsstücken oder medizinische Sensoren, die am Körper getragen werden (eHealth), genannt. Auch nicht mobile Sensoren und Endgeräte müssen oft drahtlos angeschlossen werden, da am Einsatzort kein kabelgebundenes Netzwerk zur Verfügung steht.

Die ersten Anforderungen an ein drahtloses IoT Verfahren waren

1. Geringe Kosten für Endgeräte bzw. Modems zum Einbau in Endgeräte
2. Lange Laufzeit der Endgeräte mit einer Batterieladung (10 Jahre werden gemeinhin als Minimum gesehen)

3. Signal-Durchdringung von Gebäudewänden, bis in Kellerräume hinein (beispielsweise für die Übertragung von Energie-Verbrauchsdaten)
4. Hohe Zahl von verbundenen Endgeräten pro Sendestation

Sowohl die erzielbaren Datenraten als auch die Unterstützung von Mobilität waren zunächst von untergeordneter Bedeutung; später spielten sie aber eine immer größere Rolle. Vom Standpunkt des 3GPP aus (Abschn. 4.3.3) ist GSM immer noch ein ernst zu nehmender Kandidat für M2M-Kommunikation. Schwachpunkte von GSM als IoT-Kommunikationsmittel sind allerdings die hohe Ausgangsleistung der mobilen Endgeräte und die Kapazität der Netze.

Die Verbreitung von LTE als universellem mobilen Kommunikationsdienst führte auf die Anforderung, auch IoT-Anwendungen über LTE abwickeln zu können. Durch Nutzung der LTE-Infrastruktur für die neuen Anwendungen wird vermieden, neue und zusätzliche Netze aufzubauen zu müssen. Der primäre Focus bei der LTE-Entwicklung lag auf hohen Datenraten und damit verbunden auf der Verarbeitung von breiten Frequenzbändern bis 20 MHz. Die für LTE vorwiegend verwendeten Frequenzen im 1,8 GHz- und 2,6 GHz-Bereich weisen verglichen mit GSM eine sehr viel geringere Reichweite und Eindringtiefe in Materialien auf. Gleichzeitig wachsen Rauschen und Interferenz des Signals linear mit der Bandbreite. Die Anforderungen an die Nutzung von LTE für IoT sind daher

- Verfahren zur besseren Durchdringung von Gebäudewänden
- Verbesserung der Reichweite durch besseren Signal-zu-Rausch-Abstand und schmalere Bandbreiten
- Zusätzlich entstand aus Anwendersicht der Bedarf, sehr stromsparende Endgeräte nutzen zu können.
- Das Potenzial von LTE zu einer sehr genauen Ortsbestimmung der Endgeräte muss erhalten werden

Der Einsatz von LTE als Kommunikationsmittel im IoT erfordert die Unterstützung sehr schmaler Frequenzbänder und Frequenzen unterhalb des bisherigen LTE-Spektrums. Das 3GPP hat zwei auf LTE aufbauende Standards mit Bezug zum Internet of Things entwickelt: LTE-M und NB-IOT.

In der Bezeichnung LTE-M steht das M für *Machine-Type-Communication*, also der Kommunikation Maschine-zu-Maschine. Der Standard definiert ein *LTE Narrowband* von 6 Physical Resource Blocks (1,08 MHz) innerhalb eines Standard-LTE-Signals, das selbst 5, 10 oder 20 MHz breit sein kann (Abb. 4.16). Das Endgerät wird so eingerichtet, dass nur dieser Teil des Spektrums für IoT-Kommunikation genutzt wird. Damit entfallen die Nachteile einer sehr großen Bandbreite, wie Rauschen und Interferenz. Auch die Sendeenergie wird minimiert. Die übrigen PRB des LTE-Frames können für den normalen LTE-Datenverkehr genutzt werden.

Um die Reichweite und die Durchdringung von Gebäudewänden zu verbessern, wird die Bündelung von Signalen eingeführt. Bei Bedarf können Datenblöcke nach einem defi-

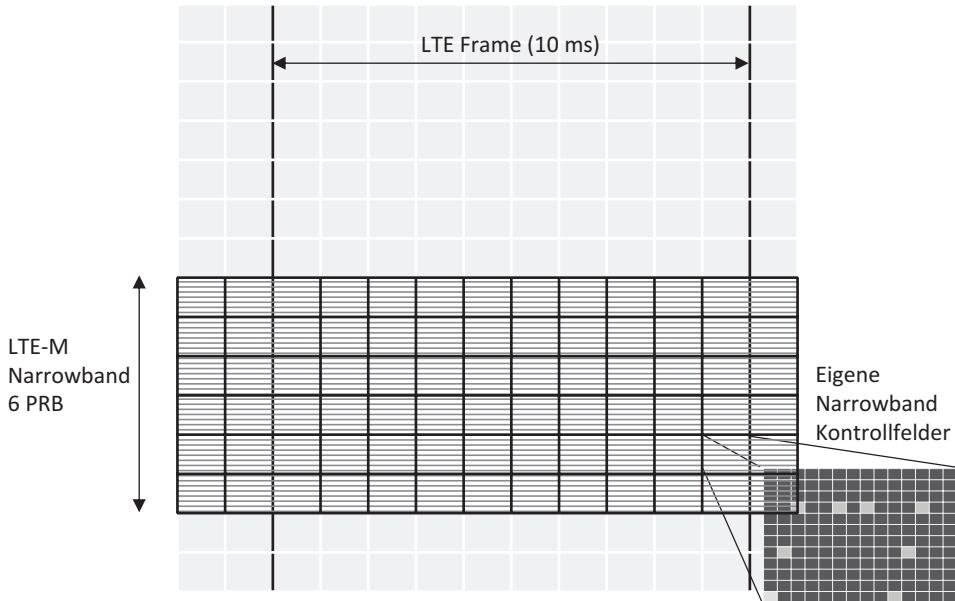


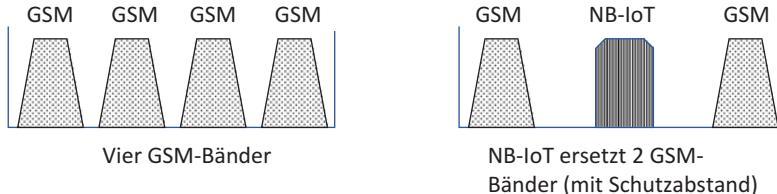
Abb. 4.16 LTE-M Narrowband mit eigenen Kontrollfeldern im LTE-Rahmen

nierten Schema in direkter Folge wiederholt gesendet und auf der Empfangsseite addiert werden, so dass sich für den Empfänger ein besser definiertes Signal ergibt. Die maximale Anzahl der Wiederholungen wird auf der Basis der Sende- und Empfangsbedingungen bei der Anmeldung des Endgerätes festgelegt. Im Coverage Enhancement Mode A (CE Mode A) sind bis zu 32 Wiederholungen eines Datenblocks zulässig, bei Coverage Mode B (CE Mode B) sind es maximal 2048 Wiederholungen. Während mit CE Mode A noch eine normale Funkkommunikation einschließlich Telefonaten möglich ist, bleibt die Anwendung von CE Mode B dem Datenverkehr unter extremen Bedingungen und mit sehr niedrigen Datenraten vorbehalten.

Internet of Things-Verkehrsmodelle verlangen nur sehr niedrige Datenraten pro Endgerät. In der Anwendung *Smart Metering*, also dem Auslesen von intelligenten Stromzählern über das Mobilfunknetz wird von ca. 12 Übertragungen pro Tag mit jeweils 32 Byte Nutzlast ausgegangen. Bei diesen Datenraten können durch LTE-M bis zu 1 Million verbundene Modems pro Quadratkilometer unterstützt werden. LTE-M ist heute durch die führenden Hersteller von Netztechnik zum großen Teil implementiert.

Die neu eingeführte Endgeräte Kategorie Cat-M0 („Kategorien von LTE-Endgeräten“, Abschn. 4.5.3) zeichnet sich durch eine besonders einfache Bauart aus. Die symmetrischen Sende- und Empfangschips sind nur einfach vorhanden. Als Konsequenz arbeitet das Gerät im Halb-Duplex Modus: Es kann jeweils nur senden oder empfangen. Hierdurch reduzieren sich Stromverbrauch und Herstellungskosten. Mit GSM wären die geforderten Batterialaufzeiten von bis zu 10 Jahren mit einem Satz handelsüblicher AA-Batterien un-

erreichbar. Zusätzlich wird ein Stromspar-Modus unterstützt, bei denen das Gerät im eingebuchten Zustand „schlafen“ kann, ohne sich für die nächste Übertragung neu anmelden zu müssen. Zur Ortsbestimmung wird das Positionierungssystem des LTE-Netzes verwendet (Abschn. 8.6.2).



Der LTE-Standard *Narrowband IOT (NB-IOT)* verwendet grundsätzlich die gleichen Methoden wie LTE-M. Er arbeitet allerdings mit einem noch schmaleren Frequenzband von nur 180 kHz, was einem LTE Physical Resource Block entspricht und mit einem GSM-Frequenzband (200 kHz) vergleichbar ist. Damit erlaubt er den Einsatz an Stelle eines GSM-Bandes und kann damit die Migration von GSM-basiertem IoT in LTE-basiertes IoT ermöglichen (Abb. 4.17). Es kann aber auch als ein PRB „in-band“ in einem LTE-Rahmen laufen und dort spezielle IoT-Dienste aufnehmen.

Durch die schmale Bandbreite von 180 kHz ist das Rauschen im Vergleich zu LTE-M nochmals geringer; der Systemgewinn von NB_IoT ist durch standardmäßig vorgesehenes Coverage Enhancement im CE Mode B Level 2 mit mehr als 160 dB um 20 dB höher als der eines LTE-Systems. Damit werden Funkzellen von mehr als 50 km Radius ermöglicht. In Situationen mit sehr schlechter Netzaufdeckung zeigt sich in Simulationen und Feldversuchen zudem, dass die erzielbaren Bitraten von NB-IOT denjenigen von LTE-M trotz der geringen Bandbreite nicht nachstehen. Bei einer Dämpfung von 164 dB werden Datenraten von mehr als 160 Bit/s erreicht. Feldtests und Simulationen zeigten, dass NB-IoT in einer Zelle über 60.000 Endgeräte anschließen kann. Dabei sandten diese Endgeräte bis zu 8 Datenpakete der Standardgröße (32 Byte Nutzlast) pro Minute mit einer Verlustrate von unter 1 %.

Die hohen Wiederholraten bei Coverage Enhancement B Level 2 und damit verbundenen langen Übertragungszeiten machen Endgeräte mit NB-IoT (und LTE-M in Mode B) weniger mobil. Ein Handover zwischen zwei Zellen ist grundsätzlich nur im Idle-Mode zulässig, wenn also gerade keine Datenübertragung stattfindet.

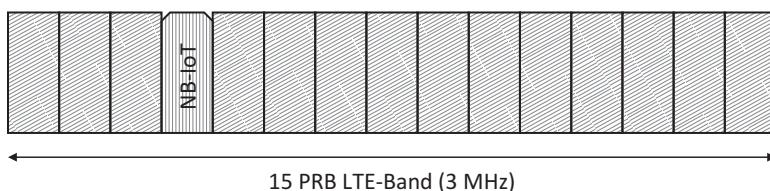


Abb. 4.17 Ein Band von NB_IOT eingebettet in ein breites LTE-Band

Die Einführung von LTE-M und NB_IOT in ein bestehendes Netz erfolgt in der Regel durch einen Software-Upgrade. Damit sind sie kostengünstiger und schneller verfügbar als eine Technologie, die ein eigenes Netz benötigt. In Deutschland werden LTE-M und NB_IOT von den drei öffentlichen Netzbetreibern Telekom, Vodafone und O2 angeboten. Dabei wird in der Regel auf die nach LTE übertragenen Frequenzbänder zwischen 700 und 900 MHz zurückgegriffen, die eine bessere Netzabdeckung als die höheren LTE-Frequenzen bieten. Narrowband IoT ist auch in den meisten europäischen und amerikanischen Ländern flächendeckend verfügbar. Roaming-Abkommen zwischen den Anbietern erlauben auch die grenzüberschreitende Nutzung. Es stehen eine Reihe von standardisierten Anwendungen zur Verfügung, die von der Überwachung von Haus- und Nutzieren bis hin zum Management von e-Ladestationen reichen. Der Spezialanbieter 450 Connect baut ein LTE-Netz im 450 MHz-Bereich auf, über das im Auftrag der Stromversorger die Überwachung und Steuerung der Anlagen für die Energiewende erfolgen soll. Mittels LTE-M sollen flächendeckend Smart Meter Gateways zur Erfassung und Steuerung von Verbrauchsdaten in Haushalten und Unternehmen angeschlossen werden.

4.6 Mobilfunk der 5. Generation (5G)

Bisher hat kein neuer Mobilfunkstandard so viel öffentliche Aufmerksamkeit erfahren, wie der 4G Nachfolger, der unter dem Sammelbegriff 5G zusammengefasst wird.

4.6.1 5G Überblick

3G rückte erst in den öffentlichen Fokus, als die hohen Beträge für die Frequenzauktion des Jahres 2000 bekannt wurden. Dagegen wurde die Einführung von 4G von der Öffentlichkeit kaum wahrgenommen. Seit der starken Verbreitung von Smartphones und mobilem Internet sowie der Durchdringung des persönlichen und geschäftlichen Lebens durch Mobilkommunikation betrifft das Thema inzwischen aber fast jeden persönlich. Überschriften wie „Der schnelle Mobilfunk kann kommen“ waren und sind an der Tagesordnung (Bauchmüller und Martin-Jung 2018). Experten sehen diese Berichterstattung kritisch, auch wenn sich das Thema so sehr gut verkaufen lässt. In der Tat ist „schneller“ nur ein Ziel unter mehreren, und 5G ist um vieles komplexer als nur ein beschleunigtes 4G. Im Folgenden werden die wichtigsten Prinzipien und technischen Elemente von 5G kurz dargestellt.

4.6.2 Anforderungen an 5G

Stärker als alle Vorgängergenerationen wurde 5G von den Anwendungen her „gedacht“. Die ITU-R hat vielfältige Anforderungen an den Mobilfunk der fünften Generation zu-

sammengestellt, die auf den ersten Blick teilweise widersprüchlich wirken. Sie sind in gleicher Weise auf die Verbesserung der mobilen Breitbandversorgung und der Echtzeit-Nutzung wie auf die Nutzung durch Maschinen im Bereich Low Power Wide Area („Internet der Dinge“, Abschn. 4.5.4) bezogen. Die folgenden Ziele stehen bei 5G im Vordergrund:

- Verbesserte mobile Breitbandkommunikation
- Mobiles Internet der Dinge für große Mengen von Endgeräten, als *massive Machine Type Communication* (mMTC) bezeichnet
- Kritische und hochzuverlässige Kommunikation; für industrielle Anwendungen, aber auch für Notfalleinsätze oder Sicherheitskräfte, als *critical Machine Type Communication* (cMTC) bezeichnet

4.6.2.1 Mobile Breitbanddienste

Das Thema „superschnelles mobiles Internet“ ist das in der Presse und von der Politik am meisten propagierte Thema im Zusammenhang mit 5G. Es geht um eine Steigerung der Datenraten auf 100 Mbit/s pro Nutzer, wann und wo immer es benötigt wird. Dazu gehört eine Transportleistung („Peak Rate“) von 10 bis 20 Gigabit/s an der Radio-Schnittstelle. Gleichzeitig muss entsprechend der kommenden Anforderungen ein bis zu 10.000-fach erhöhtes Datenvolumen bewältigt werden. Die Leitanwendungen für diese Datenraten sind Virtuelle Realität, vor allem im Bereich Lernen und Arbeiten, sowie 3D-Video. Zu den mobilen Breitbanddiensten gehört auch die Anbindung von Gebieten ohne Kabel-Infrastruktur an das Internet.

4.6.2.2 Mobiles Internet der Dinge

Dies ist ein wichtiger Bereich für die industriellen 5G-Anwendungen. Die Themen Netz-abdeckung, geringer Energiebedarf und lange Batterielaufzeiten von bis zu 10 Jahren in mobilen Endgeräten mit einem Paar handelsüblicher AA- Batterien, sowie eine extrem hohe Anzahl von parallelen Verbindungen von bis zu 1 Million angeschlossener Geräte pro Quadratkilometer sind im Kapitel Internet der Dinge unter LTE bereits besprochen worden. Wegen der Unterstützung von Millionen angeschlossener Endgeräte pro Funkzelle wird hier auch von massiver Maschine-zu-Maschine Kommunikation gesprochen (massive Machine-type Communication, mMTC). In diesem Bereich wird das Thema Internet der Dinge und IoT (Abschn. 4.5.4.5) fortgeschrieben.

4.6.2.3 Sichere Kommunikation

Hier geht es um zuverlässige Datendienste mit hohen Sicherheitsanforderungen und sehr kurzer Latenz, wie sie etwa bei autonomen Fahrzeugen oder der Automatisierung von Fabriken, sowie bei allen Interaktionen mit Echtzeitanforderungen benötigt werden. Die geforderten Datenraten von 10 Mbit/s bis maximal 50 Mbit/s könnten bereits heute durch LTE dargestellt werden. Die neu hinzukommenden Anforderungen betreffen die Latenz und die Zuverlässigkeit. An der Funkschnittstelle werden Latenzwerte von 1 ms und Ende-

zu-Ende im Netz von besser als 5 ms verlangt, was eine Verbesserung um den Faktor 10 gegenüber LTE darstellt. Gleichzeitig wird eine Verfügbarkeit und Zuverlässigkeit von besser als 99,9999 % (das sind weniger als 10 Sekunden Ausfall pro Tag) verlangt. Damit ist der Bereich Sichere Kommunikation nicht nur für industrielle Anwender, sondern auch für Behörden und Organisationen mit Sicherheitsaufgaben von höchstem Interesse. Parallel zu mMTC wird dieser Bereich auch als Critical Machine-type Communication (cMTC) bezeichnet.

Über alle Bereiche hinweg verlangt die ITU-R eine Reduktion des Energieverbrauchs um 90 % gegenüber LTE, auf der Basis vergleichbarer Leistungen.

Die ITU-R hat die Anforderungen und Beispiele von zu unterstützenden Anwendungen in einem schematischen Diagramm dargestellt (Abb. 4.18). Die drei Bereiche Mobile Breitbanddienste, Internet der Dinge und Kritische Kommunikation markieren die Eckpunkte des Anforderungsdreiecks in der Abbildung.

4.6.3 Technische Lösungen in 5G

In diesem Kapitel sollen kurz die wesentlichen technischen Lösungen zu 5G vorgestellt werden, die im verabschiedeten 3GPP-Standard enthalten oder für die kommende Weiterentwicklung geplant sind. Ähnlich wie 4G wird 5G in einer Reihe von Standardisierungsschritten entwickelt werden. Die Liste der Anwendungs-Erfordernisse aus Abb. 4.19 ist

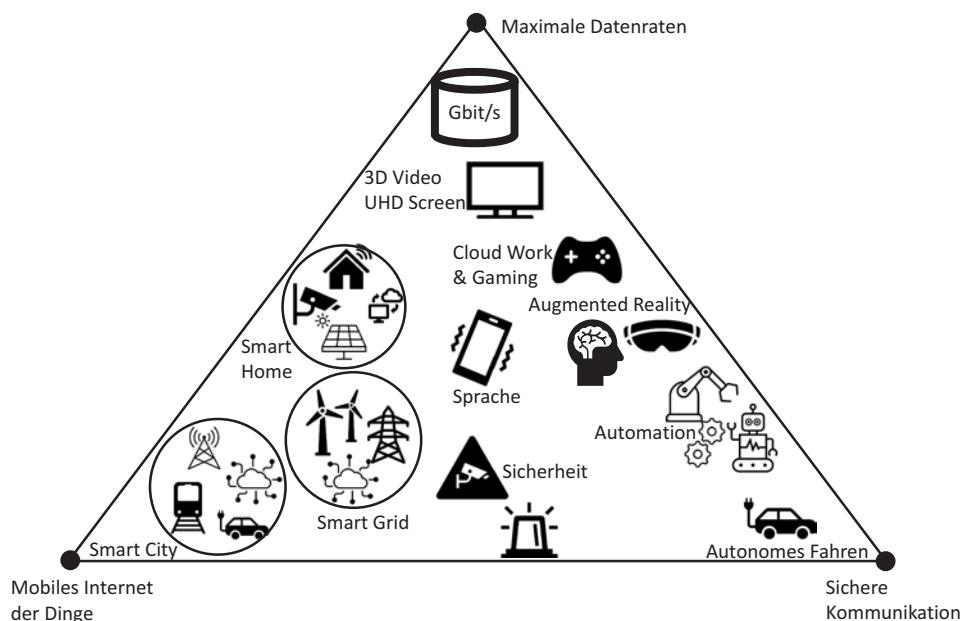


Abb. 4.18 ITU-R Anforderungen an 5G (International Telecommunications Union 2020)

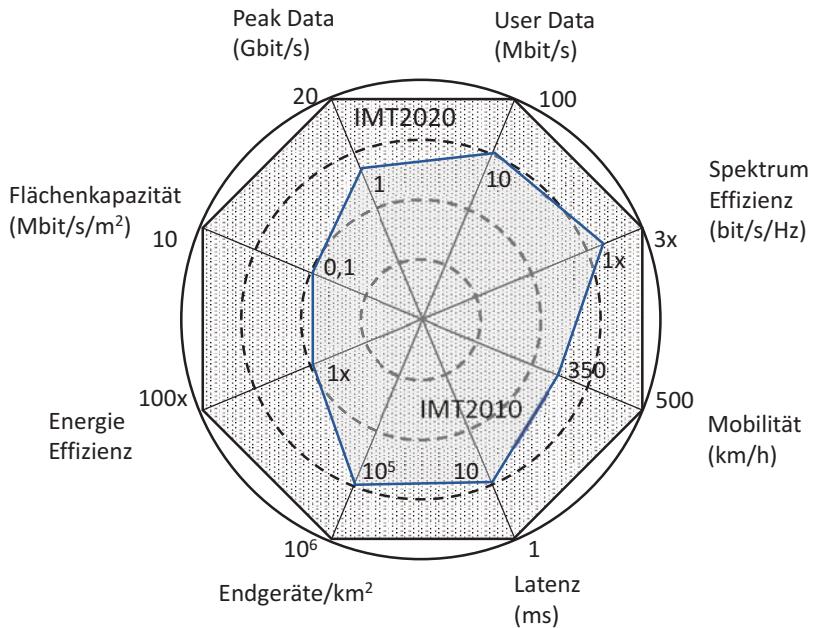


Abb. 4.19 Evolution von 4G zu 5G (International Telecommunications Union 2020)

durch die ITU-R in ein Diagramm übersetzt worden, das die Evolutionsschritte von 4G zu 5G darstellt. Die Zahlenverhältnisse zwischen 4G und 5G sind im logarithmischen Maßstab angegeben. Die Datenpunkte zu 5G liegen alle auf dem äußeren Kreis; bei einer Verbesserung um den Faktor 10 gegenüber 4G liegt der entsprechende Datenpunkt zu 4G auf dem ersten inneren Kreis, bei einem Faktor 100 auf dem zweiten inneren Kreis, und so weiter.

Die Peak Data Rate bezeichnet die höchste erreichbare Datenrate innerhalb einer Zelle: Ein Endgerät mit hinreichenden Möglichkeiten befindet sich hierbei direkt neben der Antenne der Basisstation. Die Peak Data Rate soll um den Faktor 20 gegenüber 4G steigen. Die für den einzelnen Nutzer verfügbare Datenrate soll aber nur um den Faktor 10 erhöht werden. Dies spiegelt das enorme erwartete Wachstum der Teilnehmer und Endgeräte im betrachteten Zeitraum wider. Bemerkenswert ist die Verbesserung der Energie-Effizienz um den Faktor 100. Ohne diese Bedingung würde das um den Faktor 100 wachsende Datenvolumen (Flächenkapazität) auch einen um den Faktor 100 steigenden Energieverbrauch nach sich ziehen. Die Forderung bedeutet also letztlich, das Wachstum von Datenraten und Datenvolumen ohne zusätzlichen Energieverbrauch zu bewältigen.

4.6.4 5G-Frequenzbänder und Bandbreiten

Während 4G für Bandbreiten von bis zu 20 MHz definiert wurde, sind für 5G-Frequenzbänder bis zu 400 MHz vorgesehen. Erzielbare Datenraten stehen im engen Zu-

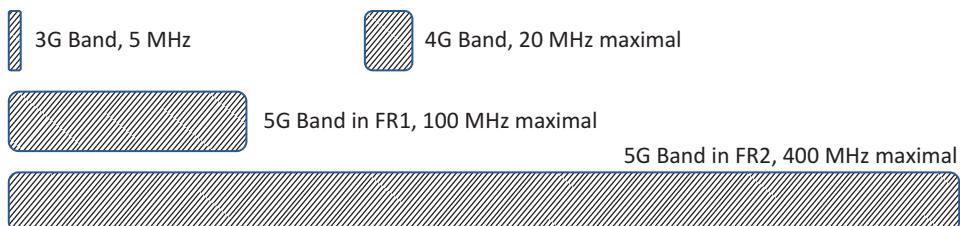


Abb. 4.20 Vergleich der größten nutzbaren Bandbreiten von 3G, 4G und 5G

sammenhang mit der verwendeten Bandbreite, so dass diese Erweiterung ein wichtiger Schritt auf das Design-Ziel darstellt. Auf einem 400 MHz-Frequenzband kann mit gleichem Verfahren nahezu bis zur 20-fachen Datenrate von 20 MHz übertragen werden. Die Abb. 4.20 zeigt die größten geplanten Frequenzbänder der Frequenzbereiche FR1 und FR2 im Vergleich mit den jeweils größten Bandbreiten von 4G und 3G.

Für 5G sind bereits eine ganze Reihe von Frequenzbändern vorgemerkt, die mit n1 bis n85 nummeriert sind. Dabei steht n für „New Radio“ zur Unterscheidung zwischen LTE und 5G-Bändern. Im Frequenzbereich FR1 der Frequenzen bis 6 GHz befinden sich viele Bänder, die heute schon für 2G, 3G oder 4G genutzt werden. Dabei werden die 2G- und 3G-Bänder nach Abschaltung der entsprechenden Systeme zur Nutzung durch 5G frei. Die derzeitigen 4G-Bänder werden zum Teil weiter genutzt, da 4G und 5G für einige Jahre koexistieren sollen. Das Frequenzband n78 von 3,4 GHz bis 3,8 GHz war seit 2001 der Technik Broadband Wireless Access nach IEEE802.16 (WiMax), einem LTE-Konkurrenten, zugeordnet. Wegen des mangelnden Erfolgs gegenüber LTE wird WiMax international kaum noch genutzt, so dass nunmehr diese Frequenzen für die neue Generation des Mobilfunkes zur Verfügung gestellt werden konnten. Das Band n78 ist sehr begehrt, bietet es doch als einziges im Bereich unter 6 GHz die Nutzung von Bandbreiten bis 100 MHz. Unterhalb von 6 GHz gibt es keine Möglichkeit, Bänder von mehr als 100 MHz Breite unterzubringen.

Oberhalb der 6 GHz-Schranke liegen Frequenzbereiche, die für Satellitenkommunikation intensiv genutzt werden und dem Mobilfunk deshalb nicht zur Verfügung stehen. Der Mobilfunk-Frequenzbereich FR2 beginnt daher bei 26 GHz. Die durch die ITU vergebenen Bänder liegen im sogenannten K_a-Band zwischen 26 GHz und 42 GHz, in dem noch hinreichend große Lücken identifiziert werden konnten, um die benötigten 400 MHz zu vergeben.

Die Bundesnetzagentur hat 2019 eine erste 5G-Frequenzauktion durchgeführt. Dabei wurden Frequenzen von 3,4 GHz bis 3,7 GHz aus dem auch international am meisten genutzten Band n78 an die vier Bewerber Deutsche Telekom, Vodafone, Telefónica O2 und 1&1 Drillisch vergeben. Zusätzlich werden auf Antrag und gegen eine Gebühr bis zu 100 MHz im Band n78 von 3,7 GHz bis 3,8 GHz an die Industrie für nicht öffentliche lokale Unternehmensnetze vergeben. Die n78-Frequenzen wurden „ungepaart“, also für die Verwendung mit dem Duplex-Verfahren TDD vergeben. Uplink und Downlink finden dabei im Zeitmultiplex auf derselben Frequenz statt.

Neben den ersteigerten 5G-Frequenzen haben die deutschen Netzbetreiber begonnen, bereits für vorherige Generationen genutzte und durch die ITU-R vorgesehene Frequenzbereiche auf 5G umzuwidmen. Dabei handelt es sich derzeit um die Bänder n1 (2100 MHz, UMTS) und n3 (1800 MHz, GSM und LTE), die in der Auktion der Bundesnetzagentur im Jahr 2015 neu vergeben worden waren. Der 700 MHz-Bereich (5G-Band n28) wurde nach Einführung des digitalen Fernsehens nach DVBT(-2) bis 2019 von den Rundfunkstationen geräumt. Die Nutzung der niedrigen Frequenzen für 5G ist entscheidend für die schnelle Verfügbarkeit des Standards in der Fläche. Wegen der kürzeren Reichweite wären bei höheren Frequenzen sehr viele zusätzliche Masten zu errichten. Im Bereich der hohen Frequenzen wurde das Band n258 im 26 GHz-Bereich als weiteres TDD-Spektrum lizenziert. Eine Übersicht der augenblicklich in Deutschland für 5G nutzbaren Frequenzen zeigt Abb. 4.21.

Die Funkschnittstelle von 5G leitet sich von 4G ab. Es gibt keine grundsätzlich neue Struktur, sondern eine evolutionäre Entwicklung. In den folgenden Absätzen wird diese Entwicklung kurz beschrieben.

4.6.4.1 Datenraten

Ein weiterer Schritt auf höhere Datenraten zu ist die Verwendung von höheren Modulationsverfahren: Definiert worden sind 256QAM und 1024QAM über die in LTE gebräuchlichen 64QAM hinaus. Mit 8 bzw. 10 Bit pro Symbol kann die erreichbare Datenrate gegenüber 64QAM um mehr als 60 % erhöht werden.

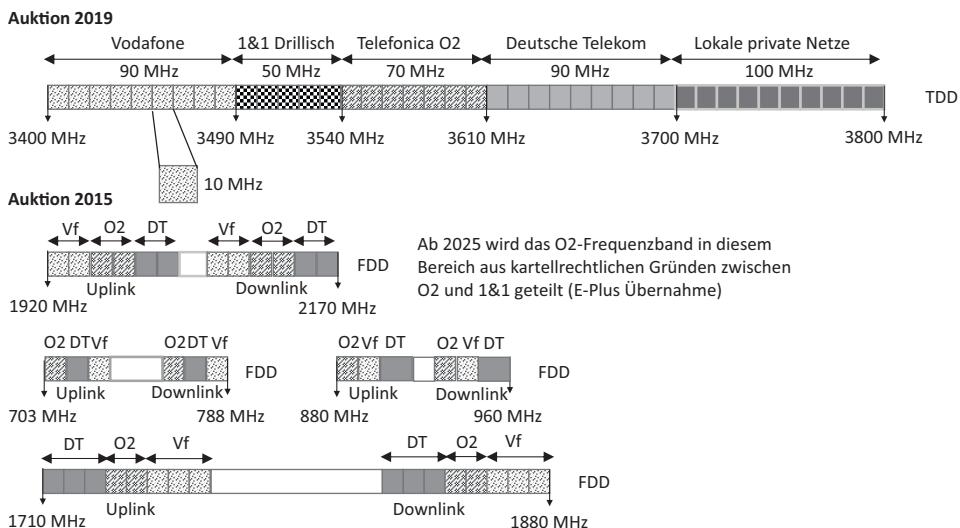


Abb. 4.21 5G-Frequenzen in Deutschland, Stand nach den Auktionen 2015 und 2019 (Bundesnetzagentur 2020)

Das MIMO-Prinzip von LTE wird zu Massive MIMO (mMIMO) mit zunächst 64 Antennenelementen ausgebaut. Dadurch wird ein „Multi-User Beamforming“ ermöglicht: Mehrere Sendekeulen können gezielt auf einzelne Endgeräte oder Gruppen von Endgeräten ausgerichtet werden. Jeder dieser Keulen kann – wie bei LTE – aus mehreren unabhängigen Datenströmen bestehen. Höhere MIMO-Schemata sind vor allem in den FR2-Bereichen in der Entwicklung. Dort unterstützt die licht-ähnliche Ausbreitungscharakteristik der Funkwellen die Bildung von engen Funkfeldern. Gleichzeitig erlaubt die kurze Wellenlänge von bis zu 1 cm kleine Antennenelemente, die in hoher Zahl zu akzeptablen Antennengrößen zusammengesetzt werden können.

4.6.4.2 TDD statt FDD

Im Zusammenhang mit mMIMO wird das bereits im Zusammenhang mit LTE entwickelte TDD-Verfahren zur dominanten Duplex-Technologie und löst das in Deutschland bislang ausschließlich verwendete FDD ab. TDD ermöglicht eine extrem schnelle Antwort der Gegenstelle auf Anweisungen zur Verlagerung der Senderichtung der einzelnen Beamforming-Funkfelder. Innerhalb desselben Rahmens stehen sowohl Downlink als auch Uplink Senderessourcen zur Verfügung. Damit kann ein MIMO-Stream präzise und flexibel gesteuert werden.

4.6.4.3 Verkürzte Rahmen und Latenz-Zeiten

5G verwendet im Grundsatz die Rahmenstruktur von 4G (Tab. 4.3). Der Standard erlaubt jedoch eine flexiblere Nutzung der Zeit- und Frequenzressourcen: Die Subframellänge kann von 1 ms (fester LTE-Wert) auf eine halbe Millisekunde und weiter in Halbierungsstufen bis zu 1/32 ms verkürzt werden. Damit verbunden verdoppelt sich in jedem Schritt die Breite der OFDM-Bänder von 15 kHz auf 30 kHz und bis zu 480 kHz. Die Datenraten verändern sich durch die Variation nicht; allerdings wird die mögliche Antwortzeit um einen Faktor bis zu 1/32 verkürzt. Auf diese Weise wird an der Funkschnittstelle eine Latenz von unter 1 ms möglich.

Für TDD-Bänder sollte eine verbindliche Aufteilung in Downlink- und Uplink-Ressourcen erfolgen, um die gegenseitige Beeinflussung zu minimieren. Die deutschen Netzbetreiber und die Bundesnetzagentur haben sich auf ein Schema DDDSU verständigt. Dabei bezeichnet D einen Downlink-Slot, U einen Uplink-Slot und S eine Umschalt-Periode. Für den Downlink steht also die dreifache Kapazität wie für den Uplink zur Verfügung.

4.6.4.4 Energie-Effizienz

Messungen in LTE haben ergeben, dass nur etwa 20 % des gesamten Energieverbrauchs auf die eigentliche Datenübertragung zurückgehen. Vereinfachte Architektur und die Cloud-Implementierung reduzieren den nicht genutzten Energieverbrauch deutlich. Verbesserte und vereinfachte Protokolle reduzieren die Brutto-Datenmenge. Dank der hohen Leistung aktueller elektronischer Komponenten können sowohl Netzkomponenten als auch Endgeräte für sehr kurze Perioden, in denen keine Daten ausgetauscht werden, in einen Schlaf-Modus versetzt werden. Ein von der Fraunhofer Gesellschaft durchgeföhrter

Test im Auftrag des Umweltbundesamtes hat gezeigt, dass das CO₂-Äquivalent von einer Stunde Video-Streaming über 5G mit 5 Gramm gegenüber 16 Gramm bei 4G deutlich verringert ist (Umweltbundesamt 2020). Bei 3G lag der Wert noch bei 90 g CO₂. Diese Werte enthalten jeweils die Anteile für die Verarbeitung und Übertragung im Kern-Netz, die in allen Technologien vergleichbar sind, und zeigen so nur eine Tendenz.

4.6.5 5G-Architektur

Die Architektur eines 5G-Netzes ist als Folge der zahlreichen neuen Anforderungen deutlich vielfältiger und damit komplexer als die Architektur eines 4G-Netzes. Die 5G-Struktur ist die eines virtuellen Netzes mit Steuerungsfunktionen in der Cloud.

Abb. 4.22 gibt einen Überblick über die Architektur eines 5G-Netzes. Der Kern-Netzanteil besteht aus Funktionen in einer privaten Operator-Cloud. Diese Funktionen ersetzen die Netzknöten des LTE-Netzes. Nachstehend sind die wichtigsten 5G-Funktionen und ihre Entsprechung in 4G beschrieben, die auch in der Abbildung durch die hellgraue Beschriftung angegedeutet sind.

- Access und Mobility Management Funktion (AMF). Dieses Modul entspricht einem Teil der MME Funktionen. Es regelt den Zugang von Endgeräten zum Netz, die

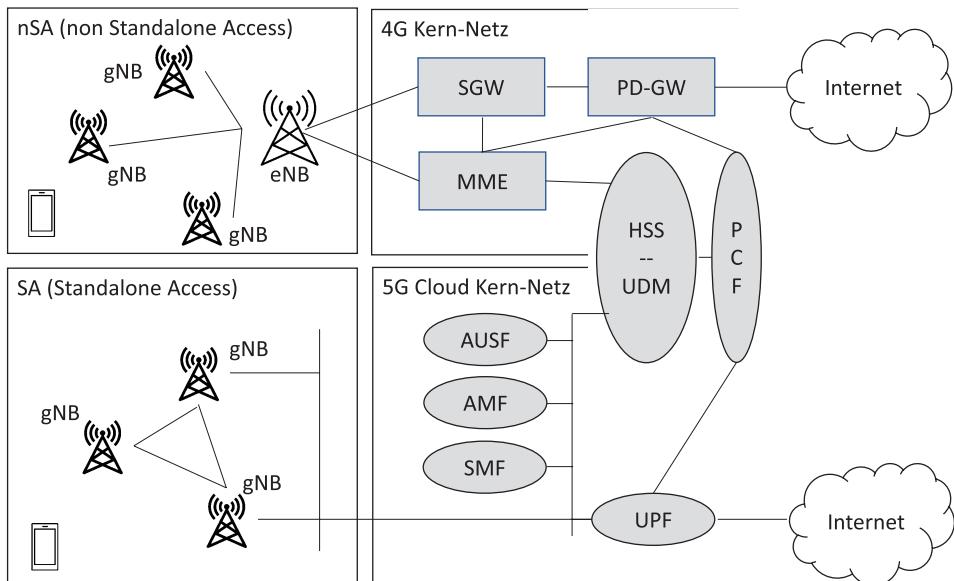


Abb. 4.22 Übersicht 5G-Architektur mit Cloud-Kern-Netz und Radio-Netz in Standalone und Non-Standalone Architektur

Authentifizierung der Teilnehmer und die Mobilität. Die Abwicklung von Kurznachrichten liegt ebenfalls bei der AMF. Die Bereitstellung und Analyse der Schlüsseldaten übernimmt dabei in Zusammenarbeit mit dem Unified Data Management die Authentication Server Function (AUSF).

- Session Management Funktion (SMF). Das SMF Modul entspricht den übrigen Funktionen der MME, die für das Management der Verbindung verantwortlich sind. Es steuert den Aufbau der Datenverbindung, und verwaltet den Datentunnel vom Endgerät zum externen Datennetz.
- User Plane Funktion (UPF). Dieses Modul kombiniert die S-GW und PDN-GW Funktionen in 4G. Durch die Virtualisierung in der Cloud ist eine physikalische Aufspaltung in zwei Knoten nicht mehr erforderlich.
- Policy Control Function (PCF). Das PCF Modul entspricht in seiner Funktionalität dem Policy and Charging Rules Server (PCRF) in 4G. Es setzt die Mindestanforderung und die Grenzen für die Datenverbindung des Teilnehmers aufgrund des hinterlegten Tarifes. Die PCF sorgt auch für die bevorzugte Behandlung priorisierter Dienste entsprechend dem Tarifmodell.
- Unified Data Management (UDM). Das Modul entspricht dem Home Subscriber System (HSS)

Daneben gibt es noch eine Reihe von anderen Modulen, die sich mit Teilnehmerverwaltung, mit Abrechnung, Qualitätsmanagement und Netzwartung befassen. Der Nachrichtenaustausch zwischen diesen Kern-Funktionen wird über APIs und Function Calls realisiert.

Die Virtualisierung ermöglicht eine flexible Reaktion auf Last-Spitzen. In Perioden hoher Anmeldetätigkeit am Netz kann zum Beispiel die AMF Funktion vervielfacht werden. Eine hohe Anzahl von verlässlichen Verbindungen, zum Beispiel bei der Steuerung eines Autobahn-Abschnittes mit autonomen Fahrzeugen, erfordert das ständige Einrichten und Verändern zahlreicher Datentunnel. Dementsprechend wird in dieser Situation das Modul SMF gefordert und durch das operative Management vervielfacht werden.

Im Radiobereich wird mit der Next Generation Node B (gNodeB, kurz: gNB) eine neue Generation von Basisstationen eingeführt. Im Vergleich zum Vorgänger eNodeB bei LTE haben die gNodeB ein einfacheres Design und reduzierte Funktionalität. Ein Teil der Steuerungs-Aufgaben wird in einem voll ausgebauten 5G-Netz künftig wieder vom Kernnetz wahrgenommen. Ermöglicht wird dies durch die schnellen Verbindungen in die Cloud-Infrastruktur. Bis ein vollständiges 5G-Kern-Netz zur Verfügung steht, muss die Steuerung der gNodeB durch das bestehende 4G-Netz ausgeführt werden.

4.6.5.1 Migration von 4G zu 5G

Die evolutionären Schritte von 2G bis zu 4G wurden im Netzbetrieb auf eine sehr einfache Weise bewältigt: Die neue Netzinfrastruktur wurde parallel zu den existierenden Netzen aufgebaut und in Betrieb genommen. Netztechnologie, für die der Bedarf zurückging, wurde zurückgebaut und möglicherweise außer Betrieb genommen. Bei 5G stößt dieses

Vorgehen an seine Grenzen: Mit Ausnahme einiger neuer Frequenzbänder ist 5G auch für Bänder definiert, die bereits für 2G, 3G oder 4G vergeben wurden. Für den Flächenausbau von 5G werden diese Bänder benötigt, da bei den höheren Frequenzen, etwa von n78, wegen der geringeren Reichweite zahlreiche Masten neu errichtet werden müssten. Der nachlassende Bedarf an 2G- und 3G-Diensten erlaubt, diese außer Betrieb zu nehmen. Für den Übergang von 4G zu 5G ist allerdings eine möglichst unterbrechungsfreie Migrationsstrategie erforderlich. Zwei wesentlichen Elemente dieser Strategie sind der *Non-Standalone Modus* (NSA) von 5G und das Feature *Dynamic Spectrum Sharing* (DSS).

Im Non-Standalone Modus wird die vorhandene 4G-Infrastruktur zur Steuerung der neuen 5G-Basisstationen gNodeB genutzt. Ein 5G-Endgerät wird sich im NSA-Modus immer am 4G-Netz anmelden und auch alle Kontroll-Nachrichten mit dem vorhandenen 4G-Netz austauschen. Das 4G-Netz registriert das Endgerät als 5G-kompatibel, und routet die Nutzdaten über einen gNodeB, der als Slave an dem vorhandenen 4G eNodeB als Master angeschlossen ist. Da die ersten gNodeB an vorhandenen 4G-Standorten errichtet werden, werden Master eNodeB und Slave gNodeB am gleichen Standort installiert sein. In der Regel wird ein neu installierter gNodeB in einem separaten 5G-Band, wie etwa n78, arbeiten. 4G und 5G können aber mittels Dynamic Spectrum Sharing (DSS) auch im selben Frequenzband genutzt werden. Moderne 4G-Basisstationen können durch einen Software-Upgrade auf die Verarbeitung von 5G-Daten im selben Frequenzband aufgerüstet werden. Die Allokation von Datenblöcken zu 4G und 5G erfolgt dann dynamisch durch den eNodeB entsprechend des Anteils der Endgeräte der beiden Standards.

4.6.6 Sichere Kommunikation und Internet der Dinge in 5G

Für die in 5G verlangte sichere Kommunikation müssen hochverfügbare Übertragungen mit kurzer Latenz ermöglicht werden. Die Kombination beider Forderungen ist ein hoher Anspruch an die Technik. Es ist bei der geforderten kurzen Latenz nicht möglich, Verfügbarkeit nur durch Wiederholungs- und Korrekturmechanismen zu schaffen. Stattdessen müssen räumliche Redundanzen geschaffen werden. Das kann über separate Wegführung von Verbindungen, aber auch die Frequenz-Diversität erfolgen. Bei hoher Bandbreite der 5G-Bänder kann durch die flexibilisierte Rahmenstruktur durch verkürzte Symbollängen Zeit für Wiederholungen geschaffen werden. Gleichzeitig können in der Frequenzdimension durch die verbreiterten OFDM-Bänder identische Datenströme in hinreichend großem Frequenzabstand geführt werden, so dass sie redundant bezüglich äußerer Störinflüsse sind. Sofern ein Endgerät im Abdeckungsbereich von mehr als einer Basisstation ist, lässt sich auch eine vollkommen redundante Führung über zwei räumlich getrennte Wege realisieren. Dazu werden die im Folgenden beschriebenen virtuellen Verbindungen genutzt.

Die M2M-Kommunikation ist durch die Entwicklung von NB-IoT und LTE-M in LTE bereits so weit fortgeschritten, dass die ITU-R Anforderungen auf diesem Sektor durch einige evolutionäre Anpassungen an die 5G-Strukturen erfüllt werden können.

4.6.7 Virtuelle Strukturen in 5G

Wie bei der 5G Architektur dargestellt nutzt 5G Cloud Strukturen und Virtualisierung. Die Bedeutung der virtuellen Strukturen reicht jedoch weit über die Effizienzsteigerungen und die Kostenersparnis hinaus, wie sie mit der Nutzung der Cloud-Technologien im Netz erreicht wird. Bei der Virtualisierung der Netzwerktechnik werden die Begriffe *Network Function Virtualization* (NFV) und *Software Defined Networking* (SDN) unterschieden. Mittels NFV werden Netzwerkfunktionen mittels Software auf einer Standard-Hardware dargestellt. SDN verfolgt den Netzmanagement-Ansatz, komplexe Netzkonfigurationen in Software darzustellen, und sozusagen auf „Knopfdruck“ verfügbar zu machen. SDN ist auch in Kombination mit traditioneller Hardware vorstellbar, entfaltet seine volle Kraft allerdings erst, wenn die Netzressourcen virtuell zur Verfügung stehen.

5G definiert auch für das Funknetz auf der Basis von RAN Hardware virtuelle Netze durch NFV. So können virtuelle Netze mit sehr verschiedenen Eigenschaften in einer Region auf derselben Hardware existieren. Die Vielfalt der Anforderungen in Bezug auf Bitrate, Latenz oder Redundanz aus Abb. 4.19 lässt sich so mit nur einer Hardware realisieren. Über die funktionale Unterscheidung hinaus können mit der Virtualisierung auch administrative Aufteilungen durchgeführt werden. Verschiedene Nutzergruppen oder virtuelle Netzbetreiber können eine gemeinsame Hardware-Basis nutzen. Der Fachbegriff hierzu ist *Network Slicing*, also die Aufteilung der Netzressourcen in „Scheiben“ für die jeweiligen Anwendungszwecke. Network Slices sind virtuelle Mobilfunknetze auf der Basis eines einzigen realen Netzes. Slices können durch gleichartige Qualitätsparameter definiert werden, sind aber auch rein administrativ möglich. Netzbetreiber können durch Slicing Kapazität örtlich, regional oder landesweit einem virtuellen Betreiber zur Verfügung stellen. Das Einrichten und das An- bzw. Abschalten von Network Slices, sowie das Kapazitätsmanagement können flexibel per SDN vom Kontrollzentrum aus durchgeführt werden, ohne jemals Umschaltungen an der Hardware vornehmen zu müssen.

Das Kern-Netz kann mehrfach redundant im Load-Sharing Betrieb an mehreren Standorten betrieben werden. Für den Netzbetreiber besteht die Option, das Kern-Netz georedundant und damit katastrophensicher und ausfallsicher auszulegen. Für spezielle Anwendergruppen ergibt sich auch die Möglichkeit, ein „eigenes“ Kern-Netz zu betreiben. So können Industrie-Kunden einen von ihnen bei einem Netzbetreiber beauftragten Netzwerk-Slice von einer Hardware im eigenen Kontrollbereich aus als Teil des gesamten Netzes zu betreiben. Für Rettungskräfte oder Sicherheitsorgane können mobile Kern-Netzkomponenten nahe am Einsatzort zur Verfügung stehen. In beiden Fällen ergeben sich ein hohes Maß an Kontrolle und schnelle Reaktionsmöglichkeiten.

4.6.8 Cloud Edge Computing

Durch 5G werden neue Formen der Cloud ermöglicht. Die verteilte Architektur des 5G Kern-Netzes erlaubt es, Cloud-Funktionen in räumliche Nähe zu den Nutzern und End-

geräten zu bringen. Dazu werden Kern-Netz Funktionen in lokale Datencenter integriert. Für den Anwender von Cloud-Diensten wie *Infrastructure as a Service* (IaaS), *Platform as a Service* (PaaS) oder *Software as a Service* (SaaS) bedeutet dies eine bessere Anbindung mit hohen Datenraten, Redundanz, kurzer Latenz und großer Flexibilität. Die Datenverarbeitung kann nahe bei der Datenquelle stattfinden. Ein Cloud-Edge-Service Angebot in einer Stadt oder Region kann durch einfache Konfiguration auch für Anwender in einer entfernten Region oder Stadt lokal vor Ort gemacht werden. Die Kombination von schnellem, flexiblem Zugang, auch zu mobilen Endgeräten, mit der globalen Präsenz eines Mobilfunknetzes kann zu neuen Anwendungen führen. Für Netzbetreiber öffnet sich ein Fenster für neue Geschäftsmodelle als Cloud Serviceprovider. Im Bereich öffentlicher Dienste und bei Sicherheits-Services können in gleicher Weise Leitstellen und Einsatzkräfte direkt an Einsatzorten mit kurzer Latenz und hoher Zuverlässigkeit mobil kommunizieren, während sie mit anderen Gruppen und zentralen Ressourcen über das globale Mobilfunknetz verbunden sind.

4.7 Fragen

1. Nennen Sie 5 historische Mobilfunkstandards
2. Wofür steht die Anzeige „E“ im Display eines Mobiltelefons?
3. Welche Netzkomponenten sind für die Vermittlung von Sprachverbindungen in den Generationen 2G (GSM), 3G (UMTS) und 4G (LTE) verantwortlich?
4. Bestimmen Sie die Anzahl der möglichen parallelen Telefongespräche in GSM über eine Basisstation mit 3x2 Konfiguration (3 Sektorantennen, mit jeweils 2 Frequenzbändern pro Sektor).
5. Wann wurde der 3G-Standard eingeführt?
6. Wie heißt das in 3G verwendete Multiplexverfahren und welchen grundsätzlichen Unterschied zu Zeit- und Frequenzmultiplex gibt es?
7. Wie unterscheiden sich die Netzarchitekturen von 2G und 3G voneinander?
8. Nennen Sie die grundsätzlichen Anforderungen des 4G-Standards an erreichbare Datenrate und Latenz
9. Welche Möglichkeiten bestehen für einen Telefonanruf im 4G Netz?
10. Beschreiben Sie 2 Veränderungen der Netz-Architektur von UMTS/3G zu LTE/4G
11. Welches Multiplexverfahren wird bei LTE eingesetzt?
12. Was ist ein Physical Resource Block (PRB)?
13. Geben Sie eine Schätzung der erzielbaren Bandbreite einer LTE-Verbindung mit 10 MHz Bandbreite und mittlerer Signalqualität an.
14. Unter welchen Umständen wird das LTE-Netz ein mobiles Endgerät an eine andere Technologie (UMTS, GSM) übergeben.
15. Nennen Sie zwei in LTE mögliche Nutzungen der MIMO-Technologie.

-
16. Bei 2G- und 3G-Netzen war es notwendig, beim Handover von einer Basisstation zu einer anderen die laufenden Verbindungen *unterbrechungsfrei* zu übergeben. Was gilt bei einem Handover bei LTE/4G?
 17. Welches sind die auf LTE aufbauenden Technologien für das Internet der Dinge?
 18. Welche grundlegenden Anforderungen an Mobilfunktechnik liegen der Generation 5G zugrunde?
-

Literatur

- Bauchmüller M, Martin-Jung H (2018) Der schnelle Mobilfunk kann kommen. Süddeutsche Zeitung, 26. November 2018
- Bundesnetzagentur (2020) Mobiles Breitband. Bonn. https://www.bundesnetzagentur.de/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Frequenzen/OeffentlicheNetze/Mobilfunknetze/mobilfunknetze-node.html. Zugegriffen am 26.08.2021
- Ericsson (2020) Ericsson Mobility Report – June 2020. Stockholm. <https://www.ericsson.com/en/mobileity-report>. Zugegriffen am 24.06.2021.
- Institut für Rundfunktechnik (2019) Sendeplatz Ismaning für bayerisches Forschungsprojekt „5G TODAY“ einsatzbereit. München: Institut für Rundfunktechnik GmbH. https://www.irt.de/fileadmin/media/downloads/pressemitteilungen/2019/Pressemeldung_Sendeplatz_Ismaning_einsatzbereit.pdf. Zugegriffen am 26.08.2021.
- International Telecommunications Union (2020) Minimum requirements related to technical performance for IMT-2020 radio interface(s) (Report ITU-R M.2410-0). Geneva. https://www.itu.int/dms_pub/itu-r/opb/rep/R-REP-M.2410-2017-PDF-E.pdf. Zugegriffen am 26.08.2021.
- Johnson C (2012) Long Term Evolution in Bullets (2. Auflage). CreateSpace Independent Publishing Platform, Northampton. 978-1-478-16617-7
- Liberg O, Sundberg M, Wang YPE, Bergman J, Sachs J (2018). Cellular Internet of Things: Technologies, Standards, and Performance. Academic Press (1. Aufl.). Academic Press, London. 978-0-128-12458-1
- LTE Broadcast Alliance (2016). LTE Broadcast – Lessons Learned from Trials and Early Developments. <https://de.slideshare.net/DannyDicks/lte-broadcast-lessons-learned-from-trials-and-early-deployments> Zugegriffen am 26.08.2021.
- Umweltbundesamt (2020) Hintergrundinformationen Klimawirkung von Videostreaming & Co. Dessau-Roßlau: Umweltbundesamt. <https://publicarea.admiralcloud.com/p/iRg9WDwNJTyr1D21Bx4mY>. Zugegriffen am 26.08.2021.
- Verband der Automobilindustrie (2019) Bestehende eCall-Übertragungsnetze müssen erhalten bleiben. Berlin: Verband der Automobilindustrie. <https://www.vda.de/de/presse/Pressemeldungen/191126-bestehende-e-call-Uebertragungsnetze-muessen-aufrechterhalten-werden.html>. Zugegriffen am 26.08.2021.



Lizenzfreie Kommunikationstechniken

5

5.1 Einführung und Lernziele

Im Folgenden sollen weitere Technologien der drahtlosen Kommunikation vorgestellt werden. Dabei handelt es sich um Anwendungen in frei verfügbaren Frequenzbändern, für die keine Funklizenz erworben werden muss. Ein weiteres verbindendes Element der vorgestellten Technologien ist ihre Verwendung in der Maschine-zu-Maschine Kommunikation, dem Internet der Dinge. Oft ermöglichen diese Kommunikationstechniken im Nahbereich den Kontakt zu Smartphones. Lizenzfreie Kommunikationslösungen können allerdings auch in Konkurrenz zu lizenzierten Netzen treten, wie bei den Low Power Wide Area-Techniken zu sehen ist. Die hier dargestellten Lösungen sind eine Auswahl der existierenden Lösungen. Sie reichen von Möglichkeiten zur drahtlosen Nahbereichskommunikation und -erfassung unter dem Begriff „Wireless Personal Area Network“ (WPAN) über lokale Netze „Wireless Local Area Networks“ (WLAN) bis zu Weitverkehrsnetzen „Low Power Wide Area Networks“ (LPWAN). Ergänzend wird im Rahmen der Nahbereichskommunikation die optische Erfassung grafischer Codes dargestellt.

Eine Übersicht der Möglichkeiten mobiler Kommunikation bietet Abb. 5.1.

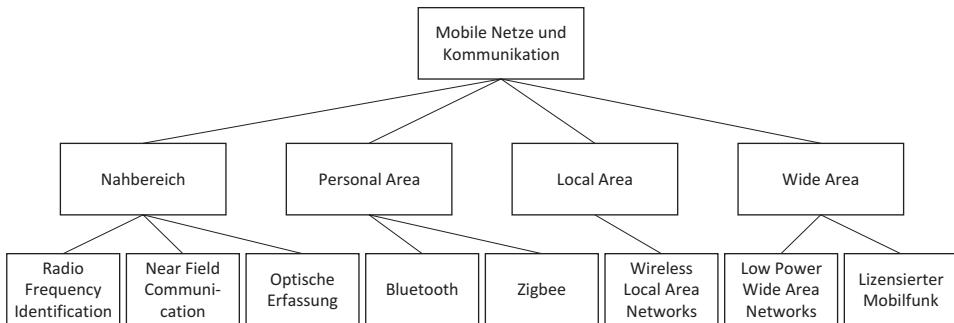


Abb. 5.1 Systeme für mobile Kommunikation

► Lernziele

- Sie erhalten einen Überblick über die verfügbaren lizenzenfreien Frequenzbereiche.
- Sie verstehen die Unterschiede in der Nutzung von lizenzierten und lizenzenfreien Frequenzen.
- Sie lernen ergänzende und alternative Techniken für die drahtlose Kommunikation neben dem Mobilfunk kennen.
- Sie verstehen, dass die Nutzung von lizenzenfreien Frequenzen über ein breites Spektrum von Entfernungen von wenigen Zentimetern bis zu 100 km möglich ist, aber auch, dass jede Nutzungsart mit spezifischen Einschränkungen verbunden ist.
- Sie erfahren, welche Kommunikationssysteme innerhalb des Internet der Dinge existieren.

5.2 Lizenzfreie Funkfrequenzen

Die Betreiber von Mobilfunknetzen erwerben ein zeitlich beschränktes, exklusives Nutzungsrecht für Frequenzbänder, in der Regel gegen Zahlung von beträchtlichen Summen. Daneben gibt es Frequenzbänder, die ohne eine kommerzielle Lizenz genutzt werden können. Dazu gehören die Industry, Science and Medical (ISM) Frequenzbänder, die von der International Telecommunications Union für die genannten Zwecke vorgeschlagen worden sind. Alle in diesem Kapitel behandelten Kommunikationstechnologien nutzen lizenzenfreie Frequenzen.

Im deutschen Recht wird die Nutzung von lizenzenfreiem Spektrum über so genannte Allgemeinzuteilungen der Bundesnetzagentur in Anlehnung an die europäische Regulierung geregelt (Bundesnetzagentur 2021). Eine Allgemeinzuteilung kann ein Frequenzband für die Nutzung durch jeden, aber auch für die Nutzung durch einen bestimmten Personenkreis erlauben.

Die Anwendungsbereiche für Allgemeinzuteilungen der Bundesnetzagentur sind

- Alarmierung und Überwachung
- Short Range Devices, also Anwendungen mit kurzer Reichweite
- Drahtlose Mikrofone
- Allgemeine Funkkommunikation, wie etwa DECT-Telefone und CB-Funk, aber auch WLAN
- Verkehr und Telematik, wie etwa intelligente Verkehrslenkung, Fahrzeug-Radar oder Zugsteuerungssysteme
- RFID-Anwendungen und die Themenkomplexe Industrial, Science and Medical.

Die Zuteilung erfolgt für eine Nutzungsart oder Anwendung unter Einhaltung von Grenzwerten wie etwa der ausgestrahlten Leistung oder der Nutzungsdauer. Die Anzahl der Nutzer ist in der Regel nicht näher bestimmt; es kann daher auch zu gegenseitigen Störungen durch Interferenz kommen. Diese potenziellen Störungen sind durch die Nutzer zu berücksichtigen. Für einige Zuteilungen existieren vordefinierte Nutzungsarten, die *Primärnutzungen*. Eine Störung einer Primärnutzung ist durch den allgemeinen Nutzer nicht erlaubt; Störungen der allgemeinen Nutzung durch den Primärnutzer sind jedoch in jedem Fall hinzunehmen. Dies gilt beispielsweise für den Betrieb von WLAN im 5 GHz-Bereich. In den meisten Fällen wird eine Begrenzung des Störopotenzials durch eine einfache Beschränkung der Sendeleistung erreicht. In einigen Frequenzbereichen, wie etwa 433 MHz oder 868 MHz, wird aber auch die maximale Belegungsdauer begrenzt. Ein Endgerät darf zum Beispiel während einer Stunde, nur 4 Sekunden lang senden (ca. 0,1 %). Häufig werden auch Dynamic Frequency Selection (DFS) und Transmission Power Control (TPC) angewendet. Durch DFS wird automatisch auf eine andere Frequenz gewechselt, wenn ein fremdes Signal auf dem gerade genutzten Band empfangen wird. TPC regelt bei jeder Datenverbindung die Sendeenergie auf das niedrigste Niveau, bei dem der Datenaustausch noch möglich ist. Geräte, die die Beschränkungen nicht einhalten, erhalten keine Betriebsgenehmigung. Tab. 5.1 zeigt die gebräuchlichen lizenzierten Frequenzbänder in Deutschland.

5.3 Radio Frequency Identification (RFID)

Als Radio Frequency Identification (RFID) wird die berührungslose und automatische Identifizierung von Objekten mittels elektromagnetischer Felder bezeichnet. Im deutschen Sprachgebrauch wird RFID mit „Funkdatenerfassung“ übersetzt. RFID gehört zu den automatischen Identifikationssystemen (Auto-ID), ebenso wie Barcode, Optical Character Recognition (OCR), Chipkarten sowie biometrische Verfahren wie z. B. Fingerabdruckverfahren und Sprach-/Gesichtsidentifizierung.

Ein RFID-System besteht aus:

- Datenträger, auch als Transponder oder Tag bezeichnet,
- Sende- und Empfangseinheit, vereinfacht auch als Erfassungsgerät bezeichnet und
- Anwendungssystem zur Speicherung und Weiterverarbeitung der Daten.

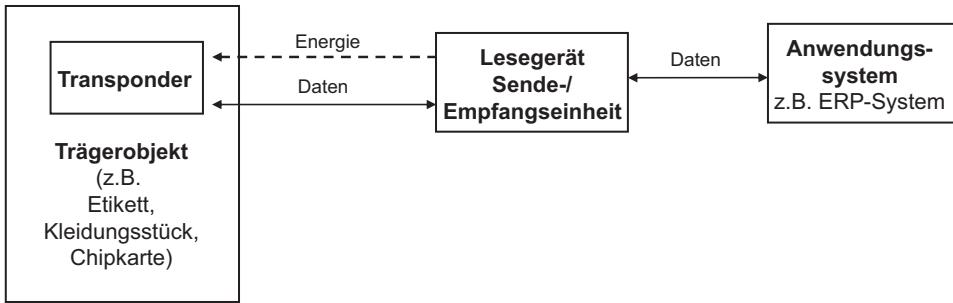
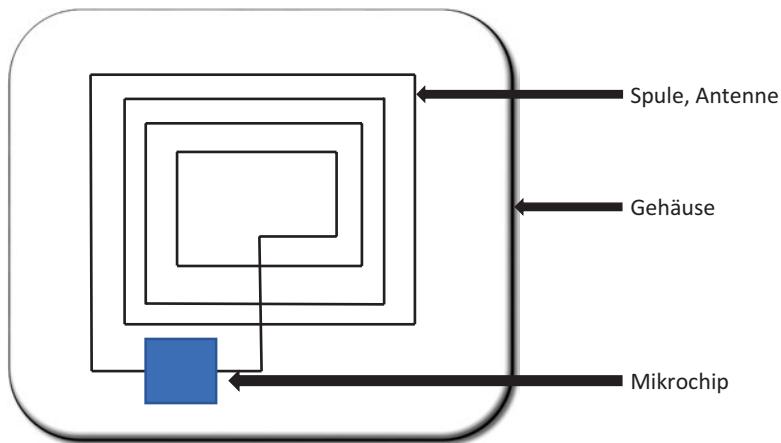
Tab. 5.1 Beispiele lizenzfreier Frequenzbänder in Deutschland

| Frequenzbereich | | Bezeichnung und Erläuterungen | Anwendungsbeispiele |
|-----------------|-------------|---|---|
| von | bis | | |
| 119 kHz | 135 kHz | LF Niedrigfrequenz/Langwelle Einschränkung der magnetischen Feldstärke | RFID induktiv |
| 13,353 MHz | 13,567 MHz | HF Hochfrequenz/Kurzwelle Einschränkung der magnetischen Feldstärke | RFID induktiv |
| 433,05 MHz | 434,790 MHz | Dezimeterwellen Einschränkung von Sendeleistung und Belegungsdauer | Handfunkgeräte, Funkthermometer, vernetzte Rauchmelder |
| 863 MHz | 870 MHz | UHF Ultrahochfrequenz Einschränkung von Sendeleistung und Belegungsdauer | Primärnutzer sind Alarmanlagen; Freigabe für LPWAN, RFID long Range, kontaktlose Schlüsselsysteme |
| 1.880 MHz | 1.900 MHz | MW | DECT Schnurlos-Telefone |
| 2.400 MHz | 2.483 MHz | Mikrowelle Im 2,4 GHz-Bereich ist die Ausgangsleistung auf 100 mW beschränkt. | WLAN, Bluetooth, RFID, IEEE 802.15.4, ZigBee, Mikrowellenherde |
| 5.150 MHz | 5.250 MHz | Im 5 GHz-Bereich bestehen in den genannten Teilbereichen unterschiedliche Einschränkungen: | WLAN in geschlossenen Räumen |
| 5.250 MHz | 5.350 MHz | Ausgangsleistungen, Verwendung von DFS und TPC, Verwendung nur in geschlossenen Räumen. | WLAN, versch. Ortungsdienste, Telematik, Wetterradar |
| 5.470 MHz | 5.725 MHz | | Verkehrstelematik, ITS-Band der ITU-R |
| 5.855 MHz | 5.905 MHz | | |
| 5.945 MHz | 6.425 MHz | Ausgangsleistung maximal 0,2 Watt. Keine Nutzung im Außenbereich oder in Straßenfahrzeugen. | WLAN Geräte mit geringer Leistung in Innenräumen (Low Power Indoor) Verfügung vom 30.06.2021 |

Transponder und Sende-/Empfangseinheit tauschen untereinander Daten und Energie über die Funkschnittstelle aus. Zwischen Sende-/Empfangseinheit und nachgelagertem Anwendungssystem läuft der Datenaustausch über herkömmliche Netzwerke (LAN bzw. WLAN, Abb. 5.2).

5.3.1 Transponder

Transponder ist ein Kunstwort, welches sich aus Transmitter (Sender) und Responder (Empfänger) zusammensetzt. Der Transponder dient vor allem als Datenträger. Je nach angewandter Technologie kann er einmalig oder auch wieder beschreibbar sein. Ein Transponder besteht unabhängig von seiner Bauform aus einem Mikrochip, einer Antenne, einem Träger bzw. Gehäuse und ggfs. einer Batterie (Abb. 5.3).

**Abb. 5.2** RFID-System**Abb. 5.3** Aufbau eines Transponders

Kernstück ist ein Speicherchip, der als Datenträger dient. Jeder Transponder besitzt eine eindeutige Identifikationsnummer und es können weitere Daten gespeichert werden, wie z. B. Produzent, Seriennummer, Verfallsdatum. Um den Speicherchip windet sich ein dünner Draht, die Antenne. Sie wird sowohl zum Senden der auf dem Chip gespeicherten Daten als auch zum Empfangen der Impulse des RFID-Lesegeräts genutzt. Transponder werden außen an einem Objekt angebracht, wie z. B. auf Paletten oder Containern, oder in ein Objekt integriert, wie z. B. in eine Chipkarte oder einen Autoschlüssel. Es besteht bei kurzen Abständen zwischen Transponder und Lesegerät keine echte Funkverbindung. Stattdessen sind die Antennen auf beiden Seiten induktiv gekoppelt, so wie die beiden Spulen in einem Transformator. Die Veränderung der Last durch Schaltvorgänge im Transponder wirkt auf die sendende Spule des Lesegerätes zurück und wird dort als Information interpretiert.

Transponder können für verschiedene Anwendungsbereiche eingesetzt werden. Zu den wichtigsten Unterscheidungsmerkmalen zählen die Bauform (Münze, kontaktlose Chip-

karte oder klebbares Etikett, auch als Smart Label bezeichnet), die Energieversorgung (aktive, passive und semiaktive Transponder), die Speicherkapazität und die Beschreibbarkeit (Read-Only, Read-Write und Write Once-Read Many). Zum Beispiel werden zur Diebstahlsicherung im Einzelhandel wiederverwendbare kostengünstige Transponder mit 1 Bit Read-Only Speicher verwendet. Für reine Identifikationszwecke kommen Transponder zur Anwendung, die bei der Herstellung bereits mit einer festen Identifikationsnummer versehen werden.

Bauformen

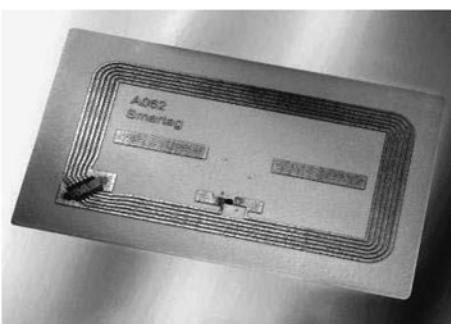
Transponder unterscheiden sich in ihrer Bauform und den damit verbundenen Eigenschaften. So gibt es beispielsweise Münzen bei Parkautomaten, Karten bei der Zutrittskontrolle, Gläsröhrchen bei der Tieridentifikation, Smartlabel (Klebeetiketten) bei Produktion und Logistik oder Armbänder in Freizeitparks und Krankenhäusern (Abb. 5.4). Die Größe wird durch Antenne und Gehäuse beeinflusst. Sie können die Größe von Büchern besitzen (z. B. in der Containerlogistik), sind aber dank heutiger Technik meist sehr klein.

Smart Label sind aufklebbare, papierdünne Transponder. Die Transponderspule wird auf eine sehr dünne Plastikfolie aufgebracht. Diese Folie wird oftmals mit einer Papier schicht laminiert und auf der Rückseite mit einem Kleber beschichtet. Smart Label können hierdurch als Selbstklebeetiketten auf einer Endlosrolle geliefert werden, um sie anschließend auf Gepäckstücke, Pakete und beliebige andere Objekte aufzukleben. Die Klebeetiketten lassen sich nachträglich noch bedrucken, sodass zusätzlich auch ein Barcode genutzt werden kann. Bei *Münz- und Scheibentranspondern* sind Chip und Antenne von einem Plastikgehäuse umgeben. Hierdurch sind sie sehr robust. Sie werden anstelle eines Schlüssels bei der Zutrittskontrolle zu Räumen sowie als Autoschlüssel mit elektronischer Wegfahrsperrre verwendet. Die Vorteile der Plastikgehäuse liegen in der Aufnahmefähigkeit von größeren Mikrochips und in der Unempfindlichkeit gegenüber mechanischen Einflüssen. *Glastransponder* werden speziell für die Tieridentifikation hergestellt und können unter die Haut injiziert werden. Kontaktlose *Chipkarten-Transponder* werden als bargeldloses Zahlungsmittel (z. B. in Kantinen) sowie als mobiles Ticket im öffentlichen Nahverkehr eingesetzt. Sie verfügen über ein eigenes Betriebssystem und unterstützen unterschiedliche Applikationen, wie z. B. Verschlüsselung und Authentifizierung.

Energieversorgung

Hinsichtlich der Energieversorgung wird zwischen aktiven, passiven und semi-aktiven Transpondern unterschieden.

Passive Transponder haben keine eigene Energieversorgung. Zum Senden bzw. Empfangen wird die Energie aus dem elektromagnetischen Feld des RFID-Lesers durch die Antenne entnommen. Wenn sich der Transponder außerhalb der Reichweite eines Lese-



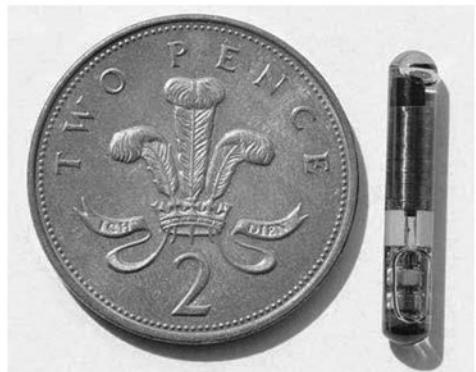
Smart Labels für Anwendungen in Logistik u. Distribution



Transponder im Chipkartenformat



Münz- und Scheibentransponder für industrielle Anwendungen



Glastransponder für Implantation unter die Haut

Abb. 5.4 Bauformen von Transpondern (Abts und Mülder 2017, S. 219)

gerätes befindet, ist dieser nicht in der Lage, ein Signal zu senden. Die Reichweite passiver Transponder beträgt zwischen einigen Zentimetern und maximal wenigen Metern. Sie sind kostengünstig und ihre Lebensdauer ist nahezu unbegrenzt.

Aktive Transponder besitzen eine eigene Energieversorgung, beispielsweise eine Batterie oder eine Solarzelle. Sie können dadurch Funksignale eigenständig erzeugen. Aktive Transponder können auch mittels Sensoren ermittelte Daten zwischenspeichern, beispielsweise den Temperaturverlauf von Kühlketten oder technische Betriebsdaten bei Flugzeugtriebwerken. Im Vergleich zu passiven sind aktive Transponder größer und teurer, allerdings ist ihre Reichweite auch größer. Ein Einsatzgebiet ist beispielsweise die automatische Erfassung von Straßenmaut-Gebühren.

Semi-aktive Transponder verfügen über eine eigene Energieversorgung, verhalten sich ansonsten aber wie passive Transponder. Sie werden nur dann aktiv, wenn sie sich in einem Antennenfeld befinden. Die Batterie verstärkt das abgegebene Signal, hierdurch erhöht sich die Sendereichweite. Oftmals werden semi-aktive Transponder im Zusammen-

hang mit zusätzlichen Sensorfunktionen genutzt, wie z. B. die Messung der Umgebungs-temperatur. Die Batterie ermöglicht in diesem Fall die Speicherung der Messdaten.

5.3.2 Lesegeräte

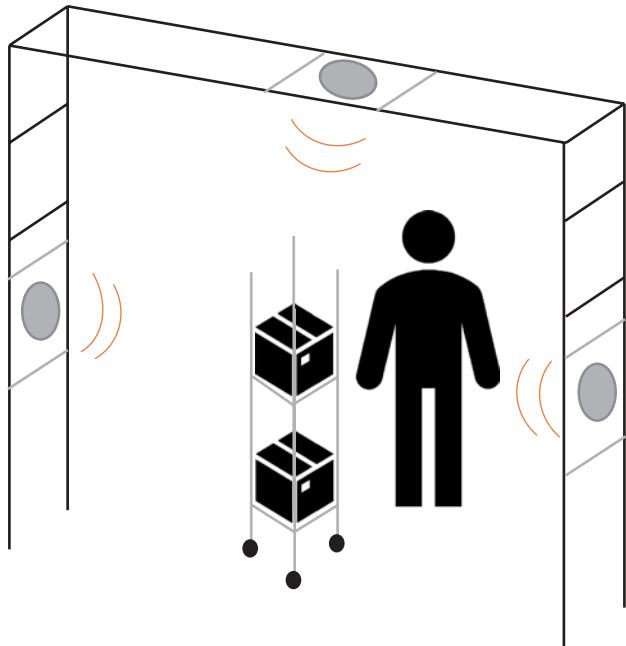
Das RFID-Erfassungsgerät – je nach Ausführung als Lese- oder Lese-/Schreibeinheit erhältlich – bildet die Schnittstelle zwischen dem RFID-Transponder und einem Anwendungssystem. Es regelt und steuert die berührungslose Kommunikation mit den RFID-Transpondern, verarbeitet die eingelesenen Daten und kommuniziert mit externen Softwareanwendungen, wie z. B. Warenwirtschaftssystemen oder ERP-Systemen. Die Lesegeräte lassen sich in zwei Gruppen einteilen:

Mobile Lesegeräte

Sie ermöglichen eine flexible ortsunabhängige Nutzung und sind für den Einsatz in Umgebungen gedacht, wo keine Verkabelung möglich ist. Eine Sonderform ist der fahrzeuggebundene Leser, angebracht in einem PKW für die Zufahrtssteuerung zu einem Parkplatz oder an einem Gabelstapler im Lager. Die mobilen Geräte bestehen aus einem Lesemodul sowie einer (integrierten oder externen) Antenne. Zudem besitzen sie einen Computer, entweder separat oder mit in das Gehäuse integriert. Die meisten Handlesgeräte verfügen über eigene Betriebssysteme mit spezifischen Programmen zum Austausch von Daten. Die erfassten Daten können im Handlesgerät zwischengespeichert und später z. B. über kabelgebundene oder funk basierte Netzwerke an ein Backend-System weitergegeben werden. Die Lesereichweite liegt zwischen zwei und zwanzig Zentimetern. Eine andere Möglichkeit für die mobile Erfassung sind Smartphones. Sie können so ausgestattet werden, dass sie sich sowohl als RFID-Reader als auch als RFID-Transponder verhalten. Es handelt sich hierbei um eine kostengünstige Lösung, die sowohl für Konsumentenanwendungen, z. B. Bezahlung im öffentlichen Personenverkehr als auch im Rahmen industrieller Anwendungen immer bedeutsamer werden.

Stationäre Lesegeräte

Stationäre Erfassungsgeräte werden fest installiert. Sie ermöglichen die regelmäßige Erfassung beim Passieren eines Objekts. Bei Gate-Lesern sind Antennen an Toren angebracht, durch die z. B. eine Palette transportiert wird, ein Gabelstapler oder auch ein Lastwagen gefahren werden kann. Es kommt hierbei auf eine zuverlässige Erkennung bei größeren Abständen oder unterschiedlichen Positionen der Transponder an. Gate-Reader verwenden in der Regel mehrere Antennen. Ein Antennentor besteht z. B. aus einem Reader und vier Antennen, je zwei an jeder Seite des Tores. Hierdurch ist es möglich, Daten über größere Entfernung und zugleich eine größere Menge an Objekten in kurzer Zeit zu erfassen sowie große Bereiche und eine große Menge an RFID-Etiketten in kürzester

Abb. 5.5 RFID-Gate-Leser

Zeit zu erfassen. Abb. 5.5 zeigt die Nutzung eines Gate-Lesers. Als weitere Ausprägungen von stationären Lesegeräten sind der Tunnelleser für Logistikanwendungen, der Zutrittsleser an Gebäuden für Personen und der Regalleser in Bibliotheken sowie die Diebstahlkontrollen im Einzelhandel zu erwähnen.

5.3.3 Backend-System

Zur Weiterverarbeitung bzw. langfristigen Speicherung werden die erfassten Daten von den Lesegeräten an zentrale Anwendungssysteme des Unternehmens übermittelt. Hierbei kann es sich z. B. um ein ERP-System handeln. Die im Allgemeinen recht wenigen Daten auf dem Transponder (z. B. nur Identifikations-Nummer) können in der Datenbank des Backend-Systems mit weiteren Datenelementen verknüpft werden, beispielsweise mit der Auftragsnummer eines Kunden. Zur näheren Charakterisierung der Weiterverarbeitungsmöglichkeiten mittels RFID erfasster Daten wird zwischen offenen und geschlossenen Systemen unterschieden.

Ein *geschlossenes* System wird innerhalb eines einzelnen Unternehmens genutzt. Als Beispiel lässt sich die Zugangskontrolle zu einem Gebäude mittels RFID-Karten anführen. Hierbei kann das System exakt an die Sicherheitsanforderungen des einzelnen Unternehmens angepasst werden. Geschlossene RFID-Systeme werden auch zwischen mehreren, eng verbundenen Unternehmen eingesetzt. Beispielsweise werden Transponder dauerhaft an Containern oder Behältern angebracht und können von den beteiligten Unter-

nehmen jeweils gelesen und ggfs. neu beschrieben werden. Von Nachteil ist, dass eine geschlossene Lösung auf ein einzelnes Unternehmen oder wenige Unternehmen zugeschnitten ist. Die Entwicklungs-, Einführungs- und Betriebskosten müssen daher von einem oder wenigen Unternehmen getragen werden.

Bei *offenen* Systemen dagegen, wie sie in der Konsumgüterindustrie oder im Handel eingesetzt werden, können die Beteiligten unternehmensübergreifend miteinander kommunizieren. Ein typisches Beispiel ist eine Lieferkette, in der Lieferanten, Hersteller, Logistikdienstleister, Produzenten und Händler Waren und Daten austauschen. Um einen reibungslosen Datenaustausch zwischen Unternehmen zu ermöglichen, müssen branchenübergreifende Standards wie z. B. der Electronic Product Code (EPC) verwendet werden, mit denen die Produkte von unterschiedlichen Unternehmen eindeutig identifiziert werden können. In offenen Systemen profitieren mehrere Akteure von den Vorteilen der Standardisierung, entsprechend lassen sich auch die Kosten aufteilen.

5.3.4 RFID Betriebsfrequenzen

RFID-Systeme empfangen und erzeugen elektromagnetische Wellen. Unter *Betriebsfrequenz* wird die Frequenz, mit der eine Sende-/Empfangseinheit sendet, verstanden. Wie alle Nutzer von Funktechnologie sind Hersteller und Nutzer von RFID Systemen nicht vollständig frei in der Wahl der Betriebsfrequenzen, sondern nutzen allgemein freigegebene Frequenzen (Tab. 5.1).

Im LF-Bereich von 125 bis 135 kHz gelangen preisgünstige passive Transponder zum Einsatz. Der Transponder moduliert seine Antwort auf das angelegte Feld des Readers. Das ist nur im Nahbereich des Readers möglich, wo ein starkes Magnetfeld vorherrscht. Die elektromagnetische Welle hat sich hier noch nicht von der Sendeantenne gelöst, und die Modulation wird vom Reader als Feldstärkeschwankung erkannt. Falls mehrere Transponder nahezu gleichzeitig von einem Reader ausgelesen werden sollen, dürfen die im Transponder gespeicherten Datenmengen nur sehr gering sein. Im Gegensatz zu höheren Frequenzen können Transponder im LF-Bereich wegen dieser Wirkungsweise ohne Probleme in feuchter Umgebung oder auf metallischen Oberflächen verwendet werden.

RFID-Systeme im HF-Frequenzbereich von 13,56 MHz haben eine ähnliche Wirkungsweise wie die Systeme im Niedrigfrequenzbereich. Sie sind beschränkt auf den Nahbereich und induktive Koppelung zwischen Sender und Empfänger. Gleichzeitig sind sie unempfindlich gegen metallische Oberflächen und Feuchtigkeit. Sie zeichnen sich wegen der höheren Frequenz im Vergleich zu LF durch eine bessere Datentransferrate aus. Da der Frequenzbereich um 13,56 MHz als Industry-Scientific-Medical Band (ISM) international einheitlich verfügbar ist, gehören diese Systeme zu den meistgefragten RFID-Anwendungen. Es lassen sich gleichzeitig bis zu 100 Transponder pro Sekunde von einem Lesegerät erfassen. Dieser Vorgang wird auch als *Pulkerfassung* bezeichnet (Schoblick und Schoblick 2005, S. 127). Eingesetzt werden RFID-Systeme im HF-Bereich bei Bibliotheken, bei der Überwachung von Kühlketten, im Handel, im Rahmen von Zeit- und Zu-

trittskontrolle und bei Skiliften. HF-Transponder erlauben kleine, einfache Bauformen bei relativ geringen Kosten eines einzelnen Transponders. Die höhere Frequenz erlaubt es, mit nur wenigen Antennenwindungen auszukommen, die auf Folie gedruckt werden, auf der anschließend der Chip befestigt wird.

Im UHF-Bereich werden für RFID-Anwendungen die beiden Frequenzen 868 MHz in Europa und 915 MHz in den USA genutzt. Der große Vorteil besteht bei UHF-RFID in der hohen Datentransferrate infolge der hohen Bandbreite zur Datenübertragung. Die Lesereichweite beträgt bis zu 4 Metern bei passiven Transpondern und bei aktiven Transpondern darüber hinaus. Die Pulkfähigkeit ist im UHF-Bereich ebenfalls sehr gut. Palettenerfassung und Container-Tracking sind wichtige Anwendungsbereiche bei UHF. Allerdings existieren bei UHF-Anwendungen auch einige Nachteile. Wenn das Label auf einer Metall-Oberfläche angebracht ist, ist der Lesevorgang störanfällig. Auch durch Feuchtigkeit wird die Lesbarkeit beeinträchtigt. Die unterschiedlichen zugelassenen Frequenzen zwischen Europa und USA stellen ein Problem für weltweit operierende Logistikunternehmen dar.

Im Mikrowellenbereich (MW, manchmal auch als Super-High-Frequency, SHF bezeichnet) kann durch die hohe Frequenz ausreichend Energie für eine Lesereichweite von bis zu 15 Metern mit passiven Transpondern realisiert werden, bei aktiven Transpondern sogar darüber hinaus. Es stehen zwei Frequenzen zur Verfügung: 2,4 GHz und 5,8 GHz. Hauptanwendungsgebiete sind Fuhrparksteuerung, Container-Tracking in der Logistik sowie öffentliche Mautsysteme. Dem Vorteil einer sehr hohen Lesegeschwindigkeit stehen auch hier physikalische Nachteile gegenüber, die in den hohen Frequenzen begründet liegen. Feuchtigkeit (Regen, Schnee) kann die Zuverlässigkeit der Erfassung beeinträchtigen. Ferner muss auch die Ausrichtung der Antenne berücksichtigt werden und es existieren keine weltweit verbindlichen Frequenzen.

Die wichtigsten Unterscheidungsmerkmale für RFID-Systeme mit ihren unterschiedlichen Betriebsfrequenzen fasst die nachfolgende Tab. 5.2 zusammen:

5.4 NFC

Bei *Near Field Communication* (NFC) handelt es sich um einen von den Herstellern NXP Semiconductors und Sony im Jahr 2002 entwickelten Standard zur sicheren mobilen Datenübertragung über sehr kurze Distanzen (10 Zentimeter). Der geringe Abstand zwischen den kommunizierenden Geräten erschwert den unbeabsichtigten Austausch sowie das heimliche Auslesen von Daten. Der Datenaustausch in NFC erfolgt durch die induktive Koppelung von Lesegerät und Tag wie bei RFID im HF-Bereich. NFC-Geräte sind kompatibel mit RFID Tags im 13,56 MHz Band.

Es gibt drei Modi von NFC. Ein NFC-Gerät kann in einem oder mehreren dieser Modi arbeiten:

- NFC Kartenemulation. Das NFC-fähige Gerät emuliert eine Smartcard und erlaubt dem Nutzer Aktionen wie mobiles Bezahlen.

Tab. 5.2 Betriebsfrequenzen und Ausprägungen von RFID-Systemen (Bundesamt für Sicherheit in der Informationstechnik 2005, S. 25 f.)

| Kriterien | Niedrigfrequenz (LF) | Hochfrequenz (HF) | Ultrahochfrequenz (UHF) | Mikrowelle (MW) |
|--|---|------------------------------------|--|--|
| Frequenz | 125–135 kHz | 13,56 MHz | 868 bzw. 915 MHz | 2,4 bzw. 5,8 GHz |
| Wirkungsweise | Induktive Koppelung an den Reader | | | Energie aus dem Feld des Readers oder Batterie; eigene Übertragung |
| Leseabstand | bis 1,2 m | bis 1,2 m | bis 4 m | bis zu 15 m |
| Datentransferrate | niedrig | mittel | hoch | sehr hoch |
| Einfluss Feuchtigkeit Umgebung | kein Einfluss | kein Einfluss | negativer Einfluss | negativer Einfluss |
| Einfluss von Tags auf metallischen Flächen | kaum Einfluss | kaum Einfluss | negativer Einfluss | negativer Einfluss |
| Ausrichtung des Transponders | nicht nötig | nicht nötig | teilweise nötig | immer nötig |
| Weltweit akzeptierte Frequenz | Ja | Ja | Teilweise: 868 MHz EU, 915 MHz USA | teilweise (5,8 GHz nicht in der EU) |
| Typische Transponder-Bautypen | Glasröhrchen, Transponder im Plastikgehäuse, Chipkarten | Smart Label, Industrie-Transponder | Smart Label, Industrie-Transponder | Großformatige Transponder |
| Beispielhafte Anwendungen | Zutrittskontrolle, Tieridentifikation | Wäschereinigung, Ticketing, | Paletten erfassung | Straßenmaut, Containertracking |

- NFC Lese/Schreibmodus (Reader/Writer). Das NFC-fähige Gerät erlaubt dem Nutzer, Daten auf NFC-Tags oder RFID-Tags in Smart Labels zu lesen, und gegebenenfalls solche Tags zu beschreiben.
- NFC Peer-to-Peer Modus erlaubt zwei NFC-fähigen Geräten im Ad-Hoc Modus miteinander in Beziehung zu treten und Daten auszutauschen.

In einer NFC-Beziehung gibt es immer einen Initiator und ein Zielgerät. Der Initiator erzeugt das elektromagnetische Feld, das vom Zielgerät (Transponder) zur Übertragung der Daten durch dosierte Entnahme von Energie moduliert wird. Im *passiven* Modus (Kartenemulation/Lese-Schreib Modus) kann der Transponder die benötigte Energie für die eigene Aktivität aus dem Feld entnehmen. Im *aktiven* Modus (Peer-to-Peer) wechseln sich die Kommunikationspartner in den Rollen als Initiator und Zielgerät ab und erzeugen abwechselnd ihr eigenes Feld.

NFC wird durch ISO 14443 (aktiv/passiv) und ISO 18092 (Peer-to-Peer) standardisiert. Die definierten Protokolle regeln die elektrischen Parameter und Übertragungseigen-

schaften. Die vom Standard spezifizierten Datenraten für den Datenaustausch betragen 106 kbit/s, 212 kbit/s und 424 kbit/s. Elementare Prozeduren wie Aktivierung, Kollisionsvermeidung und die Verwendung von Protokollen der höheren Schichten werden ebenfalls spezifiziert. Auf der Applikationsebene gibt es Standards verschiedener Organisationen, die konkrete Datenstrukturen für spezifische Anwendungen und verbundene Interaktionen definieren. Zu diesen Organisationen gehören

- das NFC-Forum, eine von den Unternehmen NXP (Philips), Sony und Nokia gegründete Organisation mit insgesamt 120 Mitgliedern. Das NFC-Forum ist der Besitzer des NFC-Labels und zertifiziert Applikationen und Geräte nach dem NFC-Standard.
- Die GSM-Association (GSMA); sie hat sich zum Ziel gesetzt, das mobile Bezahlen mit Smartphone und NFC weltweit zum Standard zu machen.
- StoLPan (Store Logistics and Payment with NFC); sie ist eine von der EU-Kommission unterstützte Organisation, die ähnliche Ziele wie die GSMA verfolgt.

NFC-Transponder können sowohl in Chipkarten als auch in Smartphones integriert sein. Die Einsatzmöglichkeiten von NFC sind sehr vielfältig. Die Abb. 5.6 zeigt die vielfältigen NFC-Anwendungsmöglichkeiten im Verlaufe eines Tages.

Die Kompatibilität mit RFID ist ein wichtiges Element von NFC. Da RFID nicht auf Bit-Ebene verschlüsselt wird, definiert auch NFC keine Verschlüsselung auf der Bit-Ebene. Die kommunizierenden Applikationen wenden jedoch auf der Anwendungsebene kryptografische Verfahren an. In der Regel wird allerdings die erforderliche Zustimmung des Nutzers für den Datenaustausch zwischen Geräten bei NFC als gegeben angenommen,

| Bereich | Transport | Fahrzeug | Büro | Shop Restaurant | Unterhaltung | Überall |
|-----------------|---|--|--|--|-------------------------------------|---|
| NFC Smartphone | Ticket Boarding Info von Poster / Kiosk Bus / Taxi bezahlen | Sitzposition Tür öffnen Parkticket | Zutritt Businesscard Log in Smart Printer | Kreditkartenzahlung Gutscheine Bonuspunkte Information teilen | Eintrittskarte Event-Information | Personalisieren Von Apps Nutzungshistorie Ticket Download |
| Serviceanbieter | Massen-transport Werbung | Transport Administration | Sicherheit | Banken Kreditkartenfirmen Geschäfte | Unterhaltung | Beliebig |

Abb. 5.6 Ein Tag mit NFC (Curran et al. 2012)

wenn Initiator und Zielgerät sich in dem für den Datenaustausch benötigten kurzen Abstand von unter 10 cm befinden.

5.5 Optische Erfassung mittels Barcode und Mobile Tagging

Der *Barcode* ist die bekannteste und älteste Methode zur automatischen Erfassung von Daten. Mittels geeigneter Lesegeräte erfolgt ein automatisches Lesen („Scannen“) von Bar- oder Strichcodes (engl. bar = Strich). Hierbei werden die Daten durch eine festgelegte Abfolge von Strichen und Trennlücken (1-D-Code) oder dunklen Feldern (2-D-Code) codiert (Abb. 5.7).

Es handelt sich um ein *optisches Leseverfahren*. Der Scanner sendet einen Lichtimpuls und wertet das reflektierte Licht aus. Der eindimensionale Strichcode codiert zumeist nur eine Identifikationsnummer. Zweidimensionale Barcodes können zusätzliche Daten enthalten. Der am häufigsten verwendete Barcode zur Identifikation von Artikeln im Handel ist die Global Trade Item Number (GTIN), früher als EAN-Code (European Article Number) bezeichnet. Falls mehr als nur die Identifikationsnummer codiert werden soll, eignet sich der Quick-Response (QR-Code, Matrixcode) besser, weil durch die zweidimensionale Darstellung mehr Daten auf gleicher Fläche codiert werden können.

Bei *Mobile Tagging* übernehmen Smartphones das Scannen. Es sind keine spezialisierten Erfassungsgeräte mehr erforderlich. Der Barcode (zumeist QR-Code) wird optisch mit Hilfe der Kamera des mobilen Endgerätes fotografiert, dekodiert und verarbeitet. Hierdurch erfolgt ein direkter Zugang z. B. zu einer responsiven Webseite (Abb. 5.8). Auf der Webseite können weiterführende Produktinformationen zur Verfügung gestellt oder

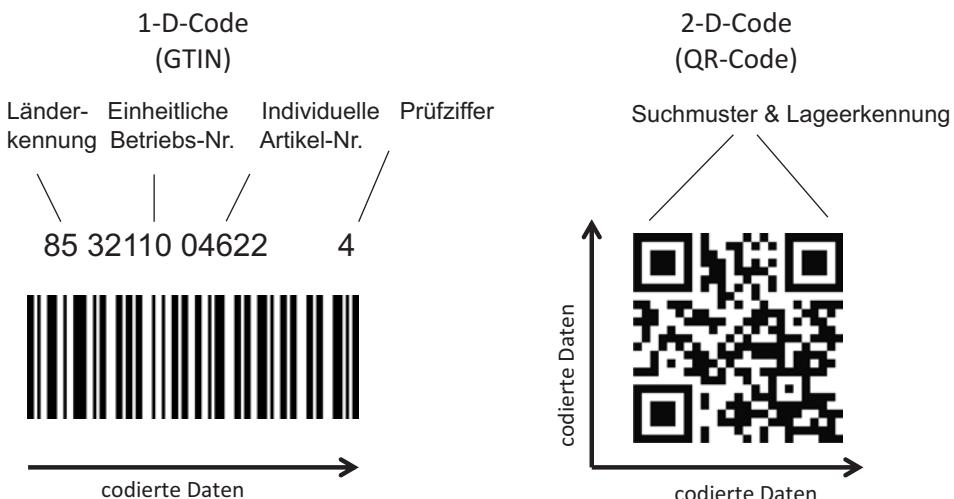


Abb. 5.7 Vergleich zwischen Strich- und Matrixcode

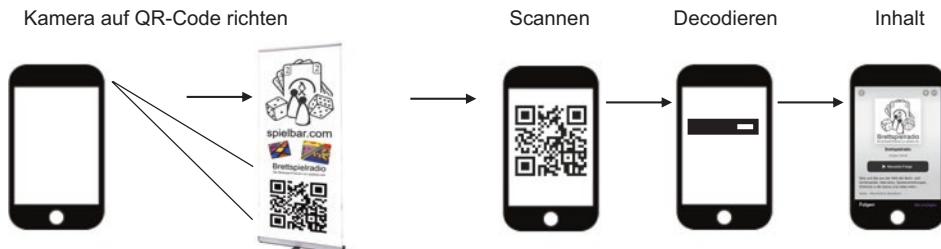


Abb. 5.8 Mobile Tagging

weiterführende Aktionen auf dem Mobilfunkgerät, wie beispielsweise ein Adressbucheintrag, ausgelöst werden. Nutzer müssen hierbei die URL-Adresse nicht mehr gesondert eintippen. Barcodes für mobiles Tagging finden sich auf Produktverpackungen, in Zeitungsanzeigen oder bei der Außenwerbung.

Barcodes „konkurrieren“ mit Smart Labels auf Basis von RFID. Im Gegensatz zu RFID muss bei Barcodes eine Sichtverbindung zwischen Lesegerät und Code bestehen. Auch müssen hinreichende Lichtverhältnisse herrschen. Das Fälschen von QR-Codes ist einfacher zu bewerkstelligen, wodurch Nutzer leicht auf gefälschte Webseiten gelenkt werden können.

5.6 Bluetooth

Die drahtlose Übertragungstechnik Bluetooth für Sprache und Daten im Nahbereich wurde ursprünglich vom schwedischen Mobilfunkunternehmen Ericsson entwickelt. Ziel dieser seit Mitte der 1990er-Jahre geschaffenen und später international standardisierten Funktechnologie war es, kurze Kabelverbindungen zwischen mobilen (z. B. Laptops) und stationären Endgeräten (z. B. Druckern) zu ersetzen.

5.6.1 Bluetooth „Classic“

Der aus Skandinavien stammende Name Bluetooth erinnert an den Wikingerkönig Harald Gormson Blåtand (Blauzahn), der von 910–987 n.Chr. lebte und Dänemark und Norwegen miteinander versöhnte. Der Bluetooth-Standard ist inzwischen eine weit verbreitete Funktechnik, die in nahezu allen Smartphones sowie Tablets und Notebooks integriert ist. Bluetooth wird von der Bluetooth Special Interest Group (SIG) weiterentwickelt, die Inhaber der Bluetooth-Marke und Herausgeber der Spezifikationen ist. In der Bluetooth SIG sind mehr als 30.000 Unternehmen zusammengeschlossen, die an der Weiterentwicklung und kommerziellen Nutzung interessiert sind. Das Institute of Electrical and Electronics Engineers (IEEE) hat den Bluetooth-Standard unter der Nummer 802.15.1 aufgenommen.

Bluetooth nutzt Mikrowellen im 2,4 GHz ISM-Band. Zur Vermeidung von Störungen durch Funkverbindungen auf dem ISM-Band und andere elektrische Geräte verwendet Bluetooth adaptives Frequency-Hopping (FHSS). Der Bluetooth Standard definiert dazu 79 Kanäle im 1 MHz Abstand, die das gesamte Band überdecken. Die Übertragung wechselt 1600-mal in der Sekunde den Kanal, und vermeidet so dauerhafte Kollisionen mit WLAN und anderen Störquellen. Die maximale Datenübertragungsrate war zunächst maximal 706 kbit/s. In der aktuellen Version Bluetooth 5.0 sind Werte von 1 Mbit/s, 2 Mbit/s und 3 Mbit/s vorgesehen.

Bluetooth-Geräte können mit bis zu 7 weiteren Geräten zu einem Piconetz (bedeutet „kleines Netzwerk“) verbunden sein. Eine Punkt-zu-Punkt Verbindung gilt dabei ebenfalls als ein Piconetz. Der Initiator eines Piconetzes sendet Verbindungsanfragen aus, die von den zu einer Verbindung bereiten Geräten in der Nähe empfangen werden können. Durch unterschiedliche Rhythmen, mit denen die Kanäle im Downlink und Uplink gewechselt werden, kommt es innerhalb von 10 s zu einer Übereinstimmung. Die Antwort erfolgt dann mit einer ID-Message und setzt den Antwortenden automatisch in den Slave-Modus. Der Master legt die Frequency-Hopping Sequenz für das Piconetz fest. Im Laufe einer Verbindung scannt der Master laufend die Kanäle und passt im Falle von Störungen die Hopping-Sequenz an.

Slaves in einem Bluetooth Piconetz können gleichzeitig Master eines weiteren Bluetooth Piconetzes sein. Die Beziehung zwischen Frequency Hopping Sequenz und MAC Adresse stellt sicher, dass die Frequency Hopping Sequenzen verschieden sind. Durch wiederholtes Anwenden von Master-Slave Beziehungen können Verkettungen von Bluetooth Piconetzen gebildet werden, über die Daten auch über größere Strecken transportiert werden kann. Es wird bei dieser Betriebsart von einem Scatternetz gesprochen.

Bevor tatsächlich Anwendungsdaten in einem Piconetz ausgetauscht werden können, sind auf den höheren Protokollsichten zunächst die beidseitig unterstützten Applikationsprofile festzulegen. Ein Applikationsprofil legt eine Reihe von Aktionen fest, die zwischen den kommunizierenden Partnern ausgetauscht werden. Für jede Aktion werden die auszutauschenden Nachrichten, ihre Formate und die Wertebereiche der ausgetauschten Daten definiert. In der Maschine-zu-Maschine Kommunikation sind solche Profile der übliche Weg, eine effektive Zusammenarbeit über die Kommunikationsschnittstelle zu erreichen. Bei Schnittstellen für den allgemeinen Gebrauch ist die Definition der Applikationsprofile eine Aufgabe der Standardisierung. Häufig werden Basisaktionen, wie sichere Verbindungsaufnahme mit Austausch von Kennungen (PIN) und das Senden und Empfangen von Daten in einem allgemeinen sogenannten General Access Profile (GAP) zusammengefasst. Das GAP umfasst auch ein Protokoll zur Vereinbarung der Nutzung weiterer spezialisierter Profile. Neben dem generischen GAP werden die folgenden Applikationsprofile häufig genutzt:

- A2DP: Advanced Audio Distribution Profile für Audiodaten in hoher Qualität
- BIP: Basic Imaging Profile zur Übertragung von Bilddateien
- HFP: Handsfree Profile für Freisprechanlagen

- HID: Human Interface Device Profile für den Anschluss von drahtlosen Tastaturen oder Mäusen an Laptops
- OBEX: Object Exchange Profile für generischen Datenaustausch. Dabei werden Dateien als abstrakte Objekte unabhängig von ihrer Beschaffenheit, Struktur oder Inhalt ausgetauscht.

Bluetooth kann Musik und Sprache in hoher Qualität übertragen. Dies wird genutzt, um Lautsprecher drahtlos an Musikquellen anzuschließen. Auch drahtlose Kopfhörer werden vorwiegend über Bluetooth mit mobilen Endgeräten verbunden. Die erforderlichen Hardware-Komponenten können ohne Probleme in kleine Geräte, wie z. B. Ohrhörer, eingebaut werden. Der Stromverbrauch ist gering; hierdurch können lange Betriebszeiten bei batteriebetriebenen Kleingeräten erreicht werden.

Bluetooth GAP enthält als Sicherheitsfeature einen Pairing-Prozess, bei dem festgelegte Kennungen (PIN) an den beteiligten Endgeräten eingeben und ausgetauscht werden. Verfügen die Mobiltelefone über NFC, kann der Austausch von PIN-Kennungen durch eine NFC-Koppelung ersetzt werden. Die zu verbindenden Geräte werden in NFC-Entfernung gehalten und tauschen über die NFC-Schnittstelle die zur Aufnahme einer Bluetooth-Verbindung benötigten Sicherheitsdaten aus. Die benötigte Zeit für Verbindungsaufnahme und Pairing kann so deutlich verkürzt werden.

Bluetooth-Geräte werden in Klassen entsprechend ihrer Übertragungsenergie und Reichweite eingeteilt. Tab. 5.3 zeigt die Klassen und ihre Parameter. Die Klassen 2 und 3 beziehen sich auf Bluetooth Low Energy Geräte (Abschn. 5.6.2).

5.6.2 Bluetooth Low Energy

Bluetooth Low Energy (BLE) wurde 2006 vom Mobilfunk-Hersteller Nokia zunächst unter dem Namen Wibree entwickelt. BLE wurde 2009 von der Bluetooth Special Interest Group (SIG) übernommen und vom IEEE in den Standard 802.15.1 integriert. Neben Bluetooth Low Energy ist auch die Bezeichnung Bluetooth Smart® gebräuchlich. Anders als der Name suggeriert ist Bluetooth Low Energy ein eigenständiger Funkstandard und

Tab. 5.3 Bluetooth Klassen, Sende-Energien und Reichweiten

| Klasse | Maximale Sendeleistung und Reichweite | |
|------------|---------------------------------------|-----|
| | (mW) | (m) |
| Klasse 1 | 100 | 200 |
| Klasse 1,5 | 10 | 100 |
| Klasse 2 | 2,5 | 10 |
| Klasse 3 | 1 | 1 |

nicht kompatibel mit Bluetooth. Allerdings unterstützen viele Chips und Endgeräte sowohl Bluetooth als auch BLE.

BLE ist ein Standard für Geräte mit sehr niedrigem Stromverbrauch für die Maschine-zu-Maschine-Kommunikation auf kurzen Distanzen. Es eignet sich vor allem für leistungsschwache Geräte (einfache Sensoren und Sender) und zielt auf geringen Stromverbrauch, einfachen Verbindungsaufbau und geringes Datentransfervolumen. Die gesamte Leistungsaufnahme eines BLE Chips liegt je nach Datenrate und Entfernung zwischen 1 % und 50 % der Werte von „klassischem“ Bluetooth. Der niedrige Energieverbrauch wird nicht durch verminderte Übertragungsleistung, sondern vor allem durch eine beschleunigte Verbindungsaufnahme und abgekürzte Prozeduren erreicht. Die Leistungsklassen aus Tab. 5.3 gelten auch für Bluetooth Low Energy. Mit einer einfachen Knopfzellen-Batterie von 1000 mAh sind bis zu 2 Jahren Betriebszeit möglich.

Bluetooth Low Energy kennt in Ergänzung zur Bluetooth Master/Slave Rollenverteilung verschiedene Rollen von Geräten, die enger gefasst sind als bei Bluetooth:

- Observer: Ein Observer ist ein Gerät, das ausschließlich Daten empfängt. Ein Beispiel ist eine Sport-Uhr, die von peripheren Sensoren Daten wie Geschwindigkeit oder Schrittzahl erhält.
- Broadcaster: Ein Broadcaster ist ein Gerät, das ausschließlich Daten sendet. Es wird keine Verbindung aufgebaut. Die Beacons im iBeacon-System (Abschn. 5.6.3) sind Broadcaster.
- Periphere Geräte sind ausschließlich Slaves. Sie senden Verbindungsanfragen aus.
- Zentrale Geräte agieren nur als Master (Server) und senden keine Verbindungsanfragen aus. Dabei kann ein PC oder Mobiltelefon Master oder Slave sein.

BLE verwendet 40 Kanäle mit 2 MHz Abstand. Davon sind 37 Kanäle für Datenübertragung vorgesehen. Dabei wird Frequency Hopping zur Vermeidung von Störungen verwendet. Auf drei Kanälen sendet ein peripherer BLE Chip nach Aktivierung Verbindungsanfragen aus. Verbindungsbereite Observer scannen nur diese Frequenzen. Das Verfahren ist schneller und stromsparender als die Verbindungsaufnahme bei Bluetooth. BLE nutzt eine Master-Slave-Architektur, die bei der Verbindungsaufnahme bereits festgelegt wird. Der Master kann im Gegensatz zu Bluetooth Classic mit bis zu 128 Slaves verbunden sein. Allerdings ist es Slaves nicht möglich, gleichzeitig Master eines weiteren Netzes zu sein. Eine Kaskadierung von Piconetzen ist also nicht vorgesehen. Periphere Geräte führen im Slave-Modus lediglich ein Minimum von Funktionen aus, und ermöglichen so extrem niedrigen Energieverbrauch und lange Laufzeiten bei Batteriebetrieb. Zentrale Geräte führen als Master alle Koordinationsaufgaben aus. Die für die Herstellung einer Verbindung benötigte Zeit wurde durch ein vereinfachtes Verfahren auf Millisekunden verkürzt. BLE erlaubt eine Übertragungsrate von 1 Mbit/s. Es werden nur sehr kurze Pakete verwendet, die sich nicht für Übertragung von Audio-, Video- oder Bilddateien eignen. Damit ist BLE ein reiner Maschine-zu-Maschine Standard. Die Reichweite in Innenräumen ist 10 m, und

Abb. 5.9 Geschwindigkeitssensor am Rennrad mit BLE-Technologie



zur Abdeckung eines Büros oder Geschäftsraumes von 1000 m² werden 5 BLE Master benötigt.

Ein Beispiel für die Anwendung von Bluetooth Low Energy ist die Übertragung von geringen Datenmengen, die von Sensoren erzeugt werden. Abb. 5.9 zeigt einen an der Kettenstange eines Rennrads angebrachten Geschwindigkeitssensor der Marke Polar. Mit einer fest eingebauten Knopfzelle arbeitet er bis zu 5 Jahre. Dabei wird die Energie der Batterie nur für den Verbindungsaufbau und Protokollaktionen genutzt. Die Energie für die bei jeder Radumdrehung übertragenen Daten, die im Wesentlichen aus Protokollelementen bestehen, wird durch Induktion von einem an einer Speiche montierten Magneten (in der Bildmitte oben) beim Passieren des Sensors bei jeder Radumdrehung erzeugt. Die Übertragung erfolgt an einen Fahrradcomputer am Lenker, an eine Smartwatch oder das Smartphone des Fahrers.

5.6.3 iBeacon

Basierend auf BLE führte Apple Inc. im Jahr 2013 den proprietären Standard und das damit verbundene System iBeacon zur Navigation in geschlossenen Räumen ein. iBeacon funktioniert nach dem Sender-Empfänger-Prinzip. Hierbei sind kleine Sender im Raum verteilt, die in vorher eingestellten Intervallen Signale in ihre unmittelbare Umgebung ausstrahlen. Insofern ist der Name treffend gewählt, denn das englische „beacon“ bedeutet

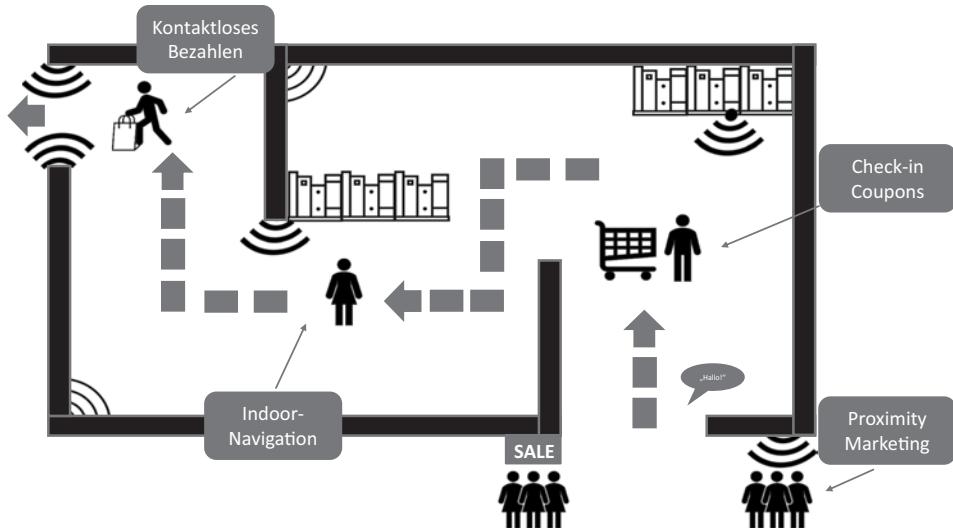


Abb. 5.10 Anwendungsszenarien von iBeacons im stationären Handel

übersetzt „Leuchtfeuer“. Die Signale können von einem Smartphone empfangen werden und an eine entsprechende Software weitergeleitet werden. Hierdurch ist es möglich, auf dem mobilen Endgerät standortbezogene Informationen anzuzeigen, zu erkennen, wann ein Kunde ein Ladenlokal betritt und wieder verlässt oder wo und wie lange er sich im Laden aufhält. Mehrere Beacons in einem Ladenlokal ermöglichen es, die Position des Empfängers im Raum relativ genau zu bestimmen und hierdurch standortgenaue Informationen oder Produktangebote zu geben (Abb. 5.10).

iBeacon ist auch für Privatpersonen für den Bereich Heim-Automation erhältlich. Hier können im Raum verteilte iBeacons in Abhängigkeit von der Anwesenheit von Personen in einem Teil der Wohnung Aktionen auslösen, wie z. B. Regulierung von Beleuchtung oder Heizung.

5.7 Zigbee

Zigbee ist ein von der Connectivity Standards Alliance (csa-iot.org, ehemals Zigbee Alliance) entwickeltes Protokoll, das digitale Personal Area Networks für Maschine-zu-Maschine Kommunikation definiert. Die Lösungen umfassen auch Anwendungen von Bluetooth und WLAN für Maschine-zu-Maschine Kommunikation. Der Name Zigbee leitet sich vom Schwänzeltanz der Bienen bei der Rückkehr von der Futtersuche ab. Die Struktur der Weiterleitung erinnerte die Entwickler entfernt an die Tanzfiguren der Bienen. Die Anwendungsbereiche liegen im Bereich Heim-Automation, Vernetzung medizinischer Geräte und anderer Projekte mit kleinen Datenraten und kurzer Reichweite. Eine Reihe von führenden Herstellern, die sowohl aus der Mikroelektronik und Kommunikations-

technik als auch von der Anwenderseite kommen, sind an der Connectivity Standards Alliance beteiligt. Im Smart Home Bereich wird Zigbee von zahlreichen Unternehmen der Beleuchtungstechnik oder der Sicherheitstechnik (z. B. vernetzte Rauchmelder) unterstützt. Zigbee wird präferiert wegen des niedrigen Energiebedarfs, den geringen Gerätekosten und der einfachen Handhabung für den Anwender durch selbtkonfigurierende Vernetzung. Die Reichweite einer direkten Zigbee Verbindung ist in der Praxis im Innenbereich auf 10 m beschränkt. Viele Zigbee-Geräte arbeiten als Router und leiten empfangene Nachrichten an angeschlossene Geräte weiter. Jedes zusätzliche Gerät erweitert so automatisch die Reichweite und verstärkt zusätzlich die Widerstandsfähigkeit (Resilienz) des Netzes gegen den Ausfall von Knoten. Ein Zigbee-Netz kann bis zu 65.000 Netzknoten umfassen und so größere Entfernung von mehr als 100 m überspannen. Damit ist es auch für Steuerungsaufgaben im industriellen und öffentlichen Umfeld einsetzbar. Beispielsweise wurden in der englischen Stadt Hampshire 90.000 Straßenlaternen mit Zigbee vernetzt (Zigbee 2019).

Der aktuelle Standard trägt die Nummer 3,0 und wird als Zigbee PRO 2015 bezeichnet. Hiermit wurden zahlreiche Herstellerprofile in einem Standard zusammengefasst. Das betrifft vor allem die Themen Beleuchtungssteuerung, Heim- und Gebäudeautomation, Handel, Gesundheit, Telekommunikation und Energieeffizienz.

Es gibt vier Klassen von Zigbee-Geräten:

Zigbee Koordinator (ZC) Für ein sternförmiges Netzwerk dient der ZC als zentraler Knoten. Alle peripheren Knoten verbinden sich mit ihm. Im Falle eines verteilten (Mesh) Netzwerks ist der ZC der Netzwerk-Master und derjenige Knoten, der das Netz gestartet hat. Er besitzt die Information über das gesamte Netz. Ein Zigbee Koordinator ist in der Regel in einem separaten Gehäuse mit externem Netzanschluss realisiert.

Zigbee Router (ZR) Ein ZR hat zwei Funktionen. Auf ihm kann eine Applikation ablaufen; zusätzlich kann er aber auch als intermediärer Knoten Daten weiterleiten. Router reagieren auf den Ausfall von Verbindungen mit einem Discovery Prozess, bei dem alternative Routen zu einem Zielknoten ermittelt werden. Dieser Prozess sorgt für die Ausfallsicherheit eines Zigbee-Netzes. Die meisten Zigbee-Endgeräte mit Anschluss an die Stromversorgung sind gleichzeitig Zigbee Router.

Zigbee End Device (ZED) Ein ZED besitzt gerade genug Funktionalität, um sich mit einem ZC oder ZR zu verbinden. ZED sind oft für Batteriebetrieb vorgesehen. ZED sind die meiste Zeit im Ruhemodus und können lange Batterielaufzeiten erzielen. Sie sind preisgünstig herzustellen. Während ZC und ZR sogenannte Fully Functioning Devices (FFD) nach IEEE 802.15.4 sind, ist ein ZED oftmals nur ein Gerät mit eingeschränkter Funktion, welches nur mit einem Router kommunizieren kann.

Green Power Device (GPD) ist ein neu eingeführter Typ von Endgerät. GPDs sind Geräte ohne Batterie, die zum Beispiel Energie induktiv aus mechanischen Aktionen (Bettigung eines Schalters) gewinnen, oder eine fest eingebaute Batterie als „lebenslange“ Energiequelle ohne Austauschmöglichkeit besitzen. GPDs arbeiten im Netz mit einem gesonderten Protokoll.

Abb. 5.11 zeigt ein Zigbee Netzwerk mit den verschiedenen Geräterollen. Der Zigbee-Standard unterstützt auch verschiedene Netztopologien.

- In der Sterntopologie ist jedes Gerät (ZR oder ZED) direkt mit dem ZC verbunden
- Die Baumtopologie erlaubt eine weitere Verzweigung der Verbindung, jedoch keine Rundwege im Netz

Die Mesh-Topologie ist ein vermaschtes Peer-to-Peer System. Hier ist jedes Gerät als Router beteiligt. In der Mesh-Topologie werden bei Ausfall einer Verbindung automatisch alternative Routen gefunden. Die Mesh-Topologie geht über die Funktionalität des 802.15.4-Standards hinaus und wird durch den Zigbee Standard auf OSI-Schicht 3 (Netzwerk) implementiert. (vgl. Abb. 5.12.)

Ähnlich wie Bluetooth verwendet Zigbee anwendungsspezifische Profile, um den Nachrichtenaustausch für Anwendungsklassen zu standardisieren. Beispiele für Profile sind

- Home Automation: Hier sind Schnittstellen im Bereich Beleuchtung, Verdunkelung, Heizung, Überwachung und Alarmierung modelliert. Zusätzlich gibt es noch die allgemeine Schnittstelle zum Ein- und Ausschalten sowie Öffnen und Schließen.
- Personal Home and Hospital Care zur Übertragung von Messwerten und Steuerung von medizinischem Gerät
- Advanced Metering Initiative mit der Festlegung von Schnittstellen zu Erfassung und Übertragung von Verbrauchswerten etwa von Strom oder Wasser und der zeitgesteuerten Anlagenbeeinflussung.

Zahlreiche weitere Profile sind von der Connectivity Standards Alliance veröffentlicht worden. Zusätzlich gibt es noch herstellerspezifische Profile, die selbst in Teilen veröffentlicht sind. Damit können zum Beispiel mit dem eigenen Gateway eines Leuchtmittelherstellers raffinierte Effekte mit der Farbtemperatur (warmes oder weißes Licht) und Helligkeit erreicht werden; mit dem allgemeinen veröffentlichten Teil des Profils kann ein Gateway eines anderen Produzenten immerhin noch zeitgesteuerte Schaltvorgänge ausführen.

Der aktuelle Standard Zigbee PRO 2015 beruht auf der Funktechnologie IEEE 802.15.4-2011, die das ISM-Band 2,4 GHz nutzt. Entsprechend der Allgemeinzuteilung dieses Bandes ist die Sendeenergie beschränkt auf 100 mW; tatsächlich werden in der Regel maximal 20 mW verwendet. Einzelne Geräte (ZED) sind auch auf 1 mW begrenzt.

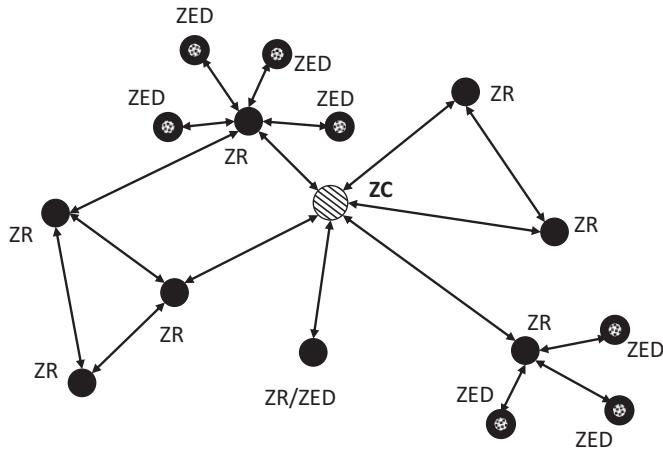


Abb. 5.11 Zigbee-Netz

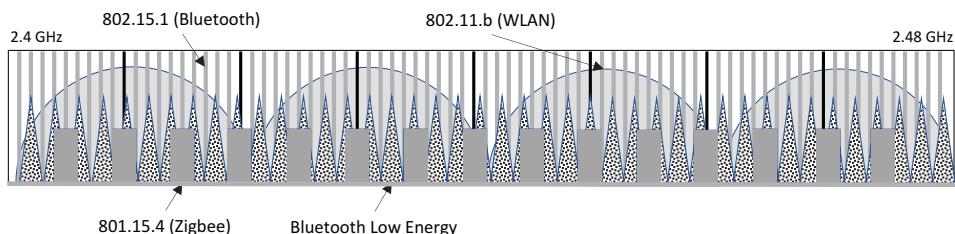


Abb. 5.12 Intensive Nutzung des 2,4 GHz ISM Bandes durch verschiedene Technologien

IEEE 802.15.4 definiert 16 Kanäle von je 2 MHz Bandbreite und mit 5 MHz Abstand im 2,4 GHz ISM Band. Die Kommunikation des Netzes erfolgt auf einem dieser Kanäle, der vom Koordinator beim Start ausgewählt wird. Diese Kanäle sind verschieden von den WLAN- und den Bluetooth-Kanälen im gleichen Frequenzband. Die Kommunikation erfolgt mittels eines modifizierten QPSK-Verfahrens (Offset-QPSK). Dabei wird zur Reduktion des Energiebedarfs beim Sender eine Verschiebung von 1 Bit zwischen den Koordinaten I und Q (Abschn. 3.3.1) eingeführt. Ähnlich wie beim SC-FDMA bei LTE vermeidet dies große Sprünge beim Wechsel von Symbol zu Symbol. Die modulierten Symbole werden durch ein CDMA-Verfahren auf die 2 MHz Bandbreite gespreizt. Zur Kollisionsvermeidung beim Netzzugriff wird CSMA/CA (Abschn. 3.3.3) verwendet. Die maximale Datenrate auf einem Zigbee-Link beträgt 250 kBit/s.

Es besteht eine Kontroverse über die Verträglichkeit der drei Technologien auf dem 2,4 GHz Frequenzband (Abb. 5.12, (Gerstner 2010, Connectivity Standards Alliance 2019)). Während Vertreter der Bluetooth SIG die Verträglichkeit zwischen Bluetooth und Zigbee kritisch sehen, präsentiert die Connectivity Standards Alliance Tests und Mess-

ergebnisse, die eine problemlose Koexistenz beider Technologien nachweisen sollen (Connectivity Standards Alliance 2019).

Beim Start des Netzes wählt der Koordinator neben dem freien Kanal eine 16-Bit Kennung für das Netz aus. Der Koordinator sendet Broadcast-Anfragen, um Endgeräte und Router zu finden. Router und Endgeräte scannen nach dem Anschalten den Frequenzbereich, um ein Netz zu finden, mit dem sie sich verbinden. Die Adressierung der Geräte im Netz wird hierarchisch vorgenommen; auch hier wird ein 16-Bit Adressraum verwendet. Der ZC weist jedem angeschlossenen ZR einen Adressraum zu, den dieser dann für die bei ihm angeschlossenen ZR oder ZED weiter unterteilen kann. Theoretisch ermöglichen die 16 Bit-Adressen also ca. 65.000 verbundene Geräte; die realistische Zahl möglicher Netzketten ist wegen der hierarchischen Adressierung allerdings viel geringer.

Die Kommunikation zwischen ZC und den Netzketten ist meist asynchron. Für die Richtung zum ZC ist der zentrale Knoten immer empfangsbereit; die peripheren Knoten können übertragen, sobald sie Daten zu senden haben. Zur Kollisionsvermeidung beim Netzzugriff wird eine Modifikation von CSMA/CA (Abschn. 3.3.3) verwendet. Dabei wartet jedes Gerät bei einem frei erkannten Kanal eine zufällige Periode, bevor es mit der Sendung beginnt. Der ZC sendet unmittelbar nach Empfang eine Bestätigung; bleibt diese aus, zeigt es für den Sender den Fehlschlag der Übertragung an. Da Zigbee-Pakete sehr kurz sind (maximal 127 Bytes), erzeugt dieses kollisionsbehaftete Verfahren keine signifikanten Overheads. In der Richtung zu den peripheren Geräten sendet der ZC nur, wenn eine Anfrage vorliegt. Die peripheren Geräte sind die größte Zeit im Sleep-Modus und senden regelmäßig Anfragen, ob Daten für sie vorliegen. Nach dem Absetzen der Anfrage sind sie eine kurze Periode empfangsbereit. Durch dieses Verfahren ist ein sehr energie-sparender Betrieb möglich.

5.8 WLAN

Bei einem Wireless Local Area Network (WLAN) handelt es sich um ein lokales Funknetzwerk. Es dient vor allem dazu, mobile Endgeräte untereinander oder mit dem Internet zu verbinden. Eine andere Bezeichnung für die verwendete Technologie ist WiFi (Wireless Fidelity) in Anlehnung an den Begriff HiFi aus der Elektroakustik.

5.8.1 WLAN Übersicht

WLAN-Verbindungen verfügen innerhalb von Gebäuden über eine Reichweite von ca. 30 m und außerhalb von bis zu 300 m. Die Reichweiten hängen stark ab von den Umgebungsbedingungen, wie beispielsweise Stärke und Material von Wänden zwischen Sender und Empfänger. Die WLAN-Technologie hat sich innerhalb weniger Jahre weltweit verbreitet.

WLAN ist eine standardisierte Technologie, die vom IEEE als Local Area Network Standard in der Serie 802.11 entwickelt wurde und laufend erweitert wird. Seit Beginn der 1980er-Jahre entstanden zahlreiche LAN-Systeme, die hinsichtlich Verkabelung, Übertragungstechnik und Zugangsverfahren eine Standardisierung notwendig machten.

Die WiFi Alliance, ein Zusammenschluss von WLAN-Herstellern, prüft und zertifiziert die Interoperabilität von WLAN-Geräten nach dem 802.11 Standard. Abb. 5.13 zeigt die wichtigsten der mehr als 20 heute existierenden WLAN-Standards und die von der WiFi Alliance im Marketing verwendeten Begriffe.

Mit der Aufspaltung in die beiden Standards 802.11a und 802.11b Ende der 1990er-Jahre wollte die IEEE zwischen Privatanwendern im 2,4 GHz-Band und professionellen Anwendern im 5 GHz-Bereich differenzieren. Die für 5 GHz vorgeschriebenen Techniken Dynamical Frequency Selection (DFS) und Power Control (TPC) (Abschn. 5.2) verteuerten die 5 GHz-Ausrüstung. Das 5 GHz-Band wurde deshalb von Privatanwendern weniger genutzt. Die Entwicklung führte dann aber letztlich zu Systemen und Geräten, die beide Frequenzbereiche separat oder gemeinsam nutzen können. Zentrale Standards, die bis heute den Markt dominieren, sind 802.11n (WiFi4) und 802.11ac (WiFi5). Unter der Bezeichnung WiFi6 wurde eine Weiterentwicklung des 802.11ac zu 802.11ax veröffentlicht. Es wird erwartet, dass bis Mitte der 2020er-Jahre – wie bei den öffentlichen Mobilfunknetzen – eine Knappheit bei der verfügbaren WLAN-Kapazität eintreten wird. Die IEEE und WiFi Alliance haben daher bereits die Erschließung von WLAN-Frequenzen im Bereich von 5,9 GHz bis 7,1 GHz vorgeschlagen. Dies würde 14 parallele Kanäle von 80 MHz oder 7 parallele Kanäle von 160 MHz zur Verfügung stellen. Der Frequenzbereich wird nicht von Radarsystemen genutzt, was die Implementierung von aufwändigen DFS-Verfahren unnötig macht. Die entsprechende Initiative wird unter dem Namen WiFi6E geführt. Die US-amerikanische Regulierungsbehörde FCC hat bereits 2020 den

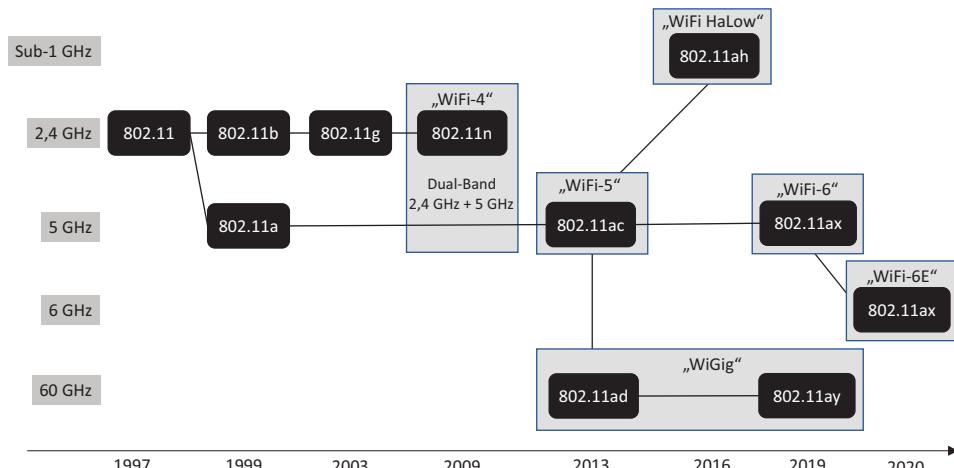


Abb. 5.13 Übersicht der WLAN Standards

gesamten vorgeschlagenen Bereich freigegeben. Seit 2021 gibt es auch in der EU eine Freigabe für den Teilbereich von 5,945 GHz bis 6,425 GHz entsprechend 6 Kanälen zu je 80 MHz.

Aus 802.11.ac wurden weitere Standards abgeleitet. Unter der Bezeichnung „WiGig“ veröffentlichte die IEEE den Standard IEEE 802.11ad, der Kommunikationslösungen im 60 GHz-Frequenzbereich definiert. Mit vier Kanälen von je 2,16 GHz bietet er extrem hohe Bitraten, ist allerdings mit einer Reichweite von wenigen Metern und sehr schwacher Durchdringung von Wänden nur innerhalb eines Raumes nutzbar. Im Bereich der drahtlosen Gerätevernetzungen könnte sich hier eine Alternative zu Bluetooth entwickeln. IEEE 802.11ay ist eine kürzlich eine unter dem Label WiFi6 veröffentlichte Weiterentwicklung, die neben weiteren Verbesserungen die Bündelung von bis zu vier Kanälen von je 2,16 GHz bietet.

Eine interessante Entwicklung ist der Standard „WiFi HaLow“ (802.11ah). Er adressiert genau wie SigFox (Abschn. 5.8.2) und Bluetooth Low Energy (Abschn. 5.5.2) den schnell wachsenden Markt des Internet of Things, speziell im Bereich des „Smart Home“ und ist im Bereich des UHF-Bandes angesiedelt. Einige Spezifika werden weiter unten besprochen.

Ein WLAN-Netzwerk kann auf verschiedene Art und Weise aufgebaut werden. Bei der ad-hoc-Verbindung „Independent Basic Service Set“ (IBSS) erfolgt ein Datenaustausch zwischen den Netzwerkeinnehmern direkt. Der Vorteil dieser Peer-to-Peer-Variante besteht darin, dass keine Infrastruktur aufgebaut werden muss. Solange sich die Geräte in Reichweite befinden, ist eine Kommunikation unter ihnen möglich. Eine sichere Verschlüsselung ist in diesem Modus nicht möglich. Über Bluetooth lässt sich eine ad-hoc-Verbindung einfacher und sicherer realisieren.

Die typische Betriebsform, das „Basic Service Set“ (BSS), liegt bei einer Funkverbindung von mobilen Endgeräten und einer Sendestation vor (auch als Access Point, WLAN-Router oder im öffentlichen Raum als WiFi-Hotspot bezeichnet), wobei die weitere Kommunikation ab der Sendestation über Kabel erfolgt. Für weit verzweigte Installationen, zum Beispiel in Hotels oder in Bürogebäuden können auch mehrere Access Points zu einem Extended Service Set (ESS) zusammengeschaltet werden. Sie werden dann vom Endgerät als ein weiträumiges WLAN wahrgenommen. Allerdings ist ein BSS kein Mobilennetzwerk. Das Endgerät ist zu jeder Zeit mit höchstens einem Access Point verbunden. Während der Verbindung erfolgt auch kein Wechsel des Access Point. Ein Wireless Distribution System (WDS), auch als WLAN-Repeater bezeichnet, ist die drahtlose Verbindung mehrerer Wireless Access Points untereinander. Hierdurch kann die Reichweite einzelner Basisstationen vergrößert werden. Die verschiedenen Betriebs-Modi werden in Abb. 5.14 verdeutlicht. Ein BSS oder ESS macht sich den potenziellen Nutzern über die regelmäßige Aussendung von sogenannten Beacon-Frames bekannt. Das sind unverschlüsselte Pakete, die den Netzwerknamen (SSID) und wichtige Verbindungsparameter übertragen.

Zur Erhöhung der Datensicherheit eines WLAN kann der Datenaustausch zwischen einem Access Point und den Clients verschlüsselt erfolgen. Als Standard für Authenti-

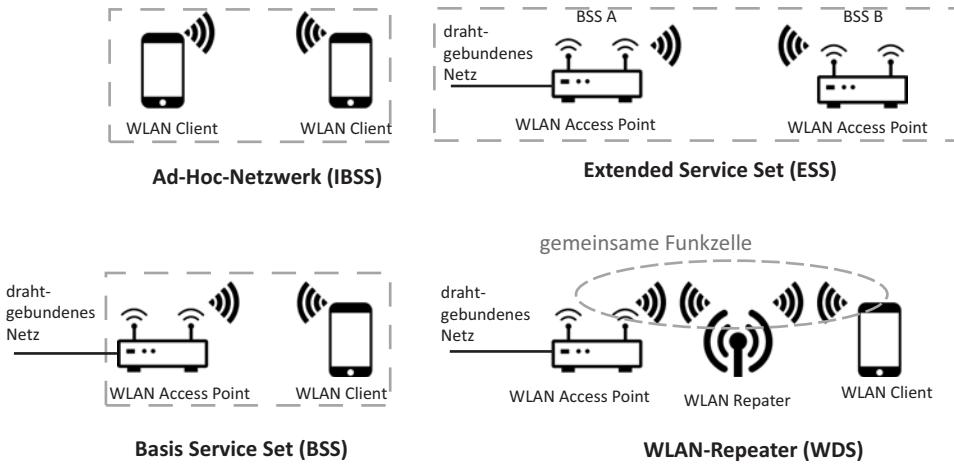


Abb. 5.14 Betriebsarten von WLAN

fizierung und Verschlüsselung dienen die Protokolle in der Serie Wireless Protected Access (WPA). Die Version WPA2 ist derzeit noch in vielen Geräten eingebaut, seit 2018 existiert der verbesserte Sicherheitsstandard WPA3. Als zusätzliches Sicherheitsmerkmal kann die Aussendung der Beacon-Frames unterdrückt werden. Beacon-Frames sind Datenpakete, die in regelmäßigen Abständen von jedem WPA an WLAN-Clients versendet werden und Konfigurations- und Sicherheitsinformationen und die Service Set Identification enthalten. Durch Unterdrückung der Beacon-Frames ist das Netzwerk nur für die Nutzer zugänglich, die den Netzwerk-Namen kennen. Allerdings eröffnet dies einem Angreifer, der selbst den Netzwerknamen kennt, die Möglichkeit, Anmeldungen zu seinem eigenen Gerät umzuleiten.

5.8.2 WLAN Funktechnik

Das historisch erste Frequenzband, das von WLAN genutzt wurde, ist das international als ISM-Band frei nutzbare 2,4 GHz-Band. Innerhalb dieses Frequenzbandes wurde eine Kanalstruktur mit 13 Kanälen von je 20 MHz Breite definiert, die von WLAN-Netzen belegt werden konnten. Dieses Kanalkonzept hat sich durch alle Standards bis heute erhalten. Abb. 5.15 zeigt die Position der Kanäle im 2,4 GHz-Band. Die Kanäle sind lediglich um jeweils 5 MHz gegeneinander verschoben, und damit nicht überlappungsfrei. Der Grund für diese Struktur bestand darin, dass durch Wahl eines verschobenen Kanals unter Umständen Störungen oder ungünstige Funk-Bedingungen vermieden werden konnten. Zwei WLANs können sich überlappende Kanäle ohne gegenseitige Beeinflussung nutzen, wenn sie einen Mindestabstand von 30 m haben. Die Nutzung der vollen Bandbreite des Bandes mit 4 parallelen Kanälen ist nur möglich durch Wahl der dunkel dargestellten Kanäle 1, 5, 9 und 13. Wenn Access Point und Endgeräte Kanalbündelung unterstützen, kön-

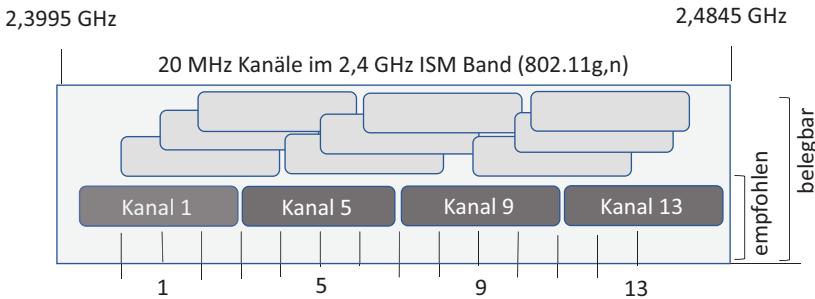


Abb. 5.15 Nutzung überlappungsfreier Frequenzen (dunkelgrau) im 2,4 GHz ISM Band

nen 2 oder sogar 4 Kanäle zu einem 40 MHz oder 80 MHz WLAN zusammengefasst werden. Ein WLAN mit 80 MHz belegt jedoch das gesamte 2,4 GHz-Spektrum und erlaubt keinen Betrieb von weiteren WLANs in der direkten Umgebung.

Im 5 GHz-Bereich steht die vierfache Bandbreite zur Verfügung. Hier können prinzipiell Bänder von 20 MHz, 40 MHz, 80 MHz und 160 MHz für ein einzelnes WLAN genutzt werden. Allerdings gelten dabei Nutzungseinschränkungen, die nicht von jedem Router erfüllt werden. Die Frequenzen von 5170 MHz bis 5250 MHz dürfen mit maximal 200 mW Leistung und ausschließlich in Innenräumen genutzt werden. Bei einer Bandbreite von 80 MHz wird dieser Bereich bereits von einem WLAN komplett belegt. Für die Nutzung des Spektrums von 5250 MHz bis 5350 MHz und des großen Bereiches von 5470 MHz bis 5725 MHz ist die Nutzung der Funktionen Dynamische Frequenzwahl (DFS) und Adaptive Leistungsregelung (TPC) vorgeschrieben. Unter anderem sendet hier das Wetterradar, das als Primärnutzer nicht gestört werden darf. Bemerkt ein Router mit DFS ein fremdes Signal, wird automatisch das Band gewechselt. Mit der Adaptiven Leistungsregelung wird die Sendeenergie kontinuierlich auf dem kleinsten möglichen Niveau gehalten. Da viele Router DFS und TPC im 5 GHz-Bereich nicht unterstützen, ist oft nur der Betrieb in den unteren 80 MHz möglich.

Die WLAN-Funktechnik ist an die Funktechnik der Mobilfunknetze angelehnt. Die Modulation erfolgt je nach Standardversion mittels PSK, QPSK oder den QAM-Verfahren (Abschn. 3.3.1). Für den Netzzugriff wird OFDM angewendet. Allerdings kommen dabei andere Symbolzeiten und Bandbreiten als bei LTE zum Einsatz. Die Symboldauer von 3,2 µs ist um den Faktor 20 kürzer als bei LTE, dafür ist die Breite der OFDM-Bänder mit 312,5 kHz entsprechend größer. In der Bandbreite von 20 MHz werden 48 OFDM-Bänder für den Datentransfer eingesetzt. Dazu gibt es 4 Pilotkanäle, auf denen ein konstantes Bit-Muster ausgesendet wird, sowie ein unbesetztes Band in der Mitte. Insgesamt werden so 16,6 MHz belegt; die übrigen 3,4 MHz dienen als Guard-Band.

Zur Regelung des kollisionsbehafteten Zugriffs der Endgeräte auf das WLAN wird allgemein das Verfahren CSMA/CA (Abschn. 3.3.3) eingesetzt. Mit dem Standard 802.11ac (WiFi5) wird neben CSMA/CA zusätzlich auch erstmals das Multi-User-fähige OFDMA angewendet. Dabei vergibt der zentrale Access Point Sende- und Empfangsberechtigungen

an die Endgeräte auch für Teile des nutzbaren Spektrums. In 802.11ax wird OFDMA zur Standard Accessmethode. Mit OFDMA werden durch die direkte Vergabe von Senderechten an die Endgeräte die Latenzen stark verkürzt, und es entfällt die aufwändige Kollisionsvermeidung. Auch können große Bandbreiten wie 160 MHz effektiver verwaltet werden, da mehrere Endgeräte zur selben Zeit senden können.

Die Angaben zu den in einem WLAN erzielbaren Brutto-Datenraten sind abhängig von der Bandbreite des verwendeten Kanals. Für einen 160 MHz-Kanal sind unter optimalen Funkbedingungen und unter Ausnutzung von Mehrfachwegen (MIMO) bis zu 1,3 Gbit/s erreichbar. Ein Teil dieser Bitrate wird allerdings für Protokolldaten und Fehlerkorrektur benötigt. Publizierte Messergebnisse zeigen für ein einzelnes Endgerät in einem 802.11ac WLAN einen Durchsatz auf TCP-Ebene von 400 Mbit/s bis 700 Mbit/s (Kolahi und Almatrook 2017).

5.8.3 WLAN und IoT

Der Maschine-zu-Maschine-WLAN-Standard WiFi HaLow wurde aus 802.11ac abgeleitet. Die WiFi Alliance und IEEE platzieren ihn als Maschine-zu-Maschine Kommunikationslösung zwischen den Personal Area Networks wie Bluetooth Low Energy und Zigbee sowie den LoRa-Netzwerken (Abschn. 5.8.1) mit großer Reichweite. IEEE 802.11ah nutzt das lizenzzfreie UHF Frequenzband bei 868 MHz. Es wurde ein besonders robustes Übertragungsverfahren auf der Basis von OFDM definiert. Damit werden Reichweiten bis zu 1 km möglich. Die erreichbaren Datenraten liegen zwischen 150 kbit/s und 350 Mbit/s.

Wie bei allen IoT-Standards sind auch bei WiFi HaLow der niedrige Energieverbrauch und eine große Zahl von anschließbaren Endgeräten von zentraler Bedeutung. Unterstützt werden bis zu 8000 Endgeräte pro Access Point und Laufzeiten von bis zu 10 Jahren für batteriegetriebene Endgeräte. Der Energieverbrauch der Endgeräte wird durch eine Reihe von Maßnahmen reduziert. Die Anzahl der Kollisionen von Nachrichten wird durch Einteilung der Endgeräte in Gruppen mit festen Zeitfenstern vermindert. Jede Kollision erzwingt eine Wiederholung und kostet damit Energie. Da die angestrebten IoT-Anwendungen in der Regel nicht zeitkritisch sind, wirkt sich die geplante Wartezeit auf das Zeitfenster nicht nachteilig aus. Es wurde eine Verschlankung des Protokolls und der Datenstrukturen vorgenommen. Die Message-Header wurden verkürzt, was wiederum die Übertragungszeit und die Kollisionswahrscheinlichkeit verringert. Für weitere Energieersparnis wurde die Möglichkeit für Endgeräte geschaffen, nur zu vorbestimmten Zeiten zu senden, sowie in einen langen Schlafmodus zu fallen, ohne die bestehende Verbindung zu lösen. Die regulatorisch vorgegebene maximale Belegungszeit von 0,1 % (4 s/Stunde) im UHF-Band erlaubt ohnehin nur wenige Aktivitätsfenster pro Stunde.

5.8.4 WLAN-Nutzung

Neben der WLAN-Nutzung innerhalb geschlossener, gesicherter Netze in der Wohnung oder im Büro wächst die Zahl der öffentlich verfügbaren Zugangspunkte (Hotspots). Hierunter werden öffentliche Funknetzwerke (Public WLAN) an zentralen, belebten Plätzen verstanden, wie z. B. in Flughäfen, Hotels oder Einkaufszentren. Alle Nutzer mobiler Geräte können Teilnehmer des öffentlichen Funknetzes werden und dadurch Zugang zum Internet erlangen.

Die überwiegende Mehrzahl aller öffentlichen Hotspots wird über Netzbetreiber angeboten, hierbei muss sich der Nutzer identifizieren. Konferenzveranstalter und Hotels bieten abgesicherte Hotspots auch ohne individuelle Authentifizierung an. Der Zugangscode ist hierbei für alle Teilnehmer gleich. Diese Art der Absicherung ist allerdings nicht automatisch mit einer Verschlüsselung verbunden, sondern soll regelmäßig lediglich den Zugang und die Nutzung durch nicht berechtigte Personen verhindern. Ferner gibt es auch offene Hotspots, die ohne Registrierung oder Identifikation genutzt werden können. Diese Form des Public-WLAN findet sich bei touristischen Sehenswürdigkeiten, Bibliotheken, Cafés oder in Innenstadtbereichen (z. B. das Freifunk-Netzwerk). Bis zum Jahr 2017 hafte der WLAN-Betreiber für missbräuchliche Nutzung. Mittlerweile wurde diese sogenannte „Störerhaftung“ jedoch weitgehend abgeschafft. Nur wenn ein WLAN-Nutzer das geistige Eigentum verletzt und keine andere Möglichkeit besteht, diese Verstöße zu unterbinden, kann der Rechteinhaber vom WLAN-Betreiber verlangen, diese Inhalte zu sperren ([Verbraucherzentrale 2021](#)).

Wurden lange Zeit WLAN und öffentlicher Mobilfunk (insbesondere LTE) als Konkurrenten angesehen, setzen sich inzwischen Kooperationen der beiden Technologien durch (sogenannte Heterogene Netze). Die in Abschn. [4.5.4.2](#) besprochene Lösung WiFi Calling ermöglicht es, eine vorhandene WLAN-Verbindung mittels eines automatisch eingerichteten VPN für Telefongespräche über das LTE-Kern-Netz zu nutzen.

5.8.5 Vergleich der Personal- und Local-Area Technologien im Internet of Things

Der Nahbereich mit Personal Area Networks (PAN) und Local Area Networks (LAN) ist für Anwendungen im Internet of Things von besonderer Bedeutung. Abb. [5.16](#) zeigt, dass mehr als zwei Drittel aller IoT-Endgeräte weltweit im Jahr 2030 in dieser Kategorie erwartet werden.

Ein Vergleich der hier vorgestellten Short Range IoT Techniken Bluetooth, BLE, Zigbee und WLAN ist unter diesem Aspekt besonders interessant (Tab. [5.4](#)):

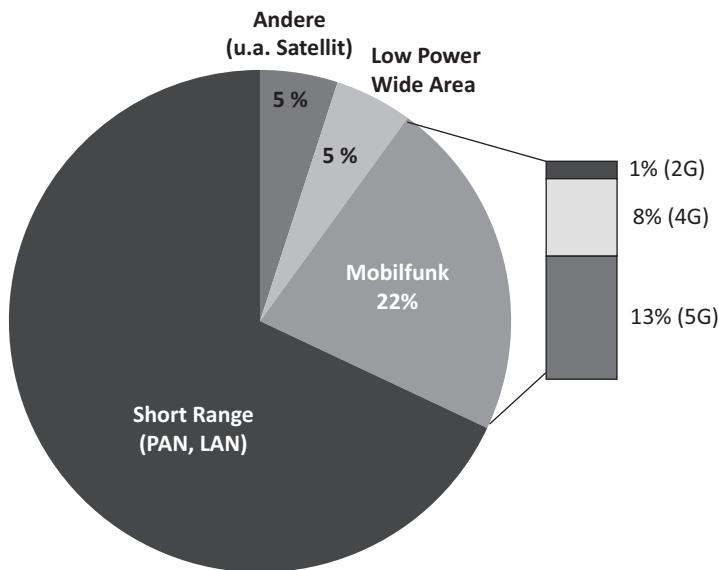


Abb. 5.16 Erwartete IoT-Anschlüsse 2030 weltweit (Statista 2020)

Tab. 5.4 Vergleich der Local und Personal Area Netze für das Internet of Things

| Technologie | WLAN | | Bluetooth | | Zigbee |
|-----------------------------------|----------------|------------------------------|-------------------------------------|------------------------|------------------------------------|
| Standard | IEEE802.11ac/n | IEEE802.11 ah | IEEE802.15.1 | [BLE] | IEEE802.15.4 |
| Frequenzen | 2,4 GHz 5 GHz | 868 MHz und 915 MHz | 2,4 GHz | 2,4 GHz | 2,4 GHz |
| Max. Sendeleistung | 100 mW | 100 mW | 100 mW | 10 mW | 10 mW |
| Reichweite | 100 m | 1000 m | 100 m | 40 m | 70 m |
| Batterie-Laufzeit (Größenordnung) | Stunden | Monate – Jahre | Stunden | Monate – Jahre | Monate – Jahre |
| Netztopologie | Stern, ESS | Stern | Stern, Zusammenschaltung von Netzen | Stern | Stern, Baum, verzweigte Strukturen |
| Anzahl Geräte/ Hub | 30 | 8000 | 7 aktiv, bis 256 verbunden | 128 | 64.000 |
| Datenrate | 1300 Mbit/s | 150 kbit/s – 350 Mbit/s | 3 Mbit/s | 1 Mbit/s | 250 kbit/s |
| Verbindungs-aufbau | 3 s | Netzabhängig (Anzahl Geräte) | 10 s | 0,3 ms | 30 ms |
| Sicherheit | WPA 2/3 | WPA2/3 | AES 128 | AES 128 | AES 128 |
| Kosten | mittel – hoch | niedrig | niedrig | niedrig – sehr niedrig | sehr niedrig |

5.9 Low Power Wide Area Netze

Unter der Bezeichnung *Low Power Wide Area Network* (abgekürzt LPWA, übersetzt: Niedrigenergie-Weitverkehrs-Netzwerke) werden Funktechnologien und Netzwerkprotokolle zusammengefasst, die eine Verbindung von Niedrigenergiegeräten wie beispielsweise batteriebetriebene Sensoren mit einem Netzwerkserver herstellen. Die Hardwarekomponenten sind auf große Reichweiten, geringen Energieverbrauch und niedrige Kosten der Endgeräte ausgelegt. Dabei werden durchweg lizenzenfreie Frequenzbänder genutzt. Da diese Bänder auch anderen Nutzern offenstehen und gleichzeitig die Sendeleistung stark beschränkt ist, entsteht das in Abb. 5.17 illustrierte Problem. Lokale Netze und andere Weitverkehrsnetze auf demselben Frequenzband entlang der Übertragungsstrecke und in der Nähe des Empfängers verursachen starke Störungen des übertragenen Signals. Das Systemdesign muss entsprechend robuste Übertragungsverfahren und insbesondere Redundanz zur Fehlerkorrektur einsetzen. Das bedeutet in Kombination mit der geringen zur Verfügung stehenden Bandbreite und den regulatorischen Restriktionen, dass nur geringe Datenraten erzielt werden können. Die Übertragung von Sprache und Medieninhalten ist dabei ausgeschlossen. Die LPWA-Netze stellen insofern keine direkte Konkurrenz für die IoT-Lösungen der öffentlichen Netze dar, sind aber interessant für spezifische Anwendungen.

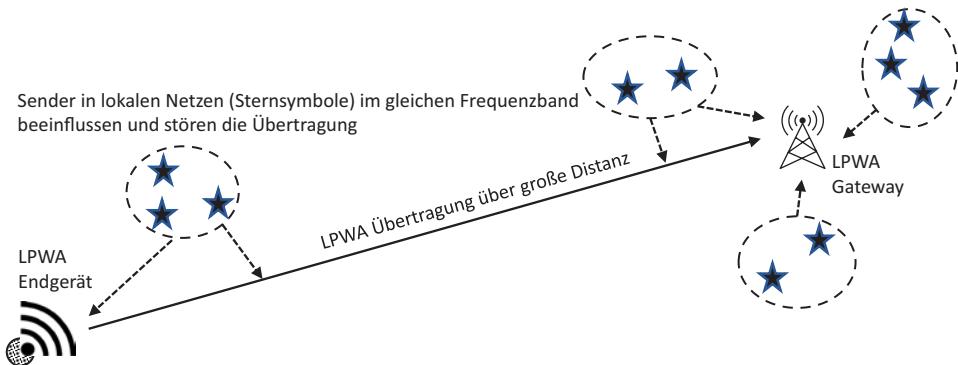


Abb. 5.17 Störquellen bei Low Power Wide Area Netzen

Ein LPWA-Netzwerk umfasst

- *Endgeräte*, insbes. Sensoren zur Messung von Füllständen, Luftdruck, Temperatur
- *Netzwerkserver*
- *Gateways* (Basisstationen), die Daten zwischen den Endgeräten und einem Netzwerkserver weiterleiten
- *Applikationsserver*, deren Programme eine Datenanalyse ermöglichen (Abb. 5.18)

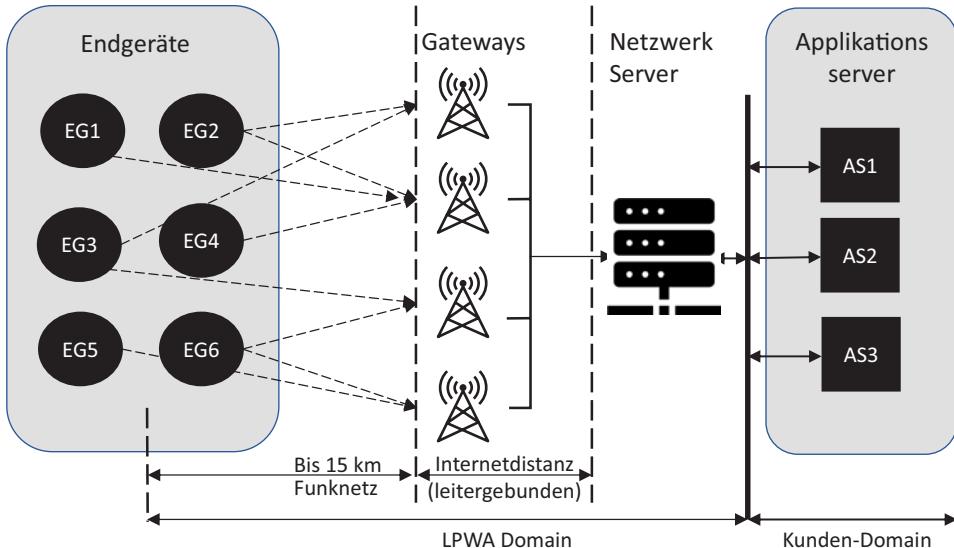


Abb. 5.18 LPWA – Architektur

Die Verbindung zwischen den Sensoren, Gateways und Netzwerkserven erfolgt innerhalb der EU über eines der lizenzenfreien UHF-Bänder bei 433 MHz oder 868 MHz, die auch für RFID genutzt werden. In den USA und in Asien werden vergleichbare lizenzenfreie Frequenzen verwendet. Ein LPWA-Netz verbindet IoT-Endgeräte mit geringem Daten- und Energiebedarf drahtlos mit dem Internet. Die LPWA-Standards haben teilweise vergleichbare Anwendungen wie die durch die Mobilfunknetze angebotenen Standards LTE-M und Narrowband-IoT (NB-IoT), wie in Abschn. 4.5 beschrieben. Es existieren mehrere LPWA-Technologien, von denen hier nur zwei beispielhaft dargestellt werden.

LPWA-Netze werden in der Industrie vor allem für das Internet der Dinge und in Städten für die Umsetzung von Smart City-Anwendungen genutzt. Im Bereich Smart Cities können die Luftqualität gemessen, Füllstände von Abfallbehältern kontrolliert oder die Belegung von Parkplätzen mittels Parksensoren überwacht werden. Die Stadt Mönchengladbach baut ein Netz von Sensoren zur Überwachung der Bodenfeuchte an Baumstandorten auf und plant, es in der Zukunft auch zur bedarfsgerechten Straßenbeleuchtung in selten genutzten Bereichen zu nutzen (Gruhn 2021). Gebietskörperschaften wie Landkreise wenden die Technologie zur Digitalisierung im ländlichen Raum an (Brinkmann 2020). Die durch die Technologie ermöglichten Datenraten von bis zu 250 Bit/s bei gleichzeitiger Beschränkung der Anzahl der Nachrichten pro Endgerät ist für die geplanten Anwendungen ausreichend. Der Fokus liegt hier eindeutig auf der Flächenabdeckung, die mit geringen Kosten erreicht werden kann.

5.9.1 LoRaWAN

Long Range Wide Area Network (LoRaWAN) ist ein Beispiel für eine frei verfügbare, offene Netzwerk-Spezifikation, die von der LoRa Alliance festgelegt wurde (LoRa Alliance 2020). Die Technik kann lizenfrei verwendet werden, allerdings ist die zugrunde liegende Hardware (Chipsatz) nur von einem Halbleiter-Hersteller (Semtech) verfügbar, der auch die grundlegende Spezifikation entwickelt hat. In Deutschland wird LoRaWAN von der Deutschen Bahn genutzt. Beispielsweise werden Bahnhofsuhrn über LoRa-Funk synchronisiert und Störungen gemeldet (Deutsche Bahn 2019).

LoRaWAN verwendet Kanäle von 125 kHz und 250 kHz Bandbreite. Die Bandbreite von 250 kHz steht nur im Uplink zur Verfügung. LoRaWAN fokussiert sich auf den Uplink: Typische Anwendungen bestehen im Übertragen von Messwerten wie Temperatur, Wasserstand, oder Zählerwerten. Für die Fernsteuerung von Geräten ist die Technologie weniger geeignet. LoRaWAN ermöglicht große Reichweiten und einen äußerst energie-sparenden Betrieb der Endgeräte (Sensoren). Dazu ist die Errichtung eines LoRaWAN-Netzes im Vergleich mit den IoT-Lösungen der lizenzierten Mobilfunknetze mit geringen Investitionen verbunden.

Auf dem physikalischen Level wird die CHIRP-Modulation (Abschn. 3.3.1 und Abb. 3.14) angewendet (Knight 2016). Die Endgeräte und Sensoren wenden zusätzlich verschiedene Spreizfaktoren an, die vom Server definiert werden. Je schwächer das empfangene Signal, desto höher wird der Spreizfaktor gesetzt. Die Spreizfaktoren verändern die Symbollängen. Je größer die Symbollänge, desto sicherer ist bei der CHIRP-Modulation die Erkennung des übertragenen Wertes. Eine hohe Spreizung verlängert jedoch die Übertragungszeit pro Bit und reduziert so die Bitrate. Die Spreizung erlaubt trotz der niedrigen erlaubten Sendeleistung von 25 mW (14 dBm) Reichweiten von 30 km. Insgesamt sind nur sehr niedrige Bitraten zwischen 250 Bit/s und 5,5 kBit/s möglich.

LoRaWAN-Endgeräte und Sensoren sind keinem Gateway fest zugeordnet. Gesendete Daten werden von mehreren Gateways empfangen und an den Server weitergeleitet. Der Server identifiziert und filtert mehrfach empfangene Datenpakete. Entsprechend gibt es auch keine Handover-Prozeduren für mobile Endgeräte. Die Unterstützung der Mobilität erfolgt einfach dadurch, dass ein bewegtes Endgerät im Lauf der Zeit den Empfangsbereich einer Basisstation verlässt, und dafür von weiteren Basisstationen empfangen wird. Insgesamt genügt es, dass immer mindestens eine Basisstation Signale dieses Endgeräts empfängt.

Der Netzzugriff durch ein Endgerät erfolgt ohne Koordination. Eine zu sendende Nachricht wird nach einer zufälligen Wartezeit gesendet. Die Wartezeit dient dazu, Häufungen von Nachrichten zu bestimmten Zeitpunkten (volle Stunde, etc.) zu verhindern. Darüber hinaus besteht keine weitere Anforderung, gleichzeitige Übertragungen zu vermeiden. Es ist die Aufgabe des Netzwerkservers, die parallel eingehenden Nachrichten zu identifizieren und zu trennen. Dabei hilft die Vergabe von unterschiedlichen Spreizfaktoren für unterschiedlich weit entfernte Endgeräte. Parallel eintreffende Nachrichten mit unterschiedlichen Spreizfaktoren lassen sich unterscheiden. Die Anzahl und Größe der Nach-

richten, die ein Endgerät pro Tag senden darf, ist nach der Allgemeinzuteilung für das Frequenzband durch die maximale Belegungszeit (Duty Cycle) von 0,1 % pro Stunde auf dem Frequenzband beschränkt. Das bedeutet, dass Übertragungen maximal 4 Sekunden dauern und auch nicht häufig stattfinden dürfen. Auch diese Einschränkung führt zu einer geringeren Kollisionswahrscheinlichkeit und reduziert die Interferenz.

Es werden drei Klassen von Endgeräten unterschieden:

- *Klasse A*: Batteriebetriebene Sensoren, sie haben die größte Energieeffizienz. Mit einer einfachen AA-Batterie wird eine Laufzeit von über 10 Jahren zugesagt. Die Klasse A muss von allen Endgeräten unterstützt werden. Klasse A Endgeräte sind nur im unmittelbaren Anschluss an ein Uplink-Paket empfangsbereit für eine Downlink-Nachricht. Anschließend gehen sie wieder in den Schlaf-Modus.
- *Klasse B*: Batteriebetriebene Geräte mit mittlerer Energieeffizienz. Zusätzlich zu den Funktionen von Klasse A-Geräten öffnen sie zu geplanten Zeitpunkten ein Fenster für den Empfang von Downlink-Nachrichten. Damit sind sie in der Lage, geplante Aktionen auszuführen.
- *Klasse C*: Bi-direktionale Geräte haben ein nahezu permanent geöffnetes Empfangsfenster. Geschlossen wird es nur, wenn eigene Pakete zu senden sind.

Bei einem IoT-Netzwerk der beschriebenen Art, das in einem frei zugänglichen Frequenzband arbeitet, spielt die IT-Sicherheit eine zentrale Rolle. Dazu gibt es bei LoRaWAN ein abgestuftes System von Schlüsseln zur Authentifikation und zur Verschlüsselung. Jeder Netzknopen meldet sich am Netzwerkserver mit einem dort bekannten Schlüssel an. Der Server antwortet mit verschiedenen Schlüsseln zur Authentifizierung des Endgerätes, zur Verschlüsselung der Daten auf Applikationsebene und zur Authentifizierung jeder einzelnen Nachricht. Replay-Attacken, die auf der langen Übertragungsstrecke unauffällig durchgeführt werden können, sollen mittels mitgesandter zufälliger Byte-Werte (Nonce) verhindert werden.

5.9.2 SigFox

Neben den veröffentlichten LPWA-Standards gibt es proprietäre, nicht-veröffentlichte Technologien mit ähnlichen Funktionsumfang und Eigenschaften. Bekanntes Beispiel ist Sigfox ([Sigfox 2017](#)), entwickelt von dem gleichnamigen französischen Telekommunikationsunternehmen. Sigfox arbeitet dabei selbst als Netzbetreiber, strebt aber auch Partnerschaften an. SigFox tritt in Deutschland unter eigenem Namen an und reklamiert eine Flächenabdeckung von über 80 %. Es fokussiert wie LoRaWAN auf Uplink-Übertragungen. Die Architektur des Netzes ist ganz ähnlich zu LoRaWAN; im Detail gibt es allerdings einige Unterschiede. Auf dem physikalischen Level repräsentiert Sigfox ein sogenanntes Ultra-Narrowband (UNB) Netzwerk. In dem 192 kHz breiten Frequenzband von 868,34 MHz bis 868,226 MHz sendet jedes Netzelement auf extrem schmalen Teil-

Tab. 5.5 Vergleich verschiedener mobiler M2M Kommunikationssysteme (Sinha et al. 2017; Mekki et al. 2019)

| Anforderungen | Lizenziert er Mobilfunk | Lizenziert er Mobilfunk mit LTE-M oder NB-IoT | LPWA | WLAN HaLow | Bluetooth Low Energy |
|-------------------------|----------------------------|---|-----------------|---------------|----------------------------|
| Datenrate | hoch | mittel | sehr niedrig | mittel | niedrig |
| Netzwerkkosten | sehr hoch | sehr hoch | niedrig | niedrig | sehr niedrig |
| Kosten der Endgeräte | mittel – hoch | mittel | sehr niedrig | niedrig | sehr niedrig |
| Batterielaufzeit | kurz | lang (mit angepassten EG) | sehr lang | kurz | sehr lang |
| Abdeckung | mittel | sehr hoch | sehr hoch | niedrig | sehr niedrig |
| Mobilität | sehr hoch | LTE-M: mittel NB-IoT: nur im Idle Mode | hoch | niedrig | sehr niedrig |

Bändern von je 100 Hz Breite. Moduliert wird mit einer binären Phasenmodulation. Das schmale Band ergibt ein sehr niedriges Niveau des thermischen Rauschens und damit eine hohe Empfänger-Empfindlichkeit. Zusätzliche Robustheit der Verbindung wird durch mehrfaches paralleles Senden auf verschiedenen Frequenzen erreicht. Die erzielten Bandbreiten der Datenübertragung liegen zwischen 100 Bit/s und 600 Bit/s.

Sigfox ist noch stärker als LoRaWAN auf den Uplink fokussiert. Es besteht aber die Möglichkeit für das Endgerät, für einige Sekunden nach Senden einer Uplink-Nachricht eine Downlink-Nachricht zu empfangen, bevor es wieder in einen Schlafmodus fällt. Sigfox erlaubt entsprechend der Regeln für das UHF-Band im Uplink maximale Nachrichtengrößen von 12 Byte und 6 Nachrichten pro Stunde oder 140 Nachrichten pro Tag. Die Übertragung von 12 Byte dauert im Mittel etwa 2 Sekunden. Im Downlink sind alle Nachrichten 8 Byte lang, und im Downlink können an jedes Endgerät bis zu 4 Nachrichten pro Tag gesendet werden. Damit können Parameter beim Endgerät gesetzt, aber auch eine Übertragung von Werten angefordert werden.

Die verschiedenen mobilen Kommunikationssysteme sind bezüglich ihrer Eignung für die LPWA Anwendung in Tab. 5.5 zusammengestellt.

5.10 Fragen

1. Erläutern Sie die verschiedenen technischen Komponenten eines RFID-Systems
2. Welche Kommunikationssysteme im Nahbereich basieren auf Funk, welche auf Basis optischer Methoden?
3. Der Logistikbereich eines Unternehmens prüft, ob anstatt der bisherigen Barcode-Etiketten zukünftig Smart Labels (RFID) verwendet werden sollen. Stellen Sie diese beiden Verfahren gegenüber, berücksichtigen Sie dabei die Kriterien Wiederbe-

schreibbarkeit, Sichtverbindung, Beeinflussung der Lesbarkeit durch Schmutz, Lese- bzw. Erkennungsrate insgesamt, Anzahl speicherbarer Zeichen auf einem Etikett, Automatisierung des Lesevorgangs und die Kosten.

4. Welche unterschiedlichen Betriebsarten von WLAN kennen Sie?
5. Inwiefern haftet der Betreiber eines öffentlichen WLAN-Netzes für die Nutzeraktivitäten?
6. Wie ist ein Transponder im Rahmen einer RFID-Anwendung aufgebaut?
7. Welche RFID-Transponder-Typen bzw. Bauformen eignen sich für
 - Patienten-Identifikation in einem Krankenhaus
 - Diebstahlschutz von hochwertigen Elektroartikeln in einem Elektro-Fachgeschäft
 - Diebstahlsicherung in einer Bekleidungsboutique
 - Zutrittskontrolle in einem Bürogebäude
 - Skipass
 - Schlüssel in einem Hotel?
8. Erläutern Sie den Unterschied zwischen geschlossenen und offenen RFID-Systemen.
9. Welche Anwendungsmöglichkeiten gibt es für iBeacons im stationären Einzelhandel?
10. Wie funktioniert Mobile Tagging?
11. Welche der in Abschn. 5.4 beschriebenen NFC-Rollen nimmt das Smartphone über seine NFC-Schnittstelle beim mobilen Bezahlen ein?
12. RFID im Hochfrequenzbereich erlaubt einen Leseabstand von 1,2 m. Die technische Beschränkung der NFC-Reichweite im gleichen Frequenzbereich auf ca. 10 cm stellt ein Sicherheitsfeature dar. Erklären Sie, warum!
13. Erklären Sie die Rolle eines Applikationsprofiles in der Gerätekommunikation.
14. Grenzen Sie Applikationsprofile gegenüber Kommunikationsstandards ab.
15. Wie verhält sich der Bluetooth Low Energy Standard zu Bluetooth?
16. Zigbee ist wegen der geringen Gerätekosten eine sehr kostengünstige Kommunikationstechnik. Könnte mit Zigbee auch eine Computervernetzung im Heimbereich (wie beim Anschluss von Druckern oder Kopfhörern) durchgeführt werden?
17. Welche Bandbreite steht einem einfachen WLAN Routermodell ohne DFS und TPC im 5 GHz-Bereich maximal zur Verfügung?
18. Benennen Sie die Komponenten eines LPWA-Systems
19. Was macht den hohen Wiedererkennungswert der „CHIRP“-Symbole aus (warum ist die LoRa-Technik robust)?
20. Vergleichen Sie die LPWA-Technik mit der LTE-Variante NB-IoT. Entscheiden Sie in den folgenden Anwendungsfällen, welcher Technik Sie jeweils den Vorzug geben würden.
 - a. Meldung von Wasserständen entlang eines Flusses an eine Zentrale.
 - b. Übertragung von Daten aus der Verkehrsüberwachung an die Zentrale mit der Möglichkeit des Rückrufes (Telefonverbindung).
 - c. Steuerung von Einfahrtstoren von einer entfernten Zentrale aus.
 - d. Kostengünstiger Betrieb von Einbruchsmeldern für Privatkunden.
 - e. Fahrstuhlierwachung mit möglichem Kontakt zu Personen bei Störungen.

Literatur

- Abts D, Mülder W (2017) Grundkurs Wirtschaftsinformatik, 9. Aufl. Springer, Wiesbaden. <https://doi.org/10.1007/978-3-658-16379-2>
- Brinkmann H (2020) Kreis startet Digitalisierungsoffensive. Rheinische Post, 16. November 2020
- Bundesamt für Sicherheit in der Informationstechnik (2005) Risiken und Chancen des Einsatzes von RFID-Systemen. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ElekAusweise/RFID/RIKCHA_barrierefrei_pdf.pdf?__blob=publicationFile&v=2. Zugegriffen am 15.09.2021
- Bundesnetzagentur (2021) Allgemeinzuteilungen. Bundesnetzagentur. https://www.bundesnetzagentur.de/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Frequenzen/Allgemeinzuteilungen/allgemeinzuteilungen-node.html. Zugegriffen am 08.09.2021
- Connectivity Standards Alliance (2019) Zigbee Technische Präsentation. Connectivity Standards Alliance. Davis: Connectivity Standards Alliance. https://zigbeealliance.org/de/developer_resources/zigbee-technische-präsentation. Zugegriffen am 29.03.2021
- Curran K, Millar A, Mc Garvey C (2012) Near field communication. Int J Electr Comput Eng 2(3):371–382. <https://doi.org/10.11591/jece.v2i3.234>
- Deutsche Bahn (2019) Bahnhofsuhren: außen analog, innen digital. Deutsche Bahn. https://www.deutschebahn.com/de/Digitalisierung/technologie/digitaler_alltag/lorawan-3232292. Zugegriffen am 08.09.2021
- Gerstner M (2010) ZigBee. Technische Universität Wien, Wien
- Gruhn A (2021) 16 Millionen Euro für Mönchengladbach. Rheinische Post, 17. Mai 2020
- Knight M (2016) Decoding the LoRa PHY – Dissecting a modern wireless network for the Internet of Things. 33C3. Chaos Computer Club, Berlin. https://media.ccc.de/v/33c3-7945-decoding_the_lora_phy. Zugegriffen am 08.09.2021
- Kolahi SS, Almatrook AA (2017) Impact of Security on Bandwidth and Latency in IEEE 802.11ac Client-to-Server WLAN. In: 2017 Ninth International Conference on Ubiquitous and Future Networks (IEEE ICUFN). IEEE, Milan, S 893–897. <https://doi.org/10.1109/ICUFN.2017.7993928>
- LoRa Alliance (2020) LoRaWAN 1.0.4 Specification Package. LoRaAlliance. https://lora-alliance.org/resource_hub lorawan-104-specification-package/. Zugegriffen am 08.09.2021
- Mekki K, Bajic E, Chaxel F, Meyer F (2019) A comparative study of LPWAN technologies for large-scale IoT deployment. ICT Express 5(1):1–7. <https://doi.org/10.1016/j.icte.2017.12.005>
- Schoblick R, Schoblick G (2005) RFID Radio Frequency Identification: Grundlagen, Eingeführte Systeme, Einsatzbereiche, Datenschutz, Praktische Anwendungsbeispiele, 1. Aufl. Franzis, Haar. 978-3-772-35920-0
- Sigfox (2017) Sigfox: Technical overview. Sigfox. <https://www.sigfox.us/technical-overview/>. Zugegriffen am 31.08.2021
- Sinha RS, Wei Y, Hwang S-H (2017) A survey on LPWA technology: LoRa and NB-IoT. ICT Express 3(1):14–21. <https://doi.org/10.1016/j.icte.2017.03.004>
- Statista (2020) Number of Internet of Things (IoT) connected devices worldwide from 2019 to 2030, by communications technology. Statista. <https://www.statista.com/statistics/1194688/iot-connected-devices-communications-technology/#statisticContainer>. Zugegriffen am 08.09.2021
- Verbraucherzentrale (2021) Störerhaftung: besserer Schutz für WLAN-Betreiber. Verbraucherzentrale. <https://www.verbraucherzentrale.de/wissen/digitale-welt/mobilfunk-und-festnetz/stoererhaftung-besserer-schutz-fuer-wlanbetreiber-19261>. Zugegriffen am 31.08.2021



Mobile Endgeräte

6

6.1 Einführung und Lernziele

Entsprechend der Entwicklung der Mobilfunknetze in Deutschland (Abschn. 1.4) wurden auch die ersten mobilen Endgeräte entwickelt. Ab 1926 konnte beispielsweise die Sprachtelefonie im Zug zwischen Berlin und Hamburg genutzt werden. Dabei war die Kooperation zwischen Reichsbahn und Reichspost zum Aufbau dieses Dienstes von entscheidender Bedeutung. Allerdings blieb die mobile Kommunikation ein Privileg der Reisenden der ersten Klasse.

Eine zunehmende Verbreitung mobiler Endgeräte in Deutschland war dann mit dem Aufkommen der Autotelefonie im A-Netz der Deutschen Bundespost ab 1958 zu verzeichnen. Der Begriff des mobilen Endgeräts bezog sich dabei insbesondere auf seine Verwendung im „Automobil“, waren die Endgeräte doch so groß, dass der wesentliche Teil im Kofferraum des Fahrzeugs installiert wurde. Nur die Bedienkonsole wurde im Cockpit verbaut. Die Größe der Endgeräte resultierte aus der Verwendung von Röhrentechnologie. Die Preise der Endgeräte bewegten sich im Bereich der Anschaffungskosten für einen Kleinwagen.

Mit Reduzierung der Größe der Funkzellen im analogen C-Netz und einer damit einhergehenden Reduzierung der Sendeleistung der mobilen Endgeräte konnten diese auch in ihrer Größe schrumpfen. Mit bis zu 800.000 Kunden in Deutschland war ein breiterer Markt für mobile Endgeräte gegeben. Die Portabilität der Geräte stand im Vordergrund, was sich auch in den Modellbezeichnungen widerspiegelte: „Portables“. Eine kleine Auswahl wird im Folgenden dargestellt.

Der technische Fortschritt ermöglichte eine weitere Verkleinerung der Endgeräte, da diese z. B. in den digitalen Mobilfunknetzen (GSM) wiederum eine niedrigere Sendeleistung benötigten und neue Batterietechnologien eine höhere Effizienz bei kleinen Bauarten erzielten.

► **Lernziele**

- Sie kennen die Geschichte der mobilen Endgeräte.
 - Sie kennen ausgewählte, historisch relevante mobile Endgeräte.
 - Sie kennen Endgeräteklassen und die zugehörigen Klassifizierungsmerkmale.
 - Sie kennen bedeutsame Betriebssysteme für mobile Endgeräte.
 - Sie können die Besonderheiten mobiler Endgeräten für Machine-to-Machine-Kommunikation und für das Internet of Things erläutern.
-

6.2 Geschichte der mobilen Endgeräte

6.2.1 Entstehung der Bezeichnung „Handy“

Interessant ist die Verwendung des englischen Adjektivs „handy“ (handlich, praktisch) als Bezeichnung für ein Mobiltelefon in der deutschen Sprache. Dabei handelt es sich um einen sogenannten Scheinanglizismus, denn die korrekte englischsprachige Produktbezeichnung lautet (je nach Region) cellular phone, cell phone, mobile phone oder in Kurzform mobile oder portable. Ein interessanter sprachlicher Effekt zeichnet sich in Slangformen der englischen Sprache ab; hier wird der nun wiederum aus dem deutschen reimportierte Begriff des „Handys“ als Substantiv tatsächlich in seiner Interpretation als Mobiltelefon verwendet. Wie die Verwendung des Begriffes Handy in die deutsche Sprache einfließen konnte, ist bislang sprachwissenschaftlich nicht geklärt. Verwendung findet die Bezeichnung etwa ab der Einführung des GSM-Netzes in Deutschland. Einen Hinweis könnte die Nutzung von „handy“ in Teilen von Modellbezeichnungen früher mobiler Endgeräte liefern. So produzierte etwa Motorola neben seinem Walkie-Talkie (SCR-300, welches schon im zweiten Weltkrieg auf dem Rücken getragen wurde) auch ein Handie-Talkie (SCR-536), welches wie ein Telefon gehalten werden konnte. Loewe produzierte Anfang der 1990er-Jahre ein analoges D-Netz-Mobiltelefon mit der Bezeichnung HandyTel 100, und Philips benannte sein handliches D-Netz Endgerät als „Handy“ in Abgrenzung zum tragbaren C-Netztelefon „Porty“ aus dem gleichen Hause. Funkamateure nutzten die Bezeichnung Handy schon vorher und meinten damit einen hand-held transceiver, also eine in der Hand gehaltene Sende- und Empfangseinrichtung.

6.2.2 Ausgewählte mobile Endgeräte in der historischen Entwicklung

Die Abb. [6.1](#), [6.2](#), [6.3](#), [6.4](#), [6.5](#), [6.6](#), [6.7](#), [6.8](#), [6.9](#), [6.10](#), [6.11](#), [6.12](#), [6.13](#), [6.14](#), [6.15](#), [6.16](#), [6.17](#), [6.18](#), [6.19](#), [6.20](#), [6.21](#), [6.22](#), [6.23](#), [6.24](#), [6.25](#), [6.26](#), [6.27](#) und [6.28](#) zeigen eine Über-



Abb. 6.1 SRA/Ericsson MTA, (Fotograf unbekannt, Quelle: https://www.computerwoche.de/i/detail/artikel/2104154/1/2036219/EL_12548184128436900724154/)

sicht bedeutsamer mobiler Endgeräte ihrer jeweiligen „Epoche“. Hierbei wird deutlich, dass mobile Endgeräte im Verlaufe der Zeit einen enormen Wandel durchlebt haben. Gewicht, Funktionsumfang, Akkulaufzeit oder Design sind nur vier ausgewählte Faktoren, welche die Entwicklung verdeutlichen.

1956 – SRA/Ericsson MTA (Mobile Telephone System A)

Noch ohne einen etablierten internationalen Mobilfunkstandard haben Hersteller in den frühen 1950er-Jahren erste Endgeräte entwickelt. Dabei entstanden proprietäre Systeme, die sich von Unternehmen zu Unternehmen unterschieden. Das SRA/Ericsson MTA (Abb. 6.1) ist ein typischer Vertreter dieser Generation. Obwohl als Mobiltelefon bezeichnet, ist klar, dass es mit einem Gewicht von über 50 kg tatsächlich stationär oder im Automobil eingebaut verwendet wurde. Das gesamte System für die Telefonie war hier auf zwei schwedische Städte begrenzt, die mit Funkzellen ausgestattet waren. Diese Einschränkung sowie unter anderem auch der Preis des Endgerätes führten dazu, dass die Nutzerzahl in einem sehr niedrigen dreistelligen Bereich verblieb. Vorteilhaft bei diesem System war die Möglichkeit, ohne manuelle Verbindungsschaltung auszukommen, sondern andere Teilnehmer direkt anrufen zu können.

1983 – Motorola DynaTAC 8000X

Motorola entwickelte bereits in den frühen 1970er-Jahren erste Prototypen mobiler Endgeräte. Die geringe Verbreitung von Mobilfunkzellen ließ jedoch einen Markteintritt unrentabel erscheinen. Nach Ausbau der Netze wurde das DynaTAC 8000X im Jahr 1983 vorgestellt (Abb. 6.2). Es wurde schnell zu einem Statussymbol, gerade weil der hohe Preis (ca. 4000 US-\$) einer weiten Verbreitung im Wege stand. Dennoch kann dieses Modell als Wegbereiter des Mobilfunk-Zeitalters genannt werden.

Abb. 6.2 Motorola DynaTAC 8000X, (https://de.wikipedia.org/wiki/Motorola_DynaTAC#/media/File:DynaTAC8000X.jpg (CC BY-SA 3.0, <https://creativecommons.org/licenses/by-sa/3.0/> Nutzer: Kozuch))



Abb. 6.3 Nokia Mobira Talkman (Fotograf unbekannt, Quelle: <https://nokiamuseuminfo.wordpress.com/1985/05/27/nokia-mobira-talkman/>)



1984 – Nokia Mobira Talkman

Nokia folgte mit der Vorstellung des Mobira Talkman. Es zeichnete sich im Vergleich mit dem Motorola-Modell durch eine deutlich höhere Akkulaufzeit aus. Mit einem Gewicht von über 5 kg war es zwar leichter als seine Vorgänger (z. B. das Nokia Mobira Senator), jedoch immer noch kein Gerät für die Westentasche. In der Werbung wurde es dennoch als „ultraportable“ bezeichnet (Abb. 6.3).

1989 – Motorola MicroTAC

1989 legte Motorola nach und brachte als Nachfolger für das DynaTAC das deutlich kleinere MicroTAC auf den Markt. Die relativ platzsparende Bauweise wurde durch eine Klappe ermöglicht, die zum Sprechen geöffnet wurde, bei Nichtgebrauch aber geschlossen blieb. So wurde das Motorola MicroTAC zum ersten Klapp-Handy überhaupt (Abb. 6.4).

Abb. 6.4 Motorola MicroTAC 9800X, (https://en.wikipedia.org/wiki/Motorola_MicroTAC#/media/File:Motorola_MicroTAC_9800x.jpg (Public Domain, Nutzer: Ross Padluck))



Abb. 6.5 IBM Simon, (https://commons.wikimedia.org/wiki/File:IBM_Simon_Personal_Communicator.png (Public Domain, Nutzer: Hohum))



1992 – IBM Simon

Als Vorläufer unserer heutigen Smartphones gilt das IBM Simon. Es kam 1992 auf den Markt und konnte mit einem Touchscreen aufwarten. Neben der Telefonie ermöglichte es außerdem den Versand von Faxen und beinhaltete kleine Spiele (Abb. 6.5).

1994 – Motorola 2900 Bag Phone

Die Mehrzahl der mobilen Endgeräte der 1980er-Jahre waren Modelle, die mitsamt einer Tasche zur Aufnahme der Batterie und der Sende-/Empfangseinheit ausgeliefert wurden. Dass sich diese Bauweise auch in den 1990er-Jahren noch wiederfindet, zeigt das Motorola 2900 Bag Phone (Abb. 6.6). Die Modelle wurden daher bevorzugt immer noch im Auto oder mittels der Tasche „über die Schulter“ getragen verwendet. Vorteile der großen Taschen waren die lange Akkulaufzeit sowie die guten Sendeleistungen der Endgeräte, da auf Miniaturisierung nicht der größte Wert gelegt werden musste.

Abb. 6.6 Motorola 2900 Bag Phone, (Herstellerbild)



Abb. 6.7 Motorola StarTAC, (https://commons.wikimedia.org/wiki/File:Telefono_cellulare,_GS-M_-_Museo_scienza_tecnologia_Milano_09735_02.jpg (CC BY-SA 4.0, <https://creativecommons.org/licenses/by-sa/4.0/> Nutzer: Federico Leva))

1996 – Motorola StarTAC

Ein Meilenstein war die Entwicklung eines ersten Klapphandys durch Motorola. Eine Domäne, in welcher der Hersteller lange Zeit eine Stärke hatte. Der Klappmechanismus machte das Motorola StarTAC seinerzeit zu einem der kleinsten und leichtesten mobilen Endgeräte (Abb. 6.7).

1997 – Nokia 9000i Communicator

1997 wird als Ursprungsjahr der modernen Smartphones angesehen. Das liegt insbesondere an der Veröffentlichung des Nokia 9000i Communicator (Abb. 6.8). Der Communicator war nicht nur ein Mobiltelefon, sondern vereinigte auch die Eigenschaften der parallel aufkommenden PDAs (Personal Digital Assistant) in einem Gerät. Das Betriebssystem beinhaltete einen HTML-fähigen Browser. Der Internetzugang erfolgte über GSM. Vorgesehen war auch die Funktionalität, Faxe zu senden und zu empfangen. Hier ist also bereits die Konvergenz auf Geräteseite zu erkennen. Ungewöhnlich beim Communicator war das Gerätedesign, da der Klappmechanismus an der Längsseite angebracht war, das Gerät also quer aufgeklappt wurde. Das Display war im Deckel verbaut, in der Unterschale fand sich eine QWERTZ-Tastatur.

Abb. 6.8 Nokia 9000i Communicator (geschlossene und geöffnete Variante), (geschlossen: <https://commons.wikimedia.org/w/index.php?curid=78140914> (CC BY 2.0, <https://creativecommons.org/licenses/by/2.0/> Nutzer: Winfel), geöffnet: https://de.m.wikipedia.org/wiki/Datei:Nokia_Communicator_9000_Opened_01.jpg (CC BY 2.0, <https://creativecommons.org/licenses/by/2.0/> Nutzer: Winfel))



Abb. 6.9 Nokia 8810, (Herstellerbild)



1998 – Nokia 8810

1998 setzte sich eine weitere einschneidende Designentwicklung durch: Die Antenne der mobilen Endgeräte wurde nun vollständig in die Gehäuse integriert. Das Nokia 8810 war damit Vorläufer und Urahn der kommenden Nokia Modellreihen (Abb. 6.9).

1999 – Nokia 7110

Das Ende der 1990er-Jahre war in Deutschland (aber auch weltweit) von einer Aufbruchsstimmung durch das Aufkeimen der New Economy geprägt. Dazu zählte auch, dass neue Technologien – im Mobilfunkbereich insbesondere das Wireless Application Protocol (WAP) – zu einem breiten Einsatz kamen. WAP ermöglichte eine schlanke Darstellung von Webseiten auf mobilen Endgeräten mit einfachen Displays. Nokia präsentierte mit dem Modell 7110 ein erstes Endgerät, welches diesen Standard unterstützte (Abb. 6.10).



Abb. 6.10 Nokia 7110, (Herstellerbild)

Abb. 6.11 Toshiba Camesse,
(Karasawa, J., Segawa, M.,
Kishimoto, Y., Aoki, M.,
Sasaki, T. (2001). Flip chip
interconnection method
applied to small camera
module. IEEE 51st Electronic
Components and Technology
Conference 2001 Proceedings.
Orlando: IEEE. 1024–1028.
doi:10.1109/ectc.2001.927938)



Das Unternehmen rückte so immer stärker in eine Vorreiterrolle für die gesamte Branche und sollte es binnen weniger Jahre zum Marktführer im Bereich der mobilen Endgeräte bringen.

1999 – Toshiba Camesse

Wie unterschiedlich die Präferenzen der Nutzer hinsichtlich ihrer mobilen Endgeräte sind, ließ sich anhand des Toshiba Camesse erkennen (Abb. 6.11). In Deutschland kaum verbreitet war dieses Endgerät ein großer Erfolg in Japan. Neben einer Kamera enthielt es bereits ein Bildbearbeitungsprogramm für die erstellten Photos. Erste Ansätze zu Social Networks und deren Nutzung auf mobilen Endgeräten waren ebenfalls in Japan zu beobachten. Es existierte eine Plattform, auf welche die Nutzer ihre erstellten Photos hochladen konnten.

2001 – Siemens SL45

Mit der Integration eines MP3-Players konnten Nutzer des Siemens SL45 (Abb. 6.12) auf Ihre eigene Musiksammlung zurückgreifen – auch wenn die Synchronisation mit dem Computer sich als umständlich herausstellte. Das Musikhören mit dem mobilen Endgerät

Abb. 6.12 Siemens SL45,
(Herstellerbild)



Abb. 6.13 RIM Blackberry 5810, (Herstellerbild)

an sich war keine Neuerung, hatten doch viele Hersteller früher bereits einen UKW-Empfänger für Radio eingebaut.

2002 – RIM BlackBerry 5810

BlackBerry-Geräte starteten Ende der 1990er-Jahre als – in den USA sehr beliebte – Pager, also kleine Endgeräte zu Alarmierungs- und Benachrichtigungszwecken. Schnell entwickelten sie sich jedoch zu leistungsfähigen Smartphones weiter. Das Modell 5810 besaß eine „richtige“ Tastatur und bot als Besonderheit einen Push-Dienst für E-Mails (Abb. 6.13). Gerade diese Funktionalität machte die Geräte in der Folge zu fast unverzichtbaren Accessoires für Geschäftsleute und Unternehmen.



Abb. 6.14 Sanyo SCP-5300, (Herstellerbild)

2002 – Sanyo SCP-5300

Die Gerätekonvergenz sollte sich in der Folge weiter fortsetzen. So verwundert es nicht, dass bald auch digitale Kameras in die mobilen Endgeräte verbaut wurden. Das Sanyo SCP-5300 war der erste Vertreter dieser Gerätekasse, welches in einem breiten Markt verfügbar war (Abb. 6.14). Seine Vorgänger finden sich insbesondere in Japan (z. B. Toshiba Camesse).

2002 – T-Mobile Sidekick

Textuelle Kommunikation war auf dem Vormarsch und wurde seit den frühen 2000er-Jahren auch auf den mobilen Endgeräten betrieben. Folglich versuchten die Anbieter dies über ihre Endgeräte zu vereinfachen. Ein Beispiel für diesen Trend war das T-Mobile Sidekick, welches mit einem neuen Design, einem großen beweglichen Display sowie einer QWERTZ-Tastatur aufwarten konnte (Abb. 6.15).

2003 – Nokia 3650

Kameras zum Fotografieren waren im Jahr 2003 bereits Standard, nun fügte Nokia einen videofähigen Chip hinzu. Die Aufnahmen hatten vergleichsweise niedrige Qualität und der eingebaute Speicher nahm nur wenige Minuten Spielzeit auf. Das Bedienkonzept wartete mit einer kreisförmigen Anordnung der Tasten auf und erinnerte damit an historische Telefone mit ihrer Wähl scheibe (Abb. 6.16).

2004 – Sharp GX30

Ein weiterer Meilenstein war mit der ersten Handykamera mit einer Auflösung von 1 Megapixel erreicht (Abb. 6.17).



Abb. 6.15 T-Mobile Sidekick, (Herstellerbild)

Abb. 6.16 Nokia 3650,
(Herstellerbild)



Abb. 6.17 Sharp GX30,
(Herstellerbild)



Abb. 6.18 Motorola Razr V3,
(Herstellerbild)



2004 – Motorola Razr V3

Spätestens seit dem Razr V3 zählen mobile Endgeräte zu den Lifestyle Accessoires. Das Razr V3 war eines der am besten verkauften Endgeräte, u. a. weil es mit seinem Klappmechanismus, dem großen Display und dem neuartigen Tastaturkonzept als Designobjekt bezeichnet werden konnte (Abb. 6.18). Viele Multimedia-Funktionalitäten wurden mit diesem Endgerät einer breiten Kundenbasis verfügbar.

2004 – Nokia 7600

Ein weiteres innovatives Designkonzept, welches sich am Markt jedoch nicht im gewünschten Maße durchsetzen konnte, wurde mit dem Modell Nokia 7600 realisiert (Abb. 6.19). Das Modell war auf eine Internetnutzung über 3G-Mobilfunknetzwerke ausgelegt. Die (theoretisch) höheren Datenübertragungsraten kamen aufgrund des schleppenden Netzausbau in Deutschland dennoch in der Fläche nicht zum Zuge.

2005 – Siemens SXG75

Location Based Services wurden als der kommende Trend bezeichnet. Entsprechend mussten die mobilen Endgeräte mit einer Ortungsfunktion ausgestattet werden. Siemens präsentierte mit dem SXG75 ein Modell mit eingebautem GPS-Empfänger (Abb. 6.20).

2007 – Apple iPhone 1. Generation

Apple Inc. betrat den Markt als Hersteller für mobile Endgeräte im Jahr 2007. Obwohl die erste Generation des iPhone kaum technische Besonderheiten aufwies, konnte es am Markt große Erfolge verzeichnen (Abb. 6.21). Dabei überzeugte die Nutzer insbesondere das durchdachte Bedienkonzept mit dem großen Touchscreen, der erstmals Multi-Touch und dynamische Bedienaktionen wie Wischen, Bewegen und Spreizen unterstützte. Mit der zweiten Generation des iPhone setzte Apple auf die Entwicklung eines kompletten Ecosystems, welches sich um die iOS-Betriebssystem-Plattform (Kap. 7) bewegte. Die Integration in ein umfassendes Software-Ecosystem, welches die Bedienbarkeit und

Abb. 6.19 Nokia 7600,
(Herstellerbild)



Abb. 6.20 Siemens SXG75, (Herstellerbild)



Abb. 6.21 Apple iPhone, (Herstellerbild)

Abb. 6.22 HTC Dream, (https://commons.wikimedia.org/wiki/File:T-Mobile_G1_launch_event_2.jpg (CC BY-SA 2.0, <https://creativecommons.org/licenses/by-sa/2.0/deed.en> Nutzer: Michael Oryl))



Abb. 6.23 Toshiba TGO1, (Herstellerbild)

Nützlichkeit eines Smartphones – und damit die Benutzer-Perspektive – in den Vordergrund stellte, war seinerzeit eine Revolution. Dem Nutzer wurde damit erstmalig ein einzelner zentraler Zugangspunkt zu vielen Diensten wortwörtlich in die Hand gegeben.

2008 – HTC Dream

Die Einführung des iPhone setzte andere Endgerätehersteller unter Druck. Aus einer Kooperation zwischen HTC und Google gemeinsam mit T-Mobile entstand das HTC Dream (Abb. 6.22). Es handelte sich hierbei um den ersten wirklichen Gegenspieler des iPhone und das erste Gerät mit Android OS als Betriebssystem. Wesentliches Differenzierungsmerkmal war das schiebbare Display, unter dem sich eine Tastatur verbarg.

2009 – Toshiba TGO1

Mit leistungsfähigen Betriebssystemen wurde der Ruf nach leistungsfähigerer Hardware lauter. Das Toshiba TGO1 (Abb. 6.23) war das erste Modell mit einem 1 GHz schnellen Zentralprozessor. Das große Display (4,1“) zeugt ebenfalls von gestiegenen Anforderungen an die Hardware der mobilen Endgeräte. Es sollte zukünftig nicht bei einem Prozessorkern bleiben.

2011 – Samsung Nexus S

Das Nexus S war das zweite Endgerät, welches aus einer engen Kooperation mit Google entstammte (Abb. 6.24). Mit diesem Modell wurde die NFC-Technologie in die Welt der mobilen Endgeräte eingeführt. So konnte eine berührungslose Datenübertragung im Kurzstreckenbereich realisiert werden.

Abb. 6.24 Samsung Nexus S,
(Herstellerbild)



Abb. 6.25 HTC One X,
(Herstellerbild)



2012 – HTC One X

Mobile Games zählen zu den wichtigsten Trends im Mobile Business. Daher überrascht es nicht, dass auch die Hardware immer stärker darauf ausgerichtet wurde. Das HTC One X bestach mit einem Tegra 3 Vierkern-Prozessor, der auf die hohen Grafikanforderungen moderner digitaler Spiele fokussierte (Abb. 6.25). Die Bedeutung von Mobile Games lässt sich aus der Einrichtung einer eigenen Kategorie im Google Play Store ablesen, die explizit Spielen für diesen Nvidia-Chip gewidmet war.

2012 – Samsung Galaxy S3

Das Samsung Galaxy S3 wurde schon mit seiner Vorstellung als der Gegenspieler der Apple iPhone 4S Baureihe positioniert (Abb. 6.26). Basierend auf der seinerzeitigen

Abb. 6.26 Samsung Galaxy S3, (Herstellerbild)



Version des Android OS und einer Samsung-eigenen Benutzeroberfläche bot es über eine State-of-the-Art-Hardwareausstattung hinaus insbesondere auf Software basierende Funktionalitäten: Sprachsteuerung, Gesichtserkennung und eine intensive Integration in das Android Ecosystem. (Kap. 7).

2012 – 2017 – Generelle Marktentwicklung

Der Markt für mobile Endgeräte ist auch seit dem Jahr 2012 nicht stehen geblieben. Große Hardware-Hersteller haben den Schritt zu Ecosystem-Orchestratoren gemacht und bieten flankierende Software, Betriebssysteme und Strukturen für Drittanbieter an. Der Markt für mobile Endgeräte ist seit dem Jahr 2008 konsequent auf diese Ecosystem-Strukturen ausgerichtet. Natürlich hat auch die Entwicklung technischer Eigenschaften nicht haltgemacht. Neue Technologien für Batterien, Chips, Displays, Kameras sowie neue Bedienkonzepte mit Fingerabdrucksensoren, Gesichts- oder Spracherkennung haben breiten Einzug in mobile Endgeräte genommen. In diesen wird auch deutlich mehr an Sensorik verbaut und eingesetzt. Gemessene Temperatur, Feuchtigkeit, Bewegung, Beschleunigung, Druck, Helligkeit, Ton/Lautstärke bieten Anwendungsfälle, die für Nutzer oder Hersteller von Interesse sind. Somit bieten moderne mobile Endgeräte dem Nutzer längere Akku-Laufzeiten, kontrastreichere und höher auflösende Displays, mehr Rechenleistung und insbesondere bessere Funktionalität – auch und insbesondere als Kamera. So verwundert es nicht, dass Smartphones längst auch hochwertige Kamerasysteme im Alltagseinsatz bei den Nutzern abgelöst haben.

2017 – Apple iPhone X

Die Vorstellung des Apple iPhone X im Jahr 2017 erregte weniger aufgrund dessen technischer Ausstattung Aufsehen. Vielmehr war der betriebswirtschaftliche Ansatz von Interesse. Mit diesem Modell hievte Apple den Einstiegspreis für diese Endgerätekategorie erstmals auf deutlich über 1000 Euro. Erste Urteile von Analysten würdigten dies zunächst kritisch, der mittelfristige Erfolg dieser Entscheidung gibt Apple Inc. – mit Blick auf die Entwicklung der Börsenkapitalisierung und der Gewinnentwicklung – nachträglich Recht (Abb. 6.27).



Abb. 6.27 Apple iPhone X, (Herstellerbild)



Abb. 6.28 Samsung Galaxy Z Flip 5G, (Herstellerbild)

2020 – Samsung Galaxy Z Flip 5G

Mit dem Galaxy Z Flip griff Samsung eine Idee aus dem 2004er Motorola Razr V3 auf: Einen Klappmechanismus, mittels dessen das Gerät bei Nichtgebrauch auf Hosentaschengröße schrumpfen konnte, während es im aufgeklappten Modus ein Display in Smartphone-Größe bot (Abb. 6.28). Das bemerkenswerte dabei war das durchgehende hochauflösende Display, welches auch im Bereich des Klappmechanismus aufgrund einer flexiblen Bauweise genutzt werden konnte. Die Entwicklung flexibler Displays geht bereits auf die ersten Jahre des aktuellen Jahrtausends zurück. Dennoch waren Endgerätehersteller viele

Jahre sehr zurückhaltend beim Einbau in Endkunden-Produkte. Weniger aus technischen Beweggründen als mehr aus Erwägungen, ob die Kunden mit solchen Displays schonend umgehen würden.

6.3 Endgeräteklassen

Aufgrund von sich unterscheidenden Anforderungen an mobile Endgeräte werden diese anders klassifiziert als Geräte im Desktop- oder Office-Segment.

6.3.1 Klassifizierungsmerkmale

Für Nutzer stehen dabei insbesondere die unmittelbar wahrnehmbaren Eigenschaften der Geräte im Vordergrund. Design- und Gestaltungsmerkmale, aber auch Beschränkungen hinsichtlich der Bedienung und Nutzung der Geräte drängen rein technische Aspekte bei der Klassifizierung manchmal in den Hintergrund.

Folgende Klassifizierungsmerkmale sind zu nennen (Auerbach und Schönher [2009](#)):

- Anschaffungskosten
- Robustheit
- Eingabeschnittstellen
- Ausgabeschnittstellen
- Kommunikation
- Mobilitätsgrad
- Leistungsfähigkeit des Akkus
- Speicherkapazität
- Betriebssystem

Die *Anschaffungskosten* unterscheiden sich von Gerät zu Gerät – teilweise immens. Dabei gilt im Prinzip, dass eine höhere Leistungsfähigkeit des mobilen Endgerätes mit einem höheren Preis einhergeht. Bei Nischenprodukten oder im Falle einer Preisdifferenzierungsstrategie des Endgeräteherstellers kann es ebenfalls zu Preisunterschieden kommen. Relevant ist dieser Aspekt für Nutzer, welche die Kostenseite von Investitionen besonders im Auge behalten.

Die *Robustheit* der mobilen Endgeräte spielt im Consumer-Segment eine wichtige Rolle, weil die Endgeräte ständig mitgeführt und genutzt werden. Besondere Anforderungen ergeben sich an die Robustheit beim beruflichen Einsatz, zum Beispiel auf Baustellen oder in Industrieanlagen. Eine Schmutz-, Feuchtigkeits- oder Temperaturresistenz ist hier oftmals gefordert. Separate Hüllen werden zum Schutz der Displays und Anschlüsse verwendet.

Die *Eingabemöglichkeiten* als zentrales Merkmal der Benutzerschnittstellen sind von großer Bedeutung. Unterschieden werden kann hier beispielsweise anhand der Ausstattung mit Stifteingabe, Joystick, physischer Tastatur, virtueller Tastatur (über Touchscreen-Displays), Sprachsteuerung oder Gestensteuerung. Bei Tastaturen wird daneben zwischen numerischen Tastaturen und vollwertigen Tastaturen (QWERTZ) unterschieden. Neue Technologien, wie die Spracherkennung oder die Steuerung per Gesten, kommen zwischenzeitlich in mobilen Endgeräten zum Einsatz und werden sicherlich die zukünftige Entwicklung der Endgeräte wesentlich beeinflussen.

Zentrale *Ausgabeschnittstelle* mobiler Endgeräte ist das Display, wobei hier unterschiedliche Technologien zur Verfügung stehen. Führende Technologien sind aktuell Organic Light Emitting Diodes (OLED) sowie Electronic Ink-Displays, die jeweils in unterschiedlichen Gerätetypen zum Einsatz kommen. Die Größe der Displays ist abhängig von der Größe des Endgerätes selbst und ist typischerweise im Bereich von 3,5 Zoll bis 13 Zoll angesiedelt. Die zweite bedeutende Ausgabeschnittstelle ist die Audioausgabe mittels integrierter Lautsprecher oder Kopfhörer.

Der *Mobilitätsgrad* mobiler Endgeräte geht umgekehrt proportional mit der Benutzerfreundlichkeit einher. Großformatige Endgeräte sind tendenziell komfortabel zu bedienen aber schwerer zu transportieren. Kleine Geräte sind leicht transportabel, weisen aber Nachteile in der Benutzerfreundlichkeit auf. Technologien wie die Spracherkennung können diese umgekehrte Proportionalität in Teilen aufheben.

Eng verbunden mit dem Format eines mobilen Endgerätes ist auch die *Leistungsfähigkeit* des Akkus für die mobile Stromversorgung. Hier gilt, dass größere Gehäuse neben größeren Displays insbesondere den Einbau stärkerer Akkus ermöglichen. Größter Stromverbraucher in mobilen Endgeräten ist jedoch das Display. Insofern beschneidet der Einbau größerer Displays gleichzeitig auch die Laufzeit. Moderne Akku-Technologien weisen im Vergleich zu ihren historischen Vorgängern eine deutlich verlängerte Gesamtlebensdauer auf. Entsprechend sind einige Endgerätehersteller dazu übergegangen, Akkus fest, d. h. nicht austauschbar, in die Endgeräte zu verbauen.

Entsprechend dem Trend im Bereich des Desktop-Computing werden auch in mobilen Endgeräten von Generation zu Generation leistungsstärkere CPUs eingebaut. Mehrprozessortechnologien haben Einzug gehalten, während gleichzeitig der Stromverbrauch der CPUs gesenkt werden konnte. Endgerätehersteller nutzen die Möglichkeiten, welche durch die fortschreitende Miniaturisierung der Bauteile gegeben sind. Ergänzend werden zwischenzeitlich auch in mobilen Endgeräten separate Chips für die Grafikverarbeitung z. B. für Mobile Games verbaut.

Die Leistungssteigerung der mobilen Endgeräte heutiger Generation kann auch an der Größe des verfügbaren *Speicherplatzes* – meist in Form elektronischer Speicher – abgelesen werden. Typische Daten, die hier durch die Nutzer verwendet werden, sind Musik und Videos, Dokumente sowie Software-Anwendungen.

6.3.2 Geräteklassen

Im Bereich der mobilen Endgeräte werden unterschiedliche *Geräteklassen* unterschieden. Neben den aktuell stark präsenten Smartphones, welche das Endkundensegment derzeit dominieren, werden weitere Klassen im Folgenden betrachtet:

- Feature Phones
- Personal Digital Assistants
- Smartphones
- Tablets
- Ultra Mobile PCs
- Netbooks/Subnotebooks
- Laptops
- Wearables
- Special Devices

Von *Feature Phones* wird gesprochen, wenn klassische mobile Endgeräte gemeint sind, d. h. Endgeräte, die mit einer numerischen Tastatur und einem vergleichsweise kleinen Display ausgestattet sind. Sie ermöglichen eine grundlegende Nutzung der Mobilkommunikation, insbesondere die Sprachtelefonie sowie das Versenden von Kurznachrichten. Darüber hinaus sind sie üblicherweise mit rudimentärer Software bestückt, so beispielsweise Kalender oder Wecker sowie einem Adressbuch.

Personal Digital Assistants (PDA) waren ursprünglich als Geräte zur Verwaltung persönlicher Daten, insbesondere Termine, Kontakte, Aufgaben und Notizen, gedacht. Dazu sind sie üblicherweise mit einer QWERTZ-Tastatur und einem vergleichsweise größeren Display ausgestattet. In der Vergangenheit, d. h. bis in die ersten Jahre dieses Jahrhunderts war das Unternehmen Palm Inc. in diesem Segment mit Abstand Markt- und Technologieführer. Nach einer Reihe von unglücklichen strategischen Entscheidungen hat das Unternehmen diese Marktstellung zwischenzeitlich völlig verloren.

Palm war mit Nokia marktführend, als die Klasse der *Smartphones* auf den Markt gebracht wurde. Ursprünglich aus der Konvergenz von Feature Phone und PDA hervorgegangen wird zwischenzeitlich von einem Smartphone gesprochen, sofern ein mobiles Endgerät mit einem Display von mindestens 3,5 Zoll, einer leistungsfähigen Hardware-Ausstattung sowie einer vollwertigen Tastatur (über ein Touchscreen-Display oder mittels physischer Tasten realisiert) ausgerüstet ist. Wesentliches Charakteristikum eines Smartphones ist jedoch der Einsatz eines Highend-Betriebssystems (z. B. Apple iOS oder Android OS).

Die Klasse der *Tablets* bildet den Übergang zu den PC-Unterklassen der mobilen Endgeräte. Durchbruch für diese Gerätekategorie war der Erfolg des Apple iPad, welches im Jahr 2010 auf dem Markt eingeführt wurde (auch wenn vorher schon Vorläufer anderer Hersteller

ler auf dem Markt existierten). Es handelt sich bei Tablets um flache Endgeräte, die typischerweise mit Touchscreen-Display und ohne physische Tastatur ausgerüstet werden. Die Bedienung erfolgt mittels Finger oder Eingabestift. Sowohl die Leistungsfähigkeit wie auch die Größe der Geräte liegt deutlich über denen der Smartphones. Auch im Segment der Tablets haben sich die Betriebssystem-Pendants der entsprechenden Smartphone-Systeme durchgesetzt, so dass hier keine Differenzierung mehr erfolgt.

Ultra Mobile PCs werden ebenfalls der Klasse der Tablets zugerechnet, jedoch sind diese zusätzlich mit einer physischen Tastatur ausgestattet und nutzen traditionelle Desktop-Betriebssysteme, insbesondere Windows.

Netbooks, *Subnotebooks* und *Laptops* sind mobile Versionen klassischer Desktop-PCs, welche sich letztlich nur in der Größe unterscheiden. Die beiden erstgenannten zeichnen sich dabei durch eine geringere Gehäuse- und Displaygröße aus.

Deutlich kleiner fallen üblicherweise die *Wearables* aus. Hierzu zählen alle Endgeräte, die unmittelbar am Körper oder in Kleidung integriert getragen werden. Typische Beispiele sind Fitness-Armbänder oder Smartwatches, deren Einführung im Segment der klassischen Uhrenhersteller zu empfindlichen Umsatzeinbußen geführt haben.

Sonderbauformen mobiler Endgeräte sind typischerweise besonderen Anforderungen in bestimmten Einsatzumgebungen folgend entstanden. So gelten beispielsweise für den Einsatz in Krankenhäusern spezielle Anforderungen an technische Geräte (Reinigung, Funkentstörung, etc.). Auch für den Einsatz im Outdoor-Bereich, z. B. auf Baustellen gelten besondere Anforderungen für mobile Endgeräte (Robustheit, Wasserdichte, etc.). Daneben werden Sonderbauformen für den Einsatz in Maschinen genutzt. Beispielhaft sei die Installation von Modulen in Verkaufsautomaten (Süßigkeiten, Tabakwaren, etc.) genannt. Ein SIM-Modul ist hier für die automatisierte Benachrichtigung des Außendienstes zwecks Nachfüllung bei anstehendem Abverkauf einzelner Artikel zuständig. SIM-Module finden sich mittlerweile in vielen technischen Geräten und Bauteilen. Es wird daher auch von der Möglichkeit der Machine-to-Machine-Kommunikation (M2M) gesprochen. Diese ist Bestandteil vieler sogenannter Internet-of-Things (IoT)-Anwendungen (Abschn. 6.5).

M2M-Endgeräte unterscheiden sich nicht nur bezüglich der Bauformen von herkömmlichen Feature- oder Smartphones. In der Regel werden zwischen kommunizierenden Geräten keine hochauflösenden Bilder ausgetauscht; die Kommunikation beschränkt sich auf kompakte Datenpakete mit Steuer- und Zustandsdaten. Entsprechend steht die erzielbare Datenrate im Hintergrund. Wichtig ist dagegen die Batterie-Laufzeit, die teilweise bis zu 10 Jahre mit einem Satz handelsüblicher AA-Batterien betragen muss (GSM Association 2016). Aus diesem Grund wird auf Displays weitestgehend verzichtet. Die Chipsätze verwenden gemeinsame Schaltkreise zum Senden und Empfangen, was zu einem sogenannten Halb-Duplexbetrieb führt. Die für den M2M-Betrieb entwickelten Protokolle sehen zusätzlich sogenannte Power-Save-Modi für den Betrieb vor, bei denen das Endgerät sich in einen Ruhemodus setzt, aus dem es nur periodisch erwacht, um die Erreichbarkeit zu gewährleisten.

6.4 Mobile Betriebssysteme

Mobile Endgeräte als kleine Computersysteme benötigen ein entsprechendes Betriebssystem zum Betrieb. Typische Funktionalitäten sind hierbei:

- Touchscreen-Bedienung
- Steuerung der Funkschnittstellen (Mobilfunk, WiFi, Bluetooth, RFID/NFC)
- GPS Navigation
- Gyroskop, d. h. ein Sensor, mit dem sich die genaue Lage bestimmen lässt, wird oft allerdings simuliert aus den GPS-Daten
- Kamera
- Spracherkennung
- Bilderkennung, einschließlich Barcode und QR-Code Erkennung
- Multimedia
- Aufruf und Nutzung von mobilen Anwendungen (Apps)

Meilensteine in der Entwicklung der Betriebssysteme für mobile Endgeräte waren die folgenden:

- bis 1992: proprietäre Embedded Systems
- 1996: Palm OS
- 1996: Windows CE
- 2000: Symbian
- 2002: BlackBerry OS
- 2005: Maemo OS
- 2007: Apple iPhone OS
- 2008: Android
- 2009: Palm webOS
- 2009: Bada OS
- 2010: Apple iOS
- 2010: Windows Phone
- 2011: MeeGo

Derzeit dominieren am Markt zwei Ecosystems (Kap. 7), welche sich um einzelne Betriebssysteme für mobile Endgeräte als dazugehöriger Plattform etabliert haben. Die bedeutsamen Betriebssysteme im Endverbrauchersegment werden im Folgenden kurz dargestellt.

6.4.1 Apple iOS, iPadOS, watchOS, tvOS

iOS, welches bis Mitte 2010 als iPhone OS bezeichnet wurde, ist das Basis-Betriebssystem der Produkte des Herstellers Apple. Die enge Einbindung in das iOS-Ecosystem wird

durch eine Integration mit Apple Software-Produkten (z. B. Musik, Film oder Literaturbibliotheken) forciert und beinhaltet somit auch den Apple AppStore, als ersten kommerziell erfolgreichen App Store. Der AppStore ist für den Nutzer die zentrale Anlaufstelle zum Erwerb von Software. Ein Qualitätssicherungs-Konzept gibt dem Nutzer eine hohe Gewähr, dass die erworbenen Apps frei von Schad-Software sind. Gleichzeitig sichert das AppStore-Prinzip Apple die Kontrolle über die verwendete Software und generiert ein beträchtliches Einkommen aus dem Provisionsanteil der Einnahmen. Das ursprüngliche Betriebssystem iPhone OS wurde in seiner ersten Version im Januar 2007 parallel zum neu erschienenen Endgerät iPhone vorgestellt. Der Betriebssystem-Kern ist eine Portierung des quelloffenen UNIX Betriebssystems Darwin auf die verwendeten ARM-Prozessoren. Das gesamte proprietäre Betriebssystem iOS wurde aus dem auf dem gleichen Kern basierenden Mac OS X entwickelt.

Die ursprüngliche Umbenennung in iOS erfolgte aufgrund der Erweiterung der Produktpalette um die ebenfalls mit diesem Betriebssystem bestückten Tablet-Modelle. Für die Bezeichnung wurde es notwendig, dass Apple den Markennamen von Cisco Systems lizenzierte. Letztere hat seit den 1980er-Jahren die Namensrechte für das Internetwork Operating System (IOS), welches in Routern und Switches zum Einsatz kommt. Die an Apple vergebene Lizenz bezieht sich nur auf den Namen iOS. Mit der Ausweitung der Nutzung der Betriebssystem-Plattform auf die Smartwatches und AppleTV-Geräte des Herstellers erfolgte später eine Aufgliederung der Betriebssysteme in die Sparten iOS, iPadOS, watchOS und tvOS, die jeweils einen spezielleren Zuschnitt auf die technischen Eigenarten der jeweiligen Geräte bieten. Apple hat sich damit von der lang vorherrschenden Grundidee gelöst, dass ein Betriebssystem für verschiedene Endgeräte-Klassen verwendet werden soll.

Den Funktionsumfang des Betriebssystems ergänzt Apple über die Zugabe bereits vorinstallierter Anwendungen, sogenannter Apps. Dabei handelt es sich insbesondere um den Internet-Browser Safari, das E-Mail-Programm Mail, ein Kalenderprogramm, ein Adressbuch, eine Kamera-Applikation zur Erstellung von Fotos und Videos, eine Foto-Verwaltung sowie mobile Versionen von Multimedia-Software zum Erwerb und zur Nutzung von Medieninhalten. Neben diesen erlangt die AppStore-Anwendung zum Kauf weiterer Programme besondere Bedeutung. Sie bietet die einzige im Betriebssystem vorgegebene Schnittstelle zur Erweiterung durch Anwendungen. Je nach Endgerät finden sich weitere vorinstallierte Anwendungen, beispielsweise beim iPhone die Möglichkeit zum Telefonieren und Senden von Kurznachrichten.

Die Bedienung des Apple-Betriebssystems ist auf die Nutzung der verbauten Touchscreen-Displays ausgelegt (Ausnahme AppleTV). Diese ermöglichen Multi-Touch-Gesten und erweitern damit das Interaktionsspektrum für den Nutzer. Bestimmte Fingerbewegungen auf dem Display lösen dabei Aktionen aus. So bewirkt das Auseinanderziehen von zwei Fingern den Zoom in ein Bild oder eine Internetseite. Scrollen erfolgt über das Ziehen eines Fingers über den Bildschirm. Eine Drehbewegung mit zwei Fingern auf dem Touchscreen-Display führt zu einer Rotation des angezeigten Inhaltes, z. B. eines Bildes. Das User-Interface und die auf einfache Gestaltung und Nutzung ausgelegten

Design-Prinzipien, welche implementiert wurden, werden immer wieder als größter Erfolgsgarant der Apple-Endgeräte genannt. Wie bei Touchscreen-Displays üblich simuliert der Finger keinen Mauszeiger, sondern ermöglicht die unmittelbare Eingabe von Informationen zur Interaktion mit dem Gerät. Das von Desktop-PCs bekannte Eingabeprinzip des „Point and Click“ wird mit der Verwendung von Touchscreen-Displays aufgegeben. Die Unterscheidung zwischen Zeigen und Klicken entfällt.

Das Betriebssystem sieht mittlerweile für die Eingabe von Text auch eine Texterkennung von handschriftlichen Bewegungen auf dem Display vor. Üblicherweise wird bei Bedarf jedoch eine virtuelle Tastatur auf dem Display eingeblendet. Da die von Apple verbauten Displays bis zu zehn unterschiedliche Berührungsstellen gleichzeitig erfassen können, erreichen geübte Schreiber Geschwindigkeiten, die an die Bedienung einer physischen Tastatur durchaus heranreichen. Da die Größe der Displays keine vollständige Abbildung einer PC-Tastatur erlaubt, besteht die virtuelle Tastatur aus mehreren Ebenen (Layer), zwischen welchen über (virtuelle) Sondertasten umgeschaltet werden kann. Funkschnittstellen (Bluetooth) ermöglichen den Anschluss einer physischen Tastatur für die Texteingabe. Einzelne Elemente für die Gestaltung der Benutzeroberfläche von Anwendungen werden über das Software Developer Kit (SDK) durch Apple bereitgestellt.

In mobilen iOS-Endgeräten sind Neigungssensoren verbaut, so dass je nach Anwendungen und Haltung des Geräts zwischen Quer- oder Hochformat der Bildschirmsicht umgeschaltet werden kann. Das iOS-Betriebssystem unterstützt daneben die Ermittlung der Lage und Beschleunigung des Endgerätes über ein eingebautes Gyroskop. Dieses Element findet insbesondere in Mobile Games Verwendung, wird aber auch von Fitness Apps zum Erfassen körperlicher Aktivitäten (Schrittzähler) genutzt. Auch Aspekte der Barrierefreiheit sind in den Betriebssystemen berücksichtigt, beispielsweise über VoiceOver oder Farbinvertierungen. Bei Voiceover wird eine Stimme/Übersetzung über eine andere Tonaufnahme oder einen aufgerufenen Text gelegt. Farbinversion bedeutet eine Umkehr der Farben, z. B. von Schwarz auf Weiß. Hierdurch kann z. B. bei starker Sonneneinstrahlung ein schwarzer Text auf weißem Hintergrund in einen weißen Text vor schwarzem Hintergrund umgewandelt werden.

In aktuellen Versionen ermöglichen die Betriebssysteme Multitasking anhand definierter Programmierschnittstellen:

- Hintergrund-Audio
- IP-Telefonie
- Hintergrund-Ortung
- Push-Benachrichtigungen
- Lokale Benachrichtigungen
- Beendigung eines laufenden Prozesses im Hintergrund
- Schnelles Wechseln von Apps

Kritik an den Betriebssystemen zeigt sich im Wesentlichen an der Zugangsbeschränkung für Anwendungsentwickler und der damit verbundenen Abschottung des Ecosystems. Im

Zentrum steht dabei der zentralisierte Prozess der Zulassung von Apps und der vorgesetzten Prüfung durch Apple. Jede App muss durch den Entwickler zur Prüfung eingereicht werden. Die Prüfung durch Apple umfasst sowohl Code-Segmente als auch Inhalte. So unterliegen beispielsweise Erotik-Angebote strengen Prüfungsvorschriften. Nach der Prüfung erfolgt die Freischaltung für den AppStore oder eine Ablehnung mit einer kurzen Begründung. Dieser Prüfungsprozess wird andererseits auch als positiv angesehen, da Nutzer jeweils davon ausgehen können, dass eine App keine Schadsoftware und keine nicht-jugendfreien oder gewaltverherrlichenden Inhalte beinhaltet (was jedoch oftmals subjektiver Wahrnehmung unterliegt). Dennoch fühlen sich Nutzer durchaus durch die von Apple getroffenen Einschränkungen bevormundet und stören sich an der Kontrolle, welche Apple über die Betriebssystem-Plattform hat. Die Verbannung der Flash-Technologie aus dem ursprünglichen iPhone OS-Betriebssystem aufgrund des großen Energieverbrauchs Flash-basierter Anwendungen hat seinerzeit zu einer beschleunigten Verbreitung moderner Webtechnologien wie HTML5 geführt.

6.4.2 Android OS

Android OS ist ein Betriebssystem für mobile Endgeräte, welches von der Open Handset Alliance entwickelt wird. Stärkster Treiber der Entwicklung und Verbreitung ist der Internet-Konzern Alphabet mit seiner Tochter Google. Basis der Entwicklung ist der Linux-Kernel, entsprechend handelt es sich bei Android um freie Software, die quell offen entwickelt wird. Aktuell ist Android das am weitesten verbreitete mobile Betriebssystem. Es wies hinsichtlich seiner Verbreitung lange Zeit die größten Wachstumsraten auf. Seit einigen Jahren sind die Marktanteile bei Neuzulassungen von Endgeräten weitestgehend konstant.

Die Entwicklung von Android begann ursprünglich nicht unter dem Dach des Alphabet-Konzerns, sondern im 2003 von Andy Rubin gegründeten Unternehmen Android. Dort wurde die Entwicklung eines Betriebssystems für mobile Endgeräte sowie von ortsbasierten Diensten betrieben. Die Übernahme durch Google erfolgte im Sommer 2005. Kurz nach der Vorstellung des iPhone OS durch Apple im Jahr 2007 machte Google das Vorhaben bekannt, gemeinsam mit 33 anderen Mitgliedern der Open Handset Alliance ein Betriebssystem für mobile Endgeräte zu entwickeln. Seit Herbst 2008 ist Android am Markt verfügbar. Inzwischen ist eine große Anzahl unterschiedlicher Geräte von diversen Herstellern mit dem Android Betriebssystem ausgestattet.

Auch Android sieht die Bedienung der mobilen Endgeräte mittels Touchscreen-Display vor, erlaubt den Endgeräteherstellern aber auch den Einsatz physischer Tasten und Tastaturen. Das grafische Design und die Funktionalität des Betriebssystems sind vergleichbar zu den Betriebssystemen von Apple. Die Open Handset Alliance hat jedoch Freiräume für die einzelnen Endgerätehersteller hinsichtlich der Gestaltung der grafischen Bedienelemente und der Benutzeroberfläche vorgesehen. So kann jeder Endgerätehersteller die zur Produktdifferenzierung notwendigen Innovationen auf Android basie-

rend entwickeln und mit dem Betriebssystem verbinden. Dies führt dazu, dass die Bedienoberflächen so unterschiedlich gestaltet sind, dass der Rückschluss auf Android als Basissystem manchmal nicht leichtfällt. Entstandene Innovationen werden häufig in Folgeversionen des Android-Betriebssystems übernommen, so dass ein fortwährender Innovationszyklus angeregt wird.

Google als führendes Mitglied in der Open Handset Alliance integriert in das Android Betriebssystem Schnittstellen zum Erwerb von Multimedia-Inhalten oder ergänzenden Anwendungen. Diese wurden im Frühjahr 2012 unter der Oberfläche Google Play vereint. Google Play ersetzte die bisherige Bezeichnung Android Market. Android setzt im Gegensatz zu iOS nicht auf einen zentralen Marktplatz für Inhalte für mobile Geräte. So entstanden neben Google Play auch andere, in Konkurrenz stehende Marktplätze wie beispielsweise SlideME, GetJar, herstellerspezifische Stores wie der Samsung Galaxy-Store oder auch der Amazon Appstore. Je nach Marktplatzbetreiber erfolgt auch bei Android eine Prüfung der eingereichten Anwendungen hinsichtlich der Programmierung (Schadsoftware) und der angebotenen Inhalte. Hier greifen die entsprechenden Pro- und Contra-Argumente wie auch bei den Betriebssystemen von Apple.

Das Android Betriebssystem ist in weiten Teilen eine freie Software. Der größte Teil steht unter der Apache-Lizenz; Ausnahmen sind der Kernel, welcher unter General Purpose Licence (GPL) vertrieben wird sowie einzelne native Anwendungen, deren Quelltext nicht verfügbar ist. Android OS-Versionen trugen neben einer Versionsnummer längere Zeit ergänzend den Namen einer Süßspeise, deren Anfangsbuchstaben jeweils im Alphabet aufsteigend war. Die Version 4 wurde mit „Ice Cream Sandwich“ bezeichnet. Vorläufer waren „Gingerbread“ (Version 2), eine Version, die nur für Smartphones entwickelt wurde, und „Honeycomb“ (Version 3), einer Version für Tablets. Die Trennung zwischen diesen Geräteklassen wurde mit „Ice Cream Sandwich“ aufgegeben, welches von Grund auf für beide Systeme vorgesehen ist. Folgende Codenamen der Versionen umfassten Titel wie „KitKat“, „Lollipop“, „Marshmallow“, „Nougat“, „Oreo“ oder „Pie“. Mit Version 10 des Betriebssystems wurde die Namensgebung aufgegeben.

Der Google Play Store ist aktuell der am schnellsten wachsende Marktplatz für digitale Güter. Darüber ist die Erweiterung des Anwendungsspektrums der mobilen Endgeräte möglich. Von Hause aus liefert Android eine geringe Anzahl an Anwendungen aus, darunter z. B. einen Webbrowser, eine Kartenanwendung, eine SMS-, E-Mail- und Adressbuchverwaltung, die Möglichkeit zum Abspielen von Multimediadaten, eine Kameraanwendung sowie eine Fotoverwaltung. Zusätzliche Anwendungen können über eine Reihe von Programmierschnittstellen mit dem Android-Betriebssystem sowie weiteren Anwendungen interagieren. Softwareentwickler haben die Wahl zwischen verschiedenen Alternativen zum Play Store, jedoch sind Netzwerkeffekte zu erkennen, die deutlich machen, dass für viele Entwickler der Marktplatz von Google erste Wahl zum Vertrieb der eigenen Produkte ist. Eine zwingende Bindung der Endkunden ein Nutzerkonto bei Google (mit der entsprechenden Einrichtung ausgewählter Dienste) zu eröffnen war nur in der Marktein-

führungsphase von Android gegeben. Die Nutzung von Google Play setzt dies jedoch weiterhin voraus.

Der Marktanteil von Android-Geräten ist weiterhin sehr stark, nachdem bereits frühzeitig andere Mitbewerber überholt wurden. Dennoch ist die reine Betrachtung des Marktanteils im Falle von Android wenig aussagekräftig. Auch wenn Android den ersten Platz in den entsprechenden Analysen belegt, zeigt sich in der Praxis, dass bei den Endkunden unterschiedliche Versionen des Betriebssystems im Einsatz sind. Android schafft es derzeit noch nicht, seine Nutzer zum regelmäßigen Update des Betriebssystems zu bewegen. Daneben entscheiden sich viele Endgerätehersteller dafür, selbst wenige Monate alte Endgeräte nicht mit den aktuellsten Versionen des Betriebssystems zu versorgen, so dass auch hier die Endkunden auf Vorgängerversionen verharren. Kritisch ist dies insbesondere mit Blick auf die Möglichkeiten der Anwendungsentwickler zu betrachten. Aufgrund der starken Zersplitterung des Marktanteils von Android auf unterschiedliche Versionsstände des Betriebssystems wird der Entwicklungsprozess für Applikationen verlangsamt. Daneben kann ggfs. nicht der durch die neueste Version des Betriebssystems angebotene Funktionsumfang als gegeben vorausgesetzt werden. Dies zeigt sich aktuell als größte Herausforderung. Apple hat hier aufgrund der Konzentration auf nur wenige hauseigene Endgeräte und die starke Fokussierung auf das eigene Ecosystem einen gewissen Vorteil. Dennoch bietet die Open Handset Alliance mit Android OS vielen Hardware-Herstellern eine nicht zu unterschätzende Gelegenheit, mit den Produkten von Apple Inc., die sich durch die oben erläuterte Denkweise „von den Diensten kommend“ auszeichnet, in den Wettbewerb zu treten. Die Fragmentierung des Marktes macht eine Steuerung entsprechend schwieriger.

Die bestehenden Freiräume für Lizenznehmer des Android-Betriebssystems, dieses nach eigenen Vorstellungen anzupassen, führt in der Praxis zu Schwierigkeiten bei der Versorgung einzelner Gerätemodelle mit Updates. Zwischen Endkunde und Endgerätehersteller besteht keine vertragliche Verpflichtung, aus der sich für den Hersteller eine Anforderung zur Aktualisierung der Software ergäbe. Der Hersteller ist durch den Kauf des Gerätes nur zur Sicherstellung des einwandfreien Betriebs im Auslieferungszustand verpflichtet. Auf Kundenseite führte dies in der Vergangenheit oftmals zu einer gewissen Unzufriedenheit.

6.5 Endgeräte für Maschine-zu-Maschine und Kritische Kommunikation

In den letzten Jahren hat sich ein separater Markt für professionelle Endgeräte in den beiden Bereichen M2M und Kritische Kommunikation entwickelt. Unter „Kritischer Kommunikation“ wird die Kommunikation in gesicherten Umgebungen durch Einsatzkräfte in Notfällen und kritischen Situationen verstanden. Das Anwendungsszenario umfasst staat-

liche Funktionen (Behörden mit Organisations- und Sicherheitsaufgaben und privatwirtschaftlichen Bereiche der Überwachung, Steuerung und Instandsetzung von Infrastruktur der Energieversorgung.

6.5.1 Kritische Kommunikation

Das typische Endgerät für Notfallkommunikation ist das „*Push-to-Talk*“-Gerät. Es ist auf die Bedürfnisse der Einsatzkräfte im professionellen Service-Bereich, sowie in Katastrophen- und Notfallsituationen zugeschnitten, benötigt auf der Netzseite aber entsprechende Infrastruktur zur Nutzung der spezifischen Eigenschaften. Die professionelle Lösung Mission Critical Push-to-Talk (MCPTT) zur Krisen- und Notfallkommunikation baut auf dem in den 2000er-Jahren unter jungen Nutzern von Mobilfunk vor allem in den USA beliebten Dienstes Push-to-Talk (PTT) auf. PTT stellte über Mobilfunknetze einen Betrieb im Stil von Handfunkgeräten („Walkie-Talkie“) zur Verfügung. Dabei waren niedrige Gebühren, Gruppenruf und sehr schneller Rufaufbau ohne Wahlvorgang zentrale Features. Durch Knopfdruck konnte eine Verbindung hergestellt werden. Die Kommunikation erfolgte im Halbduplex-Modus: Es konnte immer nur ein Teilnehmer sprechen, alle anderen hörten zu. Bei der Entwicklung von MCPTT wurde diese Grundfunktion durch eine Reihe von zusätzlichen Features erweitert:

- Eine Dispatch-Funktion, mit der Administratoren Gruppenbildung, Rechtevergabe und andere Verwaltungsfunktionen in großen Organisationen in Echtzeit durchführen können.
- Verschlüsselte Kommunikation zum Schutz gegen unbefugtes Mithören („Polizeifunk“)
- Qualitativ hochwertige Sprache durch Voice over IP oder VoLTE
- Optionen zur Übertragung von Medien (Bilder, Videos, Tondokumente)
- Netz- und Netztechnologie-übergreifende Lösung

Verschiedene Anbieter haben Endgerätelösungen für MCPTT entwickelt. Einige Namen von spezialisierten Herstellern sind RugGear (Kanada, Abb. 6.29) oder Funkwerk (Deutschland). Auch große Hersteller von Smartphones sind in diesem Markt aktiv. Zum Beispiel bietet Samsung das Xcover FieldPro an (Abb. 6.30). Allerdings fehlt hier die Unterstützung der wichtigen LTE-Bänder 31 und 72 im 450 MHz-Bereich, die international oft für die kritische- und Notfallkommunikation zugeteilt werden. Die Geräte unterscheiden sich deutlich von Mobiltelefonen oder Smartphones. Zur Ausstattung gehören zum Beispiel

- Programmierbarer Push-to-Talk-Button, mit dessen Hilfe Verbindungen in wechselnden Einsatzgruppen schnell aufgebaut werden können.
- Ein separater Notfall-Knopf zum dedizierten Absetzen eines Notrufes
- Ein starker interner Lautsprecher (> 100 dB) zum deutlichen Hören von Nachrichten oder Kommandos im Hands-free Betrieb in lauten Umgebungen.



Abb. 6.29 RugGear RG530 MCPTT Phone im Einsatz und als Draufsicht mit SOS-Button, (Herstellerbild)



Abb. 6.30 Samsung Xcover Field Pro mit MCPTT-Unterstützung, (Herstellerbild)

- Ein Anschluss für Steckverbindungen zu peripheren Geräten, wie zum Beispiel Lautsprecher
- Zertifizierte Standards für Widerstandsfähigkeit bei äußerer Bedingungen (z. B. Staub/Wasser IP68 oder IP69, Stoßfestigkeit und militärische Robustheits-Standards)
- Ausdauernde, auswechselbare Batterie mit Standby-Zeiten von 10 Tagen und mehr
- Betrieb bei Außentemperaturen von -10 Grad bis +50 Grad
- Verschiedene Ladeverfahren (USB-C, induktive Kopplung)

Die aktuellen Geräte besitzen meist ein Android-Betriebssystem. Sie unterstützen verschiedene Funkschnittstellen, von GSM über WCDMA bis LTE, und künftig auch 5G. Bei LTE sind sie auch kompatibel zu den Notfall-Frequenzen in den LTE-Bändern 31 und 72 im 450 MHz-Bereich. Gegenüber gebräuchlichen Smartphones weisen sie ein kleineres, niedriger auflösendes Display auf, das jedoch auf gute Lesbarkeit unter schwierigen Lichtverhältnissen optimiert ist.

Viele dieser Geräte sind auch in normalen Netzen einsatzfähig, weisen aber dort keine besonderen Qualitäten auf. Umgekehrt können moderne Smartphones durch eine Push-to-Talk-App zumindest an der MCPTT Gruppenkommunikation teilnehmen. Motorola bietet die App WAVE an, mit der jedes Android-Smartphone als MCPTT Terminal genutzt werden kann. Dabei verzichtet der Anwender allerdings auf die spezifischen Feld-Leistungsmerkmale für den Notfall-Einsatz.

6.5.2 Internet of Things

Bei der M2M-Kommunikation spielen viele, für die Nutzer wichtigen Features keine Rolle. Kommunikation zwischen Maschinen wird in der Regel protokoll- und datenbasiert geführt. Es handelt sich bei den Endgeräten in der Regel um Komponenten wie Sensoren oder Aktoren, die in eine M2M-Lösung eingebettet werden. Die aktuellen Komponenten der Hersteller unterstützen multiple Standards, von GSM bis LTE und 5G, inklusive der Optionen LTE-M und NB-IoT, sowie die nicht lizenzierten Netzwerk-Standards LoRaWAN und SigFox. Dies erlaubt eine flexible Verwendung in verschiedenen Netzwerk-Umgebungen.

Der Fokus liegt auf Energie-Effizienz. Insbesondere bei batteriebetriebenen Geräten ist die industrieweite Forderung nach Laufzeiten bis zu 10 Jahren mit einer AA-Batterieladung zu erfüllen. Zum Beispiel wird im Halb-Duplex-Modus auf zwei getrennte Schaltungen für Sendung und Empfang verzichtet. Die Geräte empfangen und senden auf der vom jeweiligen Standard vorgesehenen Bandbreite. Je breiter das unterstützte Band, desto höher ist der Energieverbrauch auch im Empfangsmodus. Unterstützt werden die von den Standards angebotenen Energiesparoptionen Power Saving Mode und Discontinuous Reception, die lange Kommunikationspausen ohne Signalaustausch bei fortgesetzter Anmeldung am Netz erlauben. In der Regel besitzen diese Modems serielle Schnittstellen nach Industriestandard (UART), Analog-Digital-Wandler (ADC), sowie einen General Purpose

Input-Output (GPIO), sowie einen Slot für eine SIM-Karte bzw. ein eSIM Modul, und können so mit den verschiedensten Mikrocontroller-Architekturen verbunden werden. Integrierte GNSS-Lösungen sind ebenfalls erhältlich; der Betrieb von GPS führt aber zu einer deutlichen Erhöhung des Stromverbrauchs. In Kombination mit den Sensortechnologien in Tab. 6.2 lassen sich eine Vielzahl von IoT-Lösungen erstellen. Modems zum Einbau in Endgeräte werden von einer Reihe von Herstellern angeboten, bekannt sind Sierra Wireless, U-Blox, Telit oder Quectel. Abb. 6.31 zeigt als Beispiel ein Produkt von Sierra Wireless.

Smart Meter Gateways sind digitale Stromzähler mit einer Anbindung an eine Zentrale über ein Kommunikationsnetz. Im Bereich des IoT sind sie der Anwendungsfall mit dem größten erwarteten Wachstum. Eine Energiewende mit erneuerbaren Energiequellen und einer Vielzahl von Verbrauchern, zum Beispiel für die E-Mobilität, ist ohne eine genaue Überwachung der Netze kaum zu realisieren. Smart Meter Gateways sind in der Nähe der Verbraucher angebracht und melden regelmäßig Verbrauchsdaten. Dadurch wird die laufende Beobachtung des Versorgungsnetzes und die Erkennung von kritischen Netzzuständen ermöglicht. In weitergehenden Lösungen sind auch Steuerungsmöglichkeiten denkbar. Die Anforderungen an Smart Meter Gateways werden vom Bundesamt für Sicherheit in der Informationstechnik (BSI) festgelegt. Dazu gehören technische Richtlinien und Sicherheitsanforderungen wie etwa die Verschlüsselung der Tarifdaten während der Übertragung. Seit der Allgemeinverfügung des BSI im Februar 2020 können Smart Meter Gateways in Deutschland installiert und betrieben werden. Die Netzanbindung kann sowohl über das Festnetz als auch über Mobilfunknetze erfolgen. Mobilfunknetze haben dabei den Vorteil, dass sie mit batteriebetriebenen Endgeräten unabhängig von der Stromversorgung und Netzanbindung vor Ort sind. Bedingung für diesen Einsatz sind ein geringer Energieverbrauch und eine gute Gebäudedurchdringung der verwendeten Wellen. Die Lösungen LTE-M und NB-IoT bieten sich hier sowohl im Rahmen der öffentlichen Mobilfunknetze als auch auf dedizierten Frequenzbändern an. Die Lizenz für das ehemalige Frequenzband des C-Netzes im 450 MHz-Bereich wurde zu diesem Zweck von der Bundesnetzagentur 2021 an einen Spezialnetz-Betreiber vergeben, hinter dem ein großer Teil der deutschen Energiewirtschaft steht.

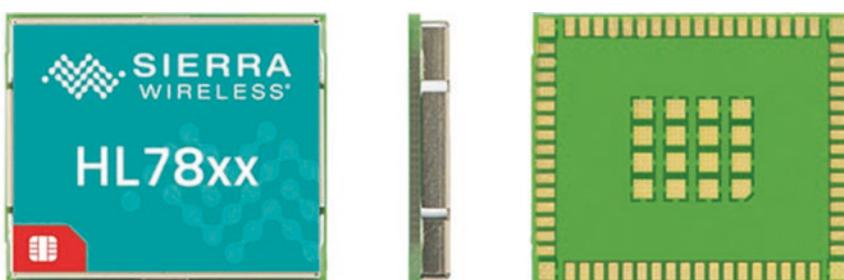


Abb. 6.31 IoT Modem HL78xx von Sierra Wireless, Vorder-, Seiten- und Rückansicht (Herstellerbild)

Tab. 6.1 Die wichtigsten Tarifanwendungsfälle für Smart Meter Gateways

| TAF-Nr | Bezeichnung des Tarifs | Beschreibung |
|--------|-------------------------|--|
| 1 | Datensparsame Tarife | Bei diesen Tarifen erfolgt eine Übertragung pro Abrechnungszeitraum (z. B. 1 Monat). Es sollen keine Rückschlüsse auf Verbrauchsverhalten ermöglicht werden. |
| 2 | Zeitvariable Tarife | Ermöglicht zeitabhängige Tarife, z. B. mit niedrigen Gebühren in den Nachtstunden |
| 6 | Abruf bei Bedarf | Ermöglicht Energieversorgern in nicht planbaren oder Ausnahmesituationen Verbrauchsdaten abzurufen. Das Smart Meter Gateway (SMGW) speichert dazu die Messwerte einer Periode (z. B. 6 Wochen) ab, die bei Bedarf abgefragt werden können. |
| 7 | Zählerstandsgangmessung | Anwendungsfall zur Kontrolle des Stromzählers. Während eines Intervalls von 15 Minuten werden laufend Daten übertragen. Es können neben Verbrauchswerten auch Einspeisewerte übertragen werden (Fotovoltaik). |

Abb. 6.32 Smart Meter

Gateway des Herstellers Power Plus Communications,
(Herstellerbild)



Die Funktionsumfänge werden vom BSI in Form von Tarifanwendungsfällen (TAF) festgelegt. Es sind insgesamt 14 solche TAF definiert; die aktuell im Einsatz befindlichen sind in Tab. 6.1 zusammengefasst.

Das LTE Smart Meter Gateway sichert die digitale Kommunikation im intelligenten Messsystem und bietet einen geschützten Zugang zum Endkunden und zur Immobilie. Abb. 6.32 zeigt ein Gateway des deutschen Herstellers Power Plus Communications. Anforderungen sind unter Anderem

Tab. 6.2 Wirkprinzipien und zugehörige Sensortypen

| Wirkprinzip | Beispiel | Anwendung bzw. Wirkungsweise |
|------------------|---|---|
| Mechanisch | Manometer, Dehnungshebel, | Messung von Druck oder Gewicht durch Ausdehnung oder Kontraktion |
| Thermoelektrisch | Thermoelement | Elektrische Ströme fließen zwischen verbundenen Metallen bei Temperaturänderung |
| Resistiv | Dehnungsmessstreifen, | Messung der Längenveränderung von Objekten durch Widerstandsdrähte. |
| Piezoelektrisch | Beschleunigungssensor, Drucksensor | Verformung von geeigneten Kristallen unter Druck erzeugt elektrische Ladungen |
| Kapazitiv | Drucksensor, Regensensor, Feuchtigkeitsmessung | Die Kapazität eines Kondensators wird durch Abstand der Platten oder etwa Feuchtigkeit zwischen ihnen verändert |
| Induktiv | Neigungsmesser, Kraftsensor, Geschwindigkeitsmessung, Verkehrszählung | Das durch eine Spule erzeugte Magnetfeld wird durch vorbeilaufende Objekte verändert |
| Optoelektronisch | CCD-Sensor, Fotozelle, Infrarotsensor (Bewegungsmelder) | Optoelektronische Elemente wandeln Licht in elektrische Ladung um. Bei Digitalkameras als integrierte Schaltungen (CCD) |
| Akustisch | Füllstandssensor, Ultraschall-Durchflussmesser, | Oberflächenwellen hängen von Fließgeschwindigkeit, Temperatur etc. von Flüssigkeiten ab und werden von Membranen aufgenommen. |
| Magnetisch | Hall-Sensoren, Reed-Kontakt | Drehzahlmessung (u. a. Kfz), elektronischer Kompass, Lageerkennung, Schaltvorgänge |

- Zertifizierung nach den einschlägigen Standards des BSI zur Datensicherheit, einschließlich Verschlüsselung und Datenschutz.
- „Plug-and-Play“-Installation vor Ort
- Anbindung über verschiedene Mobilfunkstandards, unter anderem LTE mit LTE-M und NB-IoT in verschiedenen Frequenzbändern, LPWAN, WLAN
- Unterstützung von Tarifanwendungsfällen (Minimum TAF 1, 2, 6 und 7)

Neben den digitalen Stromzählern gibt es eine große Zahl weiterer Sensoren, die im Internet of Things genutzt werden. Tab. 6.2 zeigt eine beispielhafte Übersicht der Typen zusammen mit dem genutzten Wirkprinzip.

6.6 Fragen

- 1) Wie entstand die Bezeichnung „Handy“ für ein mobiles Endgerät?
- 2) Wie heißt das erste Mobiltelefon, welches zu Beginn der 80er-Jahre des letzten Jahrhunderts veröffentlicht wurde?

- 3) In welche Klassen lassen sich mobile Endgeräte einteilen und nach welchen Klassifizierungsmerkmalen erfolgt diese Einteilung?
- 4) Wann wird von einem Smartphone gesprochen?
- 5) Welche Betriebssysteme für mobile Endgeräte sind zurzeit am weitesten verbreitet?
- 6) Was gilt als größter Erfolgsgarant der Apple Geräte?
- 7) Was ist das aktuell größte Problem bei Android, welches auch die Anwendungsentwicklung beeinflusst und verlangsamt?
- 8) Welche Leistungsmerkmale unterscheiden ein MCPTT Endgerät von einem Smartphone?
- 9) Nennen Sie wichtige Anforderungen an ein Mobilfunkgerät im Internet der Dinge (IoT).
- 10) Seit wann können in Deutschland Smart Media Gateways in Betrieb genommen werden?
- 11) Was ist ein Tarifanwendungsfall?
- 12) Warum wird ein Smart Meter Gateway über Mobilfunk und mit Batterien als Energieversorgung betrieben?
- 13) Überlegen Sie sich, welche Befürchtungen und mögliche Risiken zur Forderung nach Verschlüsselung der SMGW-Daten und zum Tarifanwendungsfall 1 geführt haben.

Literatur

- Auerbach M, Schönherr F (2009) Mobile Endgeräte für Businessanwendungen. FIR-Edition Studien. Aachen: Forschungsinstitut für Rationalisierung (FIR) e.V. 978-3-934318-40-3
- GSM Association (2016) 3GPP Low Power Wide Area Technologies. GSM Association. <https://www.gsma.com/iot/wp-content/uploads/2016/10/3GPP-Low-Power-Wide-Area-Technologies-GSMA-White-Paper.pdf>. Zugegriffen am 09.09.2021



Akteure und Ecosystems im Mobile Business

7

7.1 Einführung und Lernziele

Allein in Deutschland bestehen heute über 150 Millionen Vertragsverhältnisse im Mobilfunk. Akteure in der Mobilfunkindustrie erwirtschaften einen Endkundenumsatz von 26,5 Milliarden Euro (Bundesnetzagentur 2021). Sowohl die Zahl der Mobilfunkanschlüsse als auch das individuelle Datenvolumen sind dabei Wachstumstreiber. Weltweit gab es 2020 bereits 8,15 Milliarden Mobilfunkanschlüsse und 66 % aller Menschen besitzen ein Smartphone (Ericsson 2020). Auf einem Markt dieser Dimension sind zahlreiche Akteure in den verschiedensten Rollen aktiv. Im Folgenden sollen die wesentlichen Zusammenhänge, Strukturen und Prozesse aufgezeigt werden, bevor im weiteren Verlauf die besondere Bedeutung der Hersteller der mobilen Betriebssysteme in der sogenannten App Economy betrachtet werden sollen (Abb. 7.1).

► Lernziele

- Sie kennen Akteure, die im Mobile Business Ecosystem eine Rolle spielen.
- Sie kennen die Bedeutung der wichtigsten mobilen Plattformen und die Entwicklung zu Platform Ecosystems.
- Sie kennen die unterschiedlichen Wertschöpfungsaktivitäten im Mobile Business Ecosystem.
- Sie kennen die Aufgaben und Herausforderungen, denen sich Mobilfunknetzwerkbetreiber,
- Endgerätehersteller und Anwendungsentwickler stellen müssen.

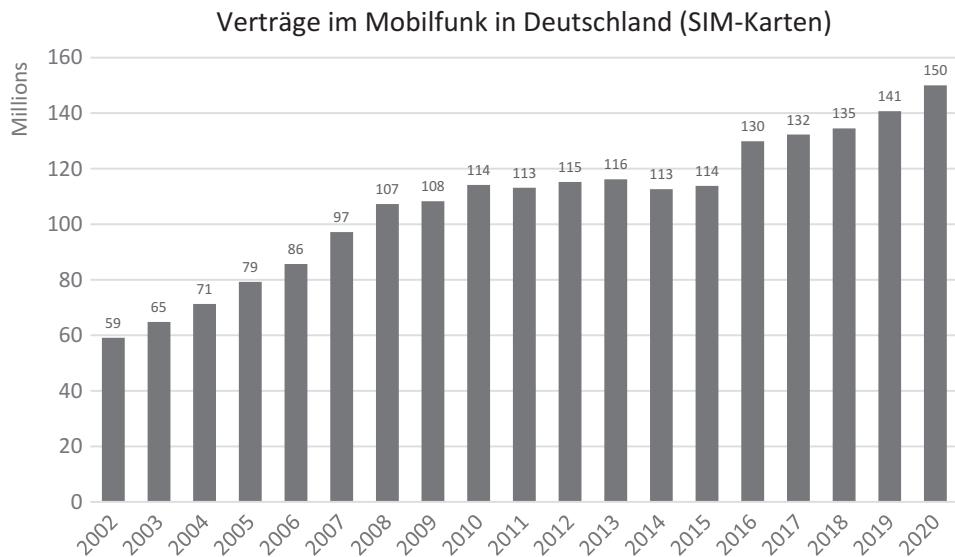


Abb. 7.1 Entwicklung der Mobilfunkverträge in Deutschland (Bundesnetzagentur 2021)

7.2 Akteure in der Mobilfunkindustrie

Im Bereich der Netzinfrastruktur gibt es drei wesentliche Bereiche, in denen sich unterschiedliche Akteure betätigen. Dies sind Regulierung und Standards, Netzaufbau und Netzbetrieb sowie Vertrieb. Abb. 7.2 gibt einen Überblick über die Bereiche und die jeweiligen Akteure, auf die im Folgenden detaillierter eingegangen werden soll.

7.2.1 Regulierung und Standards

Die *Internationale Fernmeldeunion* (englisch International Telecommunication Union, ITU) mit Sitz in Genf ist eine Sonderorganisation der Vereinten Nationen. Sie beschäftigt sich offiziell und weltweit mit technischen und regulatorischen Aspekten der Telekommunikation. In der Sektion Radio (ITU-R), werden alle Aspekte der Funkkommunikation gebündelt. Dazu gehören unter anderem die Veranstaltung der regelmäßigen Weltfunkkonferenzen, in denen völkerrechtlich verbindlich die Nutzung von Funkfrequenzen festgelegt wird. Die Studiengruppe International Mobile Telecommunications (IMT) der ITU-R beschäftigt sich mit den Anforderungen an moderne mobile Telekommunikationstechnologie. Sie legt die Kriterien für Mobilfunk der Generationen 3G bis 5G und aller zukünftigen Generationen fest. So steht das Dokument IMT-2000 für Mobilfunkdienste der 3. Generation, in IMT-Advanced wurden die Anforderungen für die 4. Generation formuliert, und in IMT-2020 sind die Bedingungen für Netze und Endgeräte in 5G niedergelegt.

| Bereich | Akteur | Beispiele |
|----------------------------|---|--|
| Regulierung und Standards | Internationale Regulierung | ITU-R, CEPT, ETSI |
| | Mobilfunk-Standards | 3GPP, IEEE, ETSI |
| | Nationale Regulierung | Bundesnetzagentur |
| | Lokale Genehmigungsbehörden | Stadtverwaltungen, Landkreise, Bauämter |
| Netzaufbau und Netzbetrieb | Nationale und internationale Mobilfunk-Netzbetreiber (Mobile Network Operators, MNO) | T-Mobile, Vodafone, Telefonica „O2“, British Telecom „Everything Everywhere“, France Telecom „Orange“, AT&T, Sprint, Verizon, China Mobile |
| | Netztechnik-Lieferanten | Cisco, Ericsson, Huawei, Mavenir, NEC, Nokia, Samsung, ZTE |
| | „Tower Companies“ | Deutsche Funkturm Management Gesellschaft (DFMG), American Towers (ATC), Crown Castle, Vantage Towers |
| | Immobilien-Partner | Vermieter, Makler, Agenturen |
| | IT-Lieferanten für Netzmanagement und Abrechnung | IBM, HP, Amdocs, Netcracker, Oracle, Salesforce |
| | Partner für Netzbetrieb und Wartung der Technik vor Ort | Netztechnik-Lieferanten, IT Outsourcer wie Tech Mahindra |
| | Mobilfunk-Netzbetreiber | T-Mobile, Vodafone, O2, AT&T, Verizon (USA), Orange (F) |
| Vertrieb | Mobile Virtual Network Operators (MVNO) | Drillisch, Mobilcom, Aldi-Talk, Fonic, Klarmobil, Blau.de, Lebara, Lycamobile |

Abb. 7.2 Akteure im Mobile Business

| ATIS USA | CCSA China | ETSI Europa | ARIB Japan | TTC Korea | TTA Korea | TSDSI Indien | Partner |
|---|---|---|---------------|--------------|--------------|-----------------|--------------------|
| Projekt Koordinationsgruppe (PCG) | | | | | | | |
| TSG RAN Radio Access Network Spezifikation GSM, UMTS, LTE, 5G | TSG SA Service and Architecture Mobile Services und System Aspekte | TSG CT Core Network and Terminals Kern-Netzwerke Endgeräte | | | | | Technische Gruppen |
| Herstellerfirmen, Netzbetreiber, Forschungsinstitutionen und Organisationen beteiligen sich über die Mitgliedschaft in einer der regionalen Partnerorganisationen | | | | | | | |
| <p>Legende:</p> <p>ARIB: Association of Radio Industries and Businesses, Japan ATIS: Alliance for Telecom Industry Solutions, USA CCSA: China Communications Standards Association, China</p> <p>ETSI: European Telecommunications Standards Institute, EU TTA: Telecommunications Technology Association, Korea TTC: Telecommunications Technology Association, Japan TSDSI: Telecom Standards Development Society, India</p> | | | | | | | |

Abb. 7.3 Die Organisation des 3rd Generation Partnership Projects (3GPP)

Das *3G Partnership Project* (3GPP) ist ein weltumspannender Zusammenschluss von Entwicklungs-, Forschungs- und Standardisierungsorganisationen (Abb. 7.3). Seine Träger (Organisatorische Partner) sind sieben internationale und regionale Standardisierungs-Organisationen wie etwa das *European Telecom Studies Institute* (ETSI). Das 3GPP wurde ins Leben gerufen, als die ITU-R in IMT-2000 zur Entwicklung eines einheitlichen globalen Standards der mobilen Kommunikation aufrief. 3GPP entwickelte die Technologie-standards UMTS und cdma2000 für 3G, LTE und LTE-Advanced für 4G und arbeitet derzeit an der 5. Generation des Mobilfunks. In regelmäßigen Release-Paketen werden alle Standards einschließlich GSM laufend weiterentwickelt und an die sich verändernden technischen Erfordernisse angepasst. Hersteller, Forschungseinrichtungen, Netzbetreiber und Behörden wirken am 3GPP über ihre Mitgliedschaft bei den organisatorischen Partnern mit. Die 3GPP-Entwicklungen sind offene Standards, als Download über die Webseite <https://www.3GPP.org> verfügbar und allgemein für Forschung und Entwicklung nutzbar. Unternehmen und Einrichtungen sichern die Rechte an ihren Beiträgen über nationale und internationale Patente ab. Ein Unternehmen, welches ein Produkt unter Nutzung von 3GPP-Material auf den Markt bringt, muss in der Regel Patentnutzungsgebühren entrichten. Die großen Hersteller haben gegenseitige Vereinbarungen zur Nutzung des Patent-Portfolios abgeschlossen.

Das European Telecommunications Standards Institute (ETSI) ist eine gemeinnützige Organisation mit Sitz in Sofia Antipolis (Frankreich). Es wird durch die Mitgliedsbeiträge ihrer über 800 Mitglieder finanziert und wurde durch die Europäische Union und die Conférence Européenne des Administrations des Postes et des Télécommunications (CEPT), der Dachorganisation von 48 europäischen Regulierungsbehörden, beauftragt, die Harmonisierung der europäischen und internationalen Telekommunikationsdienste voranzu-

treiben. Als regionale Standardisierungsbehörde arbeitet es im ITU-R mit und ist gleichzeitig ein organisatorischer Partner im 3GPP. Zu den Mitgliedern zählen Hersteller, Netzbetreiber, Forschungseinrichtungen (u. a. Fraunhofer-Institut) und Behörden wie die Bundesnetzagentur (BNetzA). Das ETSI adaptiert ITU-Standards für die Europäische Union, und vertritt gleichzeitig europäische Interessen in der globalen Standardisierung. Zu den ETSI-Verantwortlichkeiten gehört die Harmonisierung der Frequenzvergabe in der EU im Rahmen der ITU-R Festlegungen.

Als nationale Regulierungs- und Standardisierungsbehörde ist die *Bundesnetzagentur* (BNetzA) tätig. Die BNetzA ist als eine Oberste Bundesbehörde der Bundesregierung direkt unterstellt. Neben der Telekommunikation obliegt ihr auch die Regulierung der anderen nationalen Netze (Elektrizität, Gas, Schienennetz) sowie der Postdienste. Die Aufsicht über die BNetzA liegt beim Bundeswirtschaftsministerium; die fachliche Aufsicht bezüglich der Telekommunikation ist derzeit allerdings dem Bundesminister für Verkehr und Digitale Infrastruktur übertragen. Nach der Rechtsprechung des Europäischen Gerichtshofes ist der BNetzA allerdings weitgehende Unabhängigkeit von der Politik zu gewährleisten (LTO 2021) Die BNetzA ist Mitglied des ETSI, der CEPT, des 3GPP sowie der ITU, vertritt dort nationale Interessen und führt die Standards und Beschlüsse in nationales Recht über. Dazu arbeitet sie eng mit politischen Institutionen zusammen. Die Beschlüsse und Verordnungen der Bundesnetzagentur sowie alle dazugehörigen Vorgänge, werden auf ihrer Webseite publiziert. Sie erstellt regelmäßig Tätigkeitsberichte und gibt Überblicke über Marktentwicklungen, die als Download unter <https://www.bundesnetzagentur.de> erhältlich sind.

Für das operative Geschäft des Mobilfunks organisiert die BNetzA im Auftrag der Bundesregierung die Frequenzvergabe für den Mobilfunk und alle anderen mit drahtloser Kommunikation verbundenen Technologien, wie terrestrischer Fernsehempfang (DVBT), Radio und Richtfunkstrecken. Dabei richtet sie sich nach der globalen Harmonisierung der Frequenznutzung durch ITU-R und ETSI. Mobilfunkfrequenzen werden in Deutschland in aller Regel durch Auktionen vergeben (Abb. 7.4). Das Nutzungsrecht geht immer nur für einen beschränkten Zeitraum (z. B. 10 oder 20 Jahre) auf den Erwerber über. Anders als zum Beispiel in den USA kann mit Frequenznutzungsrechten in Deutschland nicht gehandelt werden. Im Falle einer Insolvenz oder sonstigen Geschäftsaufgabe fallen sie entschädigungslos an den Staat zurück. Mit dem Erwerb der Nutzungsrechte sind in der Regel Auflagen verbunden, wie etwa einen Mindestversorgungsgrad in Bezug auf Fläche oder Bevölkerung sowie eine Mindestqualität der angebotenen Dienste zu erbringen. Bei Nichtbeachtung der Auflagen drohen Konventionalstrafen und im schlimmsten Fall ein Entzug des Nutzungsrechts.

Im Jahr 2015 wurden neben der Neuvergabe von ehemaligen GSM-Frequenzen und der Bereitstellung eines zusätzlichen Frequenzbandes bei 1,5 GHz ehemalige terrestrische Fernsehfrequenzen im 700 und 800 MHz-Bereich für LTE vergeben, die entsprechend der Vorgabe durch die ITU-R mit der Einführung des digitalen DVBT2-Standards frei ge-

| Jahr | Technologie | Was wurde versteigert? | | Erlöse (ca. in Mrd. €) |
|------|---|---------------------------------------|------------|------------------------------|
| | | Frequenzbereich | Bandbreite | |
| 2000 | UMTS | 2,0 GHz | 145 MHz | 50,8 |
| 2010 | UMTS Tranche 2 | 2,0 GHz | 60 MHz | 4,4 |
| 2010 | LTE | 800 MHz, 1,8 GHz, 2,6 GHz | 320 MHz | |
| 2015 | LTE, 700/800 MHz „Digitale Dividende“ | 700 MHz, 900 MHz, 1,8 GHz, 1,5 GHz | 270 MHz | 5,1 |
| 2019 | 5G Frequenzen | 2 GHz, 3,4 bis 3,8 GHz | 420 MHz | 6,5 |

Abb. 7.4 Bedeutsame Frequenzauktionen Mobilfunk der Bundesnetzagentur

worden waren. Entsprechend der Vorgabe der World Radio Conference wurden diese Frequenzbänder als „Digitale Dividende“ kostengünstig an die Mobilfunkbetreiber vergeben, die damit insbesondere die Versorgung des ländlichen Raumes verbessern sollten. Die 5G-Frequenzen im Bereich von 3,4 bis 3,8 GHz wurden nach dem Auslaufen der so genannten WiMax-Technologie durch die ITU-R für LTE umgewidmet, und entsprechend von der BNetzA auch national an die Netzbetreiber versteigert.

Wenn Spektrum zur Vergabe ansteht, erfolgt zunächst eine Abfrage des Bedarfs. Dabei wird der Kreis der möglichen Bewerber bereits durch Vorab-Festlegungen der möglichen Nutzung eingeschränkt. Zu einer Auktion kommt es gemäß Beschluss der Präsidentenkammer der BNetzA immer dann, wenn der erkennbare Bedarf nicht durch einfache Zuweisung gedeckt werden kann. Sonst erfolgt eine Zuweisung gegen Entrichtung einer von der Behörde festgelegten Gebühr. Die Bundesnetzagentur ist auch verantwortlich für die Zuweisung von nicht lizenziertem Radio-Spektrum durch Allgemeinverfügung wie in Kap. 5 erläutert.

7.2.2 Netzaufbau und Netzbetrieb

Der Aufbau und der Betrieb eines Mobilfunknetzes gehört zu den Kernaufgaben der Mobilfunk-Netzwerkbetreiber (Mobile Network Operator, MNO). Es handelt sich um Wirtschaftsunternehmen, die durch den Vertrieb von Telekommunikationsleistungen über ihre Netze Umsätze und Gewinne erwirtschaften. Es gibt derzeit drei voneinander unabhängige öffentliche Mobilfunknetze in Deutschland. Sie werden von den international operierenden Telekommunikationskonzernen Deutsche Telekom (mit Sitz in Bonn), Vodafone (Reading, UK) und Telefónica-O2 (Madrid, Spanien) betrieben. Diese Konstellation hat sich aus der ursprünglichen Vergabe an insgesamt vier deutsche Lizenznehmer durch eine Reihe von z. T. spektakulären Übernahmen ergeben (Abb. 7.5). Dabei sind die

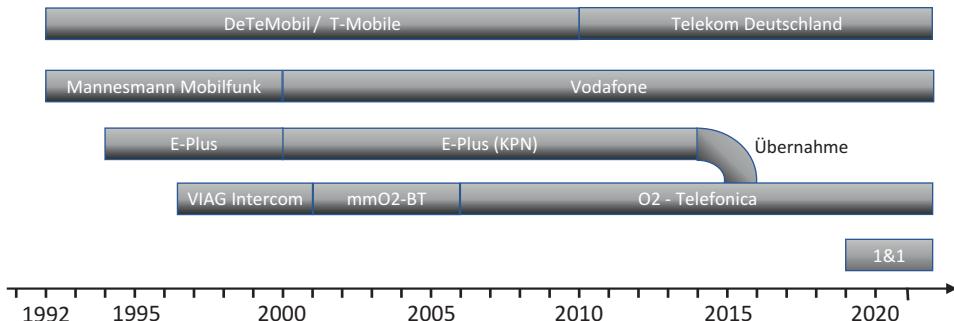


Abb. 7.5 Mobile Network Operators in Deutschland in der historischen Entwicklung

Namenswechsel der Mobilfunktochter der Deutschen Telekom lediglich Konzernrestrukturierungen geschuldet. Ein Wechsel der Besitzverhältnisse war damit nicht verbunden. Die von der Mannesmann AG gegründete Mobilfunktochter Mannesmann Mobilfunk mit dem Netz-Label „D2-Privat“ ging nach der seinerzeit teuersten Übernahme der Industriegeschichte im Jahr 2000 an die britische Vodafone. Die beiden übrigen GSM Lizenzen wurden 1994 und 1997 von zwei Konsortien um die Energiekonzerne Vebacom (E-Plus) und VIAG Interkom (E2, später O2) erworben. E-Plus wurde im Jahr 2000 an den niederländischen Konzern KPN veräußert. Die VIAG zog sich 2001 nach der UMTS-Auktion ebenfalls aus dem Konsortium zurück und überließ das Geschäft der British Telecom, die ihre Mobilfunkmarke O2 einführt. 2006 zog sich auch die British Telecom zurück und verkaufte das gesamte Mobilfunkgeschäft an die spanische Telefonica, die 2015 auch E-Plus übernahm. Zwei erfolgreiche Bieter der UMTS-Auktion in Jahr 2000, Group 3G/Quam und Mobilcom, schieden kurz nach Durchführung der Auktion wieder aus dem Markt, ohne ein Netzwerk aufgebaut zu haben. Die ersteigerten Frequenzblöcke sind entsprechend entschädigungslos an den Staat zurückgefallen. Mit der 5G-Auktion im Jahre 2019 trat das Unternehmen 1&1 Drillisch, eine Tochter des Internet Service Providers United Internet, als vierter Mobilfunk-Netzbetreiber auf, der einen Teil der 5G Funkfrequenzen ersteigte und nun in der Verantwortung steht, ein eigenes Netz entsprechend den Vergabedingungen aufzubauen. Für eine Übergangsperiode plant 1&1 Drillisch die Mitnutzung vorhandener Kapazitäten der bestehenden Netze durch ein nationales Roaming gegen Gebühr. Die Verpflichtung von O2, ein entsprechendes Abkommen abzuschließen, ist ein Teil der kartellrechtlichen Auflagen für die Übernahme von E-Plus durch Telefonica-O2.

MNO benötigen eine Lizenz zum Betrieb eines Telekommunikationsnetzes, die von der Bundesnetzagentur erteilt wird. Sie müssen zusätzlich Rechte zur Nutzung eines Frequenzbandes erwerben, auf dem sie ihre Dienste anbieten können. Die Rechte und Pflichten eines Netzbetreibers sind bezüglich des allgemeinen Geschäftsbetriebes im Telekommunikationsgesetz aus dem Jahr 2004 geregelt. Für die Regulierung der Kundenbeziehung (u. a. Vertragsrecht und Datenschutz) wurde im Jahre 2007 das Telemediengesetz vom Deutschen Bundestag verabschiedet.

Der Aufbau eines Mobilfunknetzes ist eine komplexe und kapitalintensive Aufgabe, die mit Hilfe von zahlreichen spezialisierten Partnern der verschiedenen Fachgebiete bewältigt wird. Die *Funknetzplanung* legt Wunsch-Standorte für Basisstationen fest, *Agenuren* und *Makler* werden beauftragt, Flächen für die Errichtung von Funktürmen oder geeignete Dachstandorte auf hohen Gebäuden anzumieten. Wird ein Standort selbst errichtet, sind das Baurecht sowie die lokalen Bestimmungen zu beachten. Der Auftrag zum Bau wird dann in der Regel an ein *spezialisiertes Bauunternehmen* erteilt. Alternativ haben sogenannte *Tower Companies* ein Portfolio von bereits gebauten Standorten, die sie zur Mitnutzung anbieten. Diese Unternehmen haben oft gebaute und in Betrieb befindliche Standorte eines MNO gekauft, und an den Netzbetreiber zurück vermietet. Zum Teil sind sie auch Ausgründungen von Mobilfunkunternehmen mit dem Ziel der Verwertung der Standort-Immobilien. Diese Standorte können so auch konkurrierenden MNOs und LPWAN-Betreibern zur Mitnutzung angeboten werden. Das Ziel ist, eine Belegungsquote (Tenancy) von deutlich größer als 1 zu erzielen. Die Tabelle in Abb. 7.6 zeigt die wichtigsten in Deutschland tätigen Tower Companies mit ihren Kennzahlen. Gelegentlich kommt es auch zu direkten Kooperationen von Netzbetreibern bei der Errichtung eines Standortes.

Zusätzlich zu den eigentlichen Funkstandorten müssen Leitungswege und Standorte zur Anbindung des Funknetzes an das Kern-Netz und zur internen Vernetzung von Funknetz und Kern-Netz geplant und errichtet werden. Sofern vorhanden, wird auf bestehende Übertragungsstrecken zurückgegriffen. Ansonsten können die Planer zwischen Glasfaserstrecken, traditionellen Kupferleitungen und Richtfunk wählen. In vielen Fällen müssen hierfür Gebäude; im Falle von Richtfunk sogar zusätzliche Türme errichtet werden.

Die technische Ausrüstung des Netzes mit Funk- und Übertragungsanlagen wird von den *Netzausrütern* geliefert. Die Auswahl des Lieferanten erfolgt über eine Ausschreibung. Im Markt für Netzausrüstung fand in den vergangenen 20 Jahren ein starker Konzentrationsprozess statt, so dass Mobilfunktechnik heute weltweit nur noch von wenigen Unternehmen angeboten wird. Treiber der Konzentration waren der Preisdruck am Endkundenmarkt, aber auch die Vergleichbarkeit der Produkte als Folge der immer weiter gehenden Standardisierung. Alle Anbieter arbeiten direkt bei 3GPP mit, und nehmen so erheblichen Einfluss auf die Ausgestaltung der Standards.

Die in Deutschland aktiven MNOs setzen sich auch für die in den USA entstandene Initiative Open RAN (Open Radio Access Network) ein. Open RAN verfolgt die Ziel-

| Gesellschaft | Standorte Deutschland | Standorte weltweit | Globaler Umsatz 2020 (in Millionen €) |
|-------------------|--------------------------|--------------------|--|
| Deutsche Funkturm | 28.200 | 28.200 | 187,1 |
| Vantage Towers | 19.400 | 82.000 | 945,5 |
| American Towers | 2.200 | 180.000 | 1.603,0 |

Abb. 7.6 In Deutschland tätige Tower Companies mit Standorten und globalen Umsatzzahlen laut Geschäftsberichten

setzung einer quelloffenen Software und der Interoperabilität der Komponenten im Funknetz. Etwa 80 % der gesamten Netztechnik, die heute weltweit im Einsatz ist, stammt von den drei Herstellern Ericsson, Huawei und Nokia (Statista 2019). Die einzelnen Bausteine sind zwischen den Herstellern derzeit nicht zwingend kompatibel. Viele MNOs haben daher eine Absichtserklärung zur Einführung und zum Einsatz von Open RAN-Lösungen unterzeichnet. Dabei soll mit bestehenden und neuen Partnern aus der Mobilfunkindustrie zusammengearbeitet werden. Das Angebot von Open RAN Lösungen beschränkt sich derzeit allerdings weitgehend auf LTE-Produkte nach dem 4G-Standard. Open RAN muss auch noch auf die hochintegrierten Komponenten der bisherigen Hersteller verzichten, was Auswirkungen auf Performance und Energie-Effizienz haben kann. Der neue Netzbetreiber 1&1 Drillisch setzt bei seinem 5G-Netzausbau bereits auf Open RAN Produkte.

Der *Betrieb* von Mobilfunknetzen benötigt eine umfangreiche IT-Umgebung, die von Spezialisten für die einzelnen Segmente geliefert wird. Beispiele sind das Netz-Managementsystem zur Konfiguration, Fehleranalyse und -Behebung und Performance Analyse. Die Vergabe von IP-Adressen an Endgeräte und Netzknoten sowie das IP Management mit Routern, Domain Name Servern und Firewalls gehört gleichfalls dazu. Schließlich sind die Kundenverwaltung für Millionen von Verträgen, sowie die Abrechnungssysteme für Prepaid und Postpaid Kunden ein wichtiger Bestandteil der Netzarchitektur.

Network Operation Centers (NOC) sind rund um die Uhr für den Betrieb und die Fehlerbehebung im Netz zuständig. Die Netzbetreiber erweitern das Netz regelmäßig mit zusätzlichen Basisstationen. Außerdem werden bestehende Standorte verändert, z. B. aufgrund des Auslaufens von Standort-Mietverträgen oder des Abrisses alter Gebäude mit Mobilfunkeinrichtungen. Diese Vorgänge erfordern die Neu-Konfiguration des Netzes in einer Region, die bis ins Kern-Netz hineinreichen. Aus Kundenbeschwerden über mangelnde Netz-Abdeckung und Ergebnissen von Testfahrten ergeben sich weitere Maßnahmen. Ausfälle von Netzelementen und andere Fehlfunktionen laufen über Alarm-Meldungen beim NOC ein, müssen analysiert und bearbeitet werden. Mehrere Hundert Feldtechniker (abhängig von der Netzgröße) sind täglich unterwegs, um Aufträge des NOC vor Ort auszuführen. Für die Fehleranalyse und -behebung sichern sich die Netzbetreiber die Unterstützung der Hersteller über langfristige Support-Verträge.

Es gibt unter Netzbetreibern die Tendenz, das NOC und die Feldtechnik auszulagern. Aufgrund ihrer Produktkenntnis bieten sich hier vor allem die Netzausrüster als Outsourcing-Partner an. Sie können Einsparungen durch die gleichzeitige Wartung von mehreren Netzen erzielen und verfügen aufgrund ihrer weltweiten Aktivitäten über eine umfassende Kenntnis möglicher auftretender Probleme. Auch IT-Outsourcing Spezialisten treten in den Wettbewerb um Netzbetrieb und Netzwartung ein. Neben dem Betrieb der großen öffentlichen Netze zielen sie aber vor allem auf die privaten 5G-Netze von Industrie-Unternehmen. Mit der Einführung des LTE-Standards entstand das Feature Self-Organizing Networks (SON). Im Netzaufbau können neue Basisstationen durch SON die Stationen in ihrer Nachbarschaft entdecken und sich automatisch entsprechend konfi-

gurieren. Im Betrieb trägt SON zu einer hohen Verfügbarkeit des Netzes für die Kunden bei. Beim Ausfall einer Station kann automatisch die Sendeleistung benachbarter Elemente abgestimmt verändert werden, dass die Abdeckung der Fläche erhalten bleibt und der Verlust des Service für die Netzteilnehmer vermieden wird. Zentrale Netzmanagement-Systeme führen automatische Fehlersuche durch und machen Lösungsvorschläge.

7.2.3 Vertrieb und Kundenbetreuung

Die Basisprodukte eines MNO sind eigentlich recht einfach: Es handelt sich um Gesprächsminuten, um nach Stückzahlen abgerechnete (Kurz-) Nachrichten, sowie schließlich um Datenvolumina für den mobilen Internetzugang. Wurden ursprünglich jede Gesprächsminute und jede Kurznachricht detailliert abgerechnet, sind heute mit der schwindenden Bedeutung des Gesprächsumsatzes Bündelangebote der Normalfall, die meist Inklusiv-Minuten für Telefonie, ein Kontingent an Kurznachrichten und ein maximales Datenvolumen pro Monat enthalten. Die Entwicklung von marktgerechten Kombinationstarifen ist eine anspruchsvolle Aufgabe, die bei den großen Netzbetreibern mehr Personal erfordert als etwa die Entwicklung und der Betrieb der Netze. Ein Vergleich der Entwicklung der mobilen Datenmengen und der Einnahmen der MNO, zeigt, dass der Preis pro Leistungseinheit stark abgenommen hat (Abb. 7.7). Der politisch für die europäische Einheit bedeutsame Beschluss der EU, die Roaming-Gebühren im EU-Ausland abzuschaffen, erzeugte für die Netzbetreiber einen weiteren Kostendruck. Noch hat kein Anbieter einen erfolgversprechenden Weg entdeckt, wie die immer weiter steigende Menge an Daten, die durch die mobilen Netze fließen, zu entsprechenden Umsatz- und Gewinnsteigerungen führen können. Zahlreiche „Over The Top“-Player (OTT, Abschn. 7.3) nutzen dagegen den freien Zugang zu den Teilnehmern für ihre gewinnbringenden – oftmals werbefinanzierten – Geschäftsmodelle.

Bündelangebote schaffen einen gewissen Ausgleich, da in der Regel Kontingente verkauft werden, die der Nutzer am Ende nicht ausschöpft, oder bei denen zusätzliches Volumen kostenpflichtig nachgebucht werden muss. Die Bündelung mit Endgeräten verschafft zusätzliche positive Effekte durch die lange Laufzeit der Verträge, die an die Finanzierung der Endgeräte gekoppelt sind, sowie durch den Vertrieb der Endgeräte selbst.

Die Bündelung mit Endgeräten bedingt meist den Abschluss eines Laufzeitvertrages (Postpaid), der eine feste monatliche Gebühr und gegebenenfalls ein Entgelt für Zusatzleistungen beinhaltet. Daneben gibt es auch noch das populäre Produkt „Prepaid“. Dabei erwirbt der Kunde nach Bedarf ein Guthaben, das dann nach Bedarf verbraucht wird. Ein Angebot zwischen Prepaid und Laufzeitvertrag ist das Produkt, bei dem monatlich eine feste Summe vom Prepaid-Guthaben abgebucht wird, und der Kunde dafür ein Inklusiv-Volumen zur Verfügung gestellt bekommt. Aus Kundensicht spricht für das Prepaid-Produkt der unkomplizierte Erwerb als „Mitnahmeartikel“ und das einfache Abrechnungsprinzip. Seit 2017 wurde im Rahmen der Anti-Terrorismusgesetzgebung allerdings eine

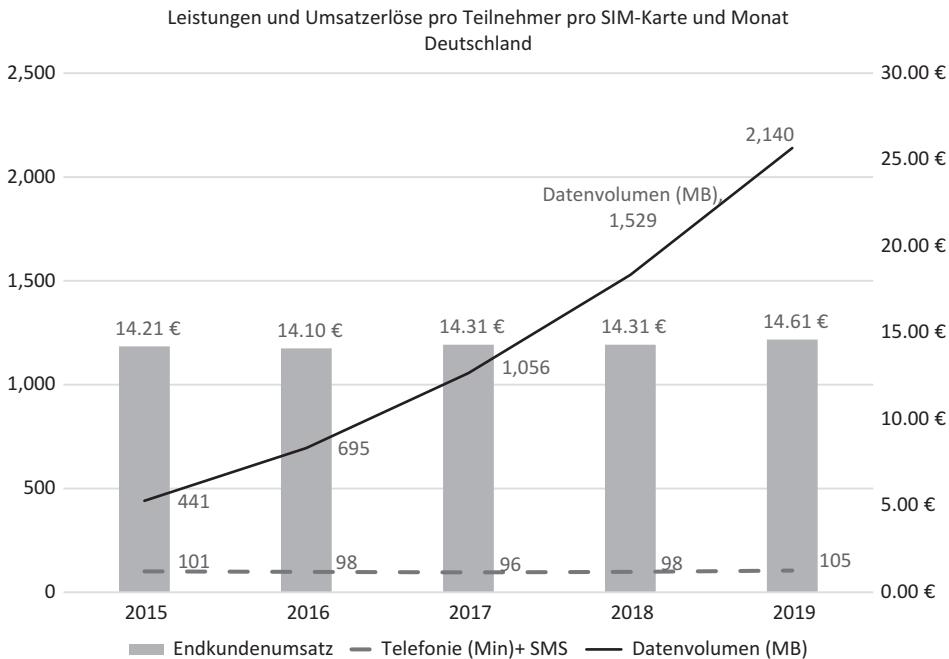


Abb. 7.7 Leistungen und Umsatzerlöse der Mobilfunkbetreiber in Deutschland (Bundesnetzagentur 2020a)

verpflichtende Registrierung für Prepaid-Karten im Telekommunikationsgesetz eingeführt, was zu einer Reduktion der Neuabschlüsse führte.

In der Regel sind für den Netzbetreiber Laufzeitverträge lukrativer. Als Maß wird der Average Revenue per User (ARPU) verwendet, also der durchschnittliche Umsatz pro Teilnehmer. Abb. 7.8 zeigt im Vergleich den ARPU für Prepaid und Vertragskunden. Allerdings hat ein gewisser Anteil von Prepaid-Kunden positive Wirkungen auf den Cash-Flow des Unternehmens. Prepaid-Kunden zahlen für die Leistung teilweise Monate vor der Inanspruchnahme und verbessern so die Liquidität. Bei den deutschen MNO liegt der Anteil der Prepaid-Kunden bei über 40 %.

Weitere Indikatoren für den Erfolg des Geschäftsverlaufes bei MNO sind die Abwanderungsrate (Churn Rate) und der Net Promoter Score. Abwanderung von Teilnehmern bedeutet in der Regel einen Wechsel zur Konkurrenz. Auch wenn die Abwanderung in der Regel durch Neugewinnung von Kunden ausgeglichen werden kann, ist eine hohe Abwanderungsrate ein erheblicher Kostenfaktor. Die Gewinnung eines neuen Kunden ist wegen der marktüblichen Promotion-Angebote immer mit Kosten oder Einnahmeausfall verbunden. Die Abwanderungsrate pro Monat beträgt für Laufzeitverträge in Deutschland im Durchschnitt etwa 1,5 %. (Statista 2021d, e, f). Da Prepaid-Kunden ihren Vertrag nicht kündigen müssen, sondern spontan ihren Netzbetreiber wechseln können, ist sie in dieser Kundengruppe naturgemäß etwas höher und liegt bei den verschiedenen Netzbetreibern

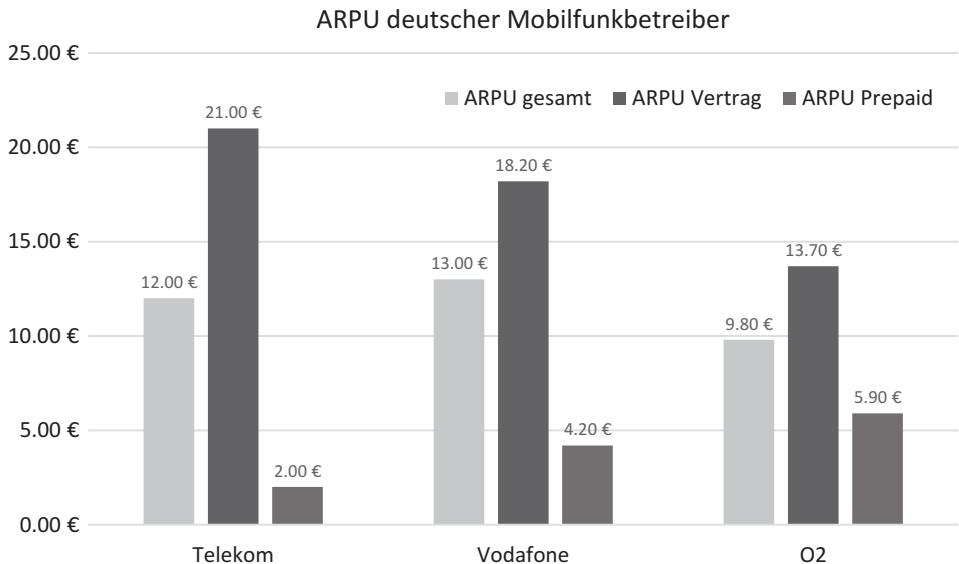


Abb. 7.8 Vergleich der monatlichen Netto-Umsätze pro Nutzer (ARPU) zwischen Prepaid und Vertragskunden, Stand 2018/19 (Statista 2021a, b, c)

bei 2 % bis 3,5 %. Beim Net Promoter Score wird – in der Regel durch Kundenbefragungen – die Bereitschaft der Kunden ermittelt, den Dienst weiterzuempfehlen. Der Net Promoter Score wird durch Auswertung von Kundenbefragungen ermittelt (Auf einer Skala von 1 bis 10: „Würden Sie dieses Produkt Ihren Bekannten weiterempfehlen?“ Der Score ergibt sich normalerweise aus der Differenz der Anzahl der stark positiven (9,10) und der eher negativen Antworten (1 bis 6).

Mobile Virtual Network Operators (MVNO) bieten ebenfalls Mobilfunkverträge (Postpaid oder Prepaid) an, teilweise im Bündel mit Endgeräten. Sie betreiben allerdings kein eigenes Netz, sondern nutzen das Netz eines MNO. Dazu werden komplexe Verträge über Modalitäten, Limitierungen und Entgelte zwischen MNO und MVNO geschlossen. Es gibt unterschiedliche Möglichkeiten für MVNOs: Angefangen bei einem einfachen Reseller-Modell über die Ausgabe eigener SIM-Karten, eine eigene Kundenbetreuung, eigene Abrechnungssysteme bis hin zu einem eigenen Kern-Netz, das mit dem Zugangsnetz des MNOs verbunden ist. Diese letzte Option wird nur selten angewendet. Die meisten MVNOs sind tatsächlich Reseller. Sie kaufen Mobilfunkleistungen zu Großhandelspreisen bei den Netzbetreibern und schaffen mit eigenen Tarifmodellen unabhängige Marktauftritte. In der Regel geben sie die SIM-Karten des Netzes mit eigenem Branding aus und erhalten sogar eigene Rufnummernblöcke innerhalb des Netzbetreiber-Rufnummernkontingents. In einigen Fällen erhalten sie von der Bundesnetzagentur auch eine eigene virtuelle Netz-ID. Viele Einzelhandelsketten bieten auf diese Weise eigene Mobilfunk-Dienste an (z. B. Aldi-Talk, Lidl Connect, Tchibo mobil). Einige MVNO sind tatsächlich Töchter der MNOs, die durch sie alternative Marktzugänge eröffnen und ein

anderes Publikum ansprechen (z. B. Blau, Congstar, Fonic, otelo). Zumeist handelt es sich dabei um Anbieter von Prepaid-Karten.

Das Marketing erfolgt fast ausschließlich über Markennamen und -image sowie günstige Tarife. Für einige international aktive MVNOs, wie Lycamobile oder Lebara, spielen auch die Reichweite und die Kosten internationaler Anrufe als Markt-Argument eine Rolle. Social Media Konzerne wie Facebook nutzen das MVNO Konstrukt, um preisgünstige exklusive Zugänge zu ihren eigenen Diensten für ein vorwiegend jugendliches Publikum zu bieten. Manche MVNOs verfügen über eigene Abrechnungssysteme. Dabei wird der Betrieb dieser Systeme häufig an den Netzbetreiber oder ein IT-Unternehmen ausgelagert. Eine der schwierigsten strategischen Fragen für einen MVNO ist, ob eine eigene Kundenbetreuung mit Callcenter aufgebaut werden soll. Dies ist nur mit erheblichem personellem und finanziellem Aufwand zu leisten. Die Qualität der fortlaufenden Betreuung der Kunden über ein Call-Center und eine gute Web-Präsenz werden häufig unterschätzt. MVNOs ohne eigenes Netz stehen oft wegen ihrer guten Kundenbetreuung in der Kundenzufriedenheit weit oben. Schon das erste MVNO, Virgin Mobile UK, ging regelmäßig als Sieger aus Kundenzufriedenheits-Umfragen hervor. Im Jahr 2020 gewann der MVNO *Consumer Cellular* zum siebenten Mal in Folge die Auszeichnung „Reader Choice Mobile Carrier“ des PC-Magazine in den USA (Gottesman 2020). Der Grund war ein ausgezeichneter Ruf ihrer Kundenbetreuung. Die ersten sechs Platzierungen der Leserumfrage gingen dabei sämtlich an MVNOs. Auch in anderen Ländern standen immer wieder MVNOs oben auf der Liste der „besten Netzwerke“.

7.3 Entwicklung der App Economy und Mobile Business Ecosystems

In den vergangenen Jahren wurde der weltweite Verkauf von mobilen Endgeräten durch den beträchtlichen Zuwachs im Bereich der Smart Devices, insbesondere Smartphones und Tablet-Computer bestimmt. Beide Typen mobiler Endgeräte basieren auf leistungsfähigen Betriebssystemen (Operating System), welche im englischen auch *Mobile Platform* genannt werden. Sie ermöglichen den Nutzern dieser Endgeräte eine breite Palette von Anwendungsszenarien. In erster Linie sind darunter die Installation und Nutzung mobiler Applikationen (Apps) zu nennen. Apps können von den Nutzern üblicherweise aus elektronischen Marktplätzen – auch App-Stores genannt – heruntergeladen und installiert werden. Diese Marktplätze sind als zweiseitige Märkte charakterisiert, da der Betreiber des Marktplatzes sowohl den Anwendungsentwicklern als auch den Nutzern eine Marktzugangsmöglichkeit eröffnet. Die einzelnen elektronischen Marktplätze werden oftmals durch die Anbieter der Betriebssysteme bereitgestellt und bieten dementsprechend jeweils ein Angebot, welches auf eine mobile Plattform spezialisiert ist. Nur wenige plattformübergreifende Marktplätze konnten sich etablieren, weisen jedoch jeweils einen deutlich niedrigeren Marktanteil auf. Aufgrund der Verbreitung von Plattformen und der Popularität von mobilen Anwendungen wird dieses Phänomen als „App Economy“ bezeichnet.

Der Erfolg von Smartphones und Tablet-Computern hat zu einem intensiven Wettbewerb zwischen Anbietern mobiler Plattformen geführt. Verschiedene mobile Plattformen strebten dabei an, das bevorzugte System für Hersteller von mobilen Endgeräten, für MNO und für Entwickler mobiler Anwendungen zu werden. Auf diesem Weg sollte eine potenziell große Zielgruppe an Nutzern mobiler Endgeräte für die jeweilige Plattform erschlossen werden. Die Ergebnisse dieses Plattformwettbewerbs haben die Realität geformt, da sie unmittelbaren Einfluss auf Innovation und Wachstum im Mobile Business hatten.

7.4 Mobile Business Ecosystem und Platform Economies

Im Folgenden soll ein tieferes Verständnis der Strukturen und der durch die Plattform-Anbieter genutzten Marktstrategien entwickelt werden. Aufgrund der seit 2012 relativ unveränderten Entwicklung in diesem Segment wird insbesondere auf die Jahre 2007 bis 2011 Bezug genommen. Grundsätzlich sind Endgerätehersteller, MNO und Mobile Platform Provider die drei maßgeblichen Akteure in der App Economy dieser Zeit. Die Rolle der MNO an diesem Geschäft hat allerdings (wie bereits dargestellt) in den letzten Jahren kontinuierlich abgenommen. Der gewählte Zusammenhang und Zeitrahmen sind aus drei Gründen relevant. Erstens veränderte sich die Mobilfunkbranche laufend. Ein Anschub war insbesondere die steigende Nachfrage nach neu(artig)en Endgeräten durch die Nutzer. Aus der Entwicklung neuer Endgeräte bildeten sich über den Zeitverlauf außerdem kontinuierlich neue Bindungen und Zugehörigkeiten zwischen beteiligten Unternehmen. Zweitens stellten diese drei Gruppen von Akteuren den Kern des sich formierenden Mobile Business Ecosystems dar, da sie wesentlich an der Entwicklung, an der Herstellung und dem Vertrieb von mobilen Endgeräten, von Software und Hardware sowie von Mobilfunknetzwerken beteiligt waren. Schließlich konnte in der gewählten Zeitspanne ein rascher Anstieg in Bezug auf die Einführung und Nutzung von Smartphones sowie die Entstehung von mehreren neuen mobilen Plattformen wie iOS, Android OS, LiPS, LiMo oder webOS beobachtet werden. Jeder Versuch, die Zukunft der mobilen Telekommunikation zu verstehen, erfordert daher ein Verständnis für die Entwicklung des Mobile Business Ecosystem in den letzten beiden Jahrzehnten.

Die Mobilfunkbranche agiert sehr dynamisch, was vor allem durch die kontinuierlichen technologischen Fortschritte bedingt ist. Die enormen Markttchancen haben zu einem Eintritt einer Vielzahl neuer Marktteilnehmer geführt, während sich andere Marktteilnehmer neu positionieren mussten. Daneben haben die Unternehmen ihre Aktivitäten auf benachbarte Wertschöpfungsstufen ausgedehnt. So hat sich beispielsweise Apple Computer Inc. in diesem Kontext in Apple Inc. umbenannt, was eine Ausdehnung der Geschäftsbereiche auf z. B. digitale Dienstleistungen und digitale Produkte reflektiert. Dieses Phänomen wurde auch bei MNOs beobachtet, die sich aufgrund ihrer einzigartigen Marktposition aktiv in anderen Bereichen als ihrem Kerngeschäft einbrachten (z. B. als Portalanbieter, Inhaltsanbieter und Anwendungsentwickler – damit jedoch nur leidlich erfolg-

reich waren). Die Abbildung des Mobile Business Ecosystems mittels linearer, eindimensionaler Supply Chain-Prozesse (sogenannter Pipeline-Geschäftsmodelle) ist daher unzureichend. Die Zusammenhänge sind als Wertschöpfungsnetzwerk zu betrachten. Die Mobilfunkbranche kann als ein komplexes System mit zahlreichen zwischenbetrieblichen Beziehungen über verschiedene Segmente hinweg beschrieben werden.

Der Erfolg von Smartphones und Tablets hat zu einem Wettbewerb zwischen mobilen Plattformen im Mobile Business Ecosystem geführt. Mehr als 40–50 verschiedene mobile Plattformen existierten im Jahr 2010, wobei sieben dieser Plattformen seinerzeit ca. 97 % des gesamten Marktes bedienten (Basole und Karla 2011). Zu den Hauptakteuren gehörten seinerzeit Symbian, Windows Mobile, BlackBerry, webOS, mehrere Varianten Linux-basierter Plattformen sowie die beiden Marktführer Apple iOS und Android OS.

Die in den vorhergehenden Kapiteln beschriebene Steigerung der Nutzung mobiler Datendienste wurde durch die Einführung von Smartphones und Tablets maßgeblich beeinflusst. Die Einführung innovativer Konzepte im Management der einzelnen mobilen Plattformen führte dazu, dass zwischenzeitlich neben dem Mobile Business Ecosystem nun auch jede einzelne mobile Plattform ihr eigenes Ecosystem etabliert hat. Diese Entwicklung wurde von Apple durch Einführung des iPhone im Jahr 2007 ausgelöst. Das Endgerät war hier eng mit der vom Unternehmen angebotenen iTunes-Software verknüpft und hat sich seitdem zu einem kommerziellen und kulturellen Phänomen entwickelt. Der Erfolgsfaktor bestand und besteht somit nicht nur im Gerät selbst, sondern auch im hoch-integrierten System des App Stores als Bestandteil des iTunes Stores, welcher einen einfachen Download von Anwendungen und Inhalten sowie eine einfache Verwaltung und integrierte Zahlungswege ermöglichte. Das führte wiederum dazu, dass Content-Provider den Weg über den App Store zum Kunden suchten.

Der Erfolg von Apples App-Store-Konzept regte andere Marktbeteiligte dazu an, ihre eigenen Platform Ecosystems zu entwickeln. App Stores dienen als elektronische Märkte für digitale Güter und ermöglichen den Marktteilnehmern des Ecosystems eine Zusammenarbeit. Über die App Stores können Anwendungsentwickler und Servicedienstleister ihre Angebote für eine bestimmte Plattform anbieten und vertreiben.

Seit der Einführung im Jahr 2007 konnten sehr bemerkenswerte Entwicklungen beobachtet werden: Während MNOs ihre Kontrolle und ihren Einfluss auf das Mobile Business Ecosystem weitgehend verloren haben, konnten Plattformanbieter und Anwendungsentwickler ihren Einfluss deutlich verbessern. App Stores, so zeigt die Entwicklung, sind das primäre Gateway für Endbenutzer zu mobilen Anwendungen und Inhalten. Folglich werden plattformgebundene App Stores auch in der Zukunft eine entscheidende Rolle bei der Entwicklung des Mobile Business Ecosystems spielen.

Die Entstehung der Mobile Platform Ecosystems hat insbesondere die Anwendungsentwickler deutlich positiv beeinflusst. Vor der Einführung von App Stores war der Marktzugang für diese Gruppe recht begrenzt. Anwendungsentwickler sahen sich in der Regel dominierenden MNOs gegenüber. Um ihre Anwendungen im jeweiligen Portal des MNOs anbieten zu können – was den traditionellen Zugriffskanal für mobile Nutzer darstellte –

musste ein Vertragsabschluss zwischen diesen Parteien stattfinden. MNO-Portale, die einst die Verbreitung von Inhalten dominierten, verloren im Kontext von Mobile Platform Ecosystems ihre Bedeutung im Vergleich zu den App Stores der Plattformanbieter. Obwohl die Nutzer häufig auch die Möglichkeit hatten, eine Anwendung direkt von der Webseite des Entwicklers herunterzuladen, wurde diese Option nur selten genutzt, da die Transaktionskosten zu hoch waren. Die Einführung von integrierten App Stores hat die Spielregeln grundsätzlich verändert. Anwendungsentwickler können ihre Produkte seitdem auf zweiseitigen elektronischen Märkten anbieten und profitieren von gesenkten Markteintrittsbarrieren, wie reduzierten Suchkosten und der einfachen Handhabung von Zahlungsprozessen. Dies hat zu einem massiven Eintritt vieler kleiner und mittelständischer Software-Unternehmen sowie zu einer enormen Anzahl von selbstständigen Entwicklern geführt. Zwei Aspekte gilt es hierbei zu beachten: Obwohl große aktive Entwicklerstudios existieren, boten viele aktive Entwickler nur eine geringe Anzahl von Anwendungen an, in vielen Fällen nur eine einzige Anwendung in einem bestimmten App Store. Zudem wurde ein Entwicklungsansatz für eine parallele Entwicklung einer Anwendung für mehrere mobile Plattformen erst im Verlauf der Zeit entwickelt.

Das bereits angedeutete Wachstum im Bereich der mobilen Plattformen in den vergangenen Jahren ist insbesondere auf den Markteintritt von iOS und Android OS zurückzuführen. Einige Plattformen haben darüber hinaus Änderungen erfahren. So wurde aus Palm OS zwischenzeitlich HPs webOS, welches aber nach einer kurzen Phase der Aktivität wieder eingestellt wurde. Auch im Segment der Endgerätehersteller haben sich Veränderungen in den vergangenen Jahren ergeben. Beispielhaft sei der Markteintritt von Huawei, ZTE, Samsung, Xiaomi, LG, Dell oder Lenovo als große Anbieter mit weltweitem Aktionsradius genannt. Dieses enorme Wachstum im Mobile Business Ecosystem deutet sowohl auf das globale Wachstum der Branche als auch den Wert von Allianzen – insbesondere im Android OS Ecosystem – hin. Spannend sind auch die Bestrebungen von Huawei zur Etablierung eines eigenen Betriebssystems mit entsprechendem Ecosystem.

7.4.1 Entwicklung der Mobile Platform Ecosystems

Interessant für das Verständnis der Entwicklung des Mobile Business Ecosystems im Zeitraum 2007 bis 2011 und der gesamten Branche sind zudem die unterschiedlichen Strategien der einzelnen Anbieter mobiler Platform Ecosystems, der Endgerätehersteller und der MNOs. Es war lange Zeit nicht selbstverständlich, mit jedem mobilen Endgerät jedes beliebige Mobilfunknetzwerk nutzen zu können. Über den Direktvertrieb (welcher aufgrund der direkten Kundenbeziehung eine bedeutende Rolle in vielen nationalen Märkten spielte) hatten MNOs eine bedeutsamere Stellung inne, als dies heutzutage der Fall ist. In die andere Richtung betrachtet offenbaren sich hier ganz unterschiedliche Strategien der Anbieter mobiler Plattformen. Während beispielsweise Google mit seiner Android OS-Plattform bestrebt war, recht früh eine möglichst breite Abdeckung über Partnerschaften mit vielen MNOs zu erzielen, agierte Apple mit iOS völlig anders. Apple strebte

zunächst eine monopolartige Abdeckung einzelner nationaler Märkte bis zu einer gewissen Sättigungsgrenze an, bevor die exklusive Bindung an ausgewählte Partner zu Gunsten einer breiten Bedienung der Märkte umgestellt wurde. So kann zwischen 2007 und 2011 ein deutlicher Anstieg in der durchschnittlichen Anzahl von Partnerschaften mit mobilen Plattformen je Endgerätehersteller festgestellt werden. Endgerätehersteller streben also eine Diversifizierung ihres Angebotes über die installierten Betriebssysteme an. Ausnahmen bilden natürlich diejenigen Plattformen, welche bereits durch einen Endgerätehersteller bereitgestellt wurden. Beispiele hierfür sind Apple oder BlackBerry, deren Betriebssysteme nur für hauseigene Geräte lizenziert waren und im Falle von Apple immer noch sind. Insgesamt zeigt sich, dass sich das Mobile Business Ecosystem heutzutage auf wenige mobile Plattformen konzentriert und Apples iOS-Ableger und Android OS den Markt weitestgehend beherrschen.

Die Abb. 7.9 zeigt eine Visualisierung des Mobile Business Ecosystems im Jahr 2010. Die betrachteten Segmente der Mobile Platform Provider, Endgerätehersteller und MNOs sind darin als Knoten dargestellt. Die Größe der Knoten zeigt den weltweiten Marktanteil der Plattformen. Eine Kante verbindet ein Unternehmen mit einer Plattform, wenn ein Endgerätehersteller ein Gerät mit dem entsprechenden Betriebssystem ausliefert oder ein MNO ein Gerät mit diesem Betriebssystem anbietet.

Einige generelle Beobachtungen können gemacht werden: Während Symbian – dominierende Plattform der Zeiten vor der Einführung von Smartphones im Jahr 2007 – noch 2010 als führende Plattform angesehen werden kann, hat vor allem das Wachstum von Apple iOS, BlackBerry, Windows Mobile und Android OS zu einer Verringerung des

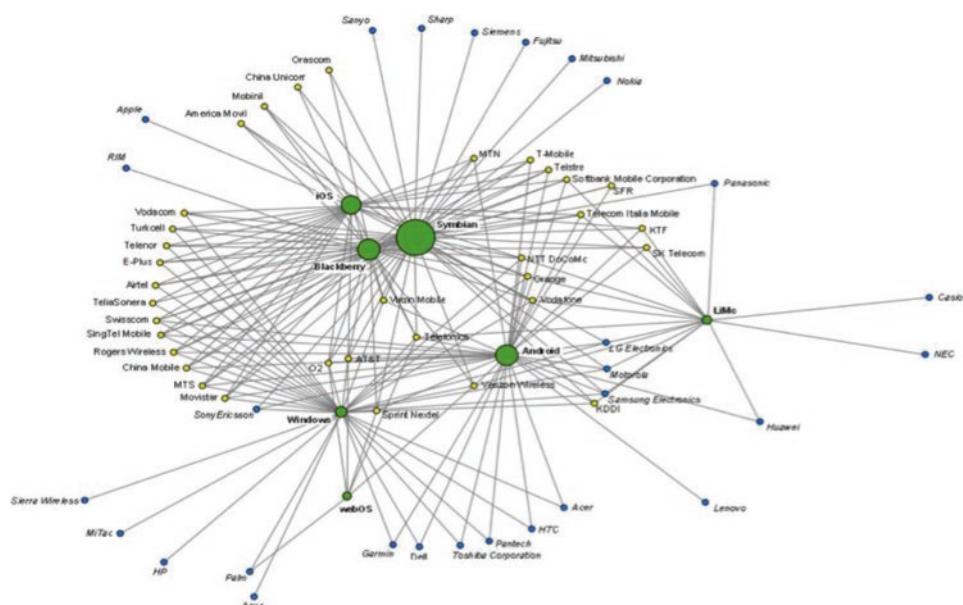


Abb. 7.9 Mobile Business Ecosystem 2010 (Basole und Karla 2011, S. 318)

Marktanteils von Symbian geführt. Diese Feststellung bestätigt sich auch durch das fundamental langsamere Wachstum der Anzahl von aktiven Entwicklern für die Symbian-Plattform. Im Gegensatz dazu ist die Zahl aktiver Entwickler vor allem für Apple iOS und Android OS immens gestiegen. Eine weitere wichtige Beobachtung im betrachteten Zeitrahmen ist, dass mehrere Endgerätehersteller (z. B. Samsung, Motorola und LG) Geräte mit unterschiedlichen Plattformen anboten, was darauf hindeutet, dass bis dahin keine einzelne führende Plattform am Markt existierte und daher jeweils mehrere Lizenzierungsvereinbarungen getroffen wurden. Interessant ist die relative Position der Plattform Windows Mobile im Mobile Business Ecosystem, da diese zu keinem Zeitpunkt eine zentrale Rolle gespielt hat. Eine ähnliche Beobachtung kann für LiMo, eine der Linux-basierten Plattformen, gemacht werden. Mit der Einführung der Windows Phone 7-Betriebssystemgeneration konnte jedoch zumindest ein rasantes Wachstum der Anzahl der aktiven Entwickler für Windows Phone 7 beobachtet werden. Dies reichte letztlich dennoch nicht, um den verspäteten Start in die Smartphone-Welt noch auszugleichen. Es konnte auch festgestellt werden, dass einige der größeren MNOs (z. B. AT&T, Vodafone, Orange und T-Mobile) eine größere Anzahl von Plattformen und Endgeräten anboten.

Vor dem Jahr 2007 konnten mit Symbian, Windows Mobile und BlackBerry drei Cluster im Mobile Business Ecosystem identifiziert werden, wobei Symbian die klar dominierende Plattform mit fast 75 % des gesamten Marktes darstellte. Nahezu alle großen Endgerätehersteller und MNOs nutzten die Symbian-Plattform. Auf Platz 2 der Bedeutungsrangliste folgte Windows Mobile. Auffallend war, dass es mehrere kleinere Endgerätehersteller gab, die ausschließlich die Windows-Mobile-Plattform in ihre Produktpalette integrierten.

Im Jahr 2007 stellte Apple die erste Generation des iPhone mit dem Betriebssystem iOS vor. Angesichts des enormen Hypes, der radikalen technologischen Innovationen und der attraktiven Gestaltung des iPhone hatte die iOS-Plattform eine unmittelbare Auswirkung auf das Mobile Platform-Ecosystem. Im Jahr 2007 verzeichneten zwei andere Plattformen ihr Debüt: Zum einen wurde Android veröffentlicht, eine von Google unterstützte Plattform, die von der Open Handset Alliance, einer Gruppe von führenden Technologieunternehmen, getragen wurde. Zum anderen wurde die Plattform LiMo eingeführt, eine Linux-basierte Plattform, die vor allem von Technologieunternehmen aus Europa und Asien und einigen Mitgliedern der Android-Plattform unterstützt wurde.

Einige Einzelbeobachtungen sollen im Folgenden hervorgehoben werden: Beachtenswert im Mobile Business Ecosystem im Jahr 2008 war die rasche Zunahme an Geschäftsbeziehungen zwischen Apple und MNOs. Daneben war in diesem Jahr zu erkennen, dass BlackBerry, Windows Mobile und Android Marktanteile hinzugewinnen konnten, während sich die Führungsposition der Symbian-Plattform weiter abschwächte. Im Jahr 2008 fand zudem eine Konsolidierung unter den Linux-Plattformen statt, da LiPS ankündigte, sich der LiMo-Plattform anzuschließen. In Bezug auf das Jahr 2009 konnte ein kontinuierliches Wachstum der Marktanteile von iOS und Android einerseits sowie eine signifikante Abnahme der Anteile von Symbian und einer Stagnation der Marktanteile von BlackBerry, Windows Mobile und LiMo andererseits festgestellt werden. Im Jahr 2010 konnte

sich noch keine individuelle dominierende Plattform herausbilden. Sowohl für Windows Mobile als auch Symbian konnte ein verringriger Marktanteil festgestellt werden, während BlackBerry relativ stabil geblieben ist. Eine der interessantesten Beobachtungen ist jedoch, dass Android OS einen großen Anstieg des Marktanteils verzeichnen konnte, was darauf zurückzuführen ist, dass eine zunehmende Zahl von Endgeräteherstellern Android OS als ihre bevorzugte Plattform annahmen und MNOs die Plattform zunehmend in ihr Serviceangebot integrierten. Zweifellos wies zu diesem Zeitpunkt Android die größte Dynamik unter allen mobilen Plattformen auf, obwohl sich dies beispielsweise nicht eindeutig in der Anzahl der aktiven Anwendungsentwickler für die Plattform widerspiegeln. Die Strategie Googles als Mobile Platform Provider, mittels einer breiten Diversifizierung den Marktanteil zu steigern, scheint bereits zu diesem Zeitpunkt erfolgreich zu sein.

Die sich fortlaufend verändernden Strukturen des Mobile Business Ecosystems hatten enorme strategische und wirtschaftliche Auswirkungen auf die Akteure in allen Marktsegmenten der Mobilfunkbranche. Das hohe Tempo der Umstellung des Marktes sowie die wachsende Nachfrage der Verbraucher führten zu einer engeren Zusammenarbeit der wichtigsten Beteiligten. Mobile Platform Provider spielten und spielen eine besonders wichtige Rolle innerhalb der konvergierenden Mobilfunkbranche, da sie die Erstellung und Distribution von neuen Anwendungen und Inhalten ermöglichen und vorantreiben. In der Tat bieten die mobilen Plattformen mit den an sie angeschlossenen zweiseitigen Marktplätzen für Apps und Inhalte deren Anbietern einen vereinfachten Marktzugang. Hieraus lassen sich wiederum Vorteile für viele Akteure innerhalb des Mobile Business Ecosystems generieren.

Markteffekte haben in der Zeit seit 2010 für eine massive Bereinigung gesorgt. Die Entwicklung vieler kleinerer mobiler Plattformen wurde eingestellt. Einige Plattform-Betreiber sahen sich bedeutsamen technischen Herausforderungen gegenübergestellt und haben zwischenzeitlich weitestgehend das Feld räumen müssen, z. B. Microsoft oder BlackBerry. Weltweit haben sich heute zwei bedeutsame Plattformen in verschiedenen Ausprägungen durchgesetzt, die durch eine Ecosystem-Strategie der Betreiber massiv unterstützt werden: Apples mobile Plattformen (ursprünglich iOS) sowie die auf Android OS basierenden Plattformen.

7.4.2 Auswirkungen auf Netzbetreiber

Eine entscheidende Veränderung für MNOs ging mit der Einführung des App Store-Konzepts einher: Die Kontrolle über Inhalte und Anwendungen sowie insbesondere auch über die Behandlung von Zahlungsvorgängen lag ursprünglich ausschließlich bei ihnen, denn die MNOs waren die einzigen Marktteilnehmer mit einer vertragsgebundenen direkten Beziehung zum Konsumenten. In der App Economy gilt dies nicht mehr. Hier liegt die Kontrolle deutlich auf Seiten der Mobile Platform Provider und teilweise bei den Endgeräteherstellern.

Auch in einem anderen Bereich wirkt sich die Entwicklung der App Economy aus: In der Vergangenheit wurde die mobile Datennutzung vor allem durch mobile Portale der MNOs

angetrieben. MNOs haben seit jeher Zusatzdienste zum reinen Verbindungsgeschäft von Endgerät zu Endgerät bzw. zum Internet in ihrem Angebot gehabt. Die SMS (Short Message Service) war ein solches Zusatzgeschäft, welches sich in den 1990er- und 2000er-Jahren zur Cash-Cow der Branche entwickelte. Nach zunächst großen Nutzerraten und hohen Zuwächsen erfolgt der Einbruch bei SMS mit Verbreitung von Smartphones und der Verfügbarkeit von kostenfreien Angeboten wie WhatsApp oder iMessage. Abb. 7.10 zeigt die Entwicklung der SMS zwischen 2009 und 2018 vor dem Hintergrund der seit 2012 wachsenden WhatsApp-Nutzerzahlen. Auf dem Höhepunkt des SMS-Volumens wurden allein in Deutschland fast 60 Milliarden SMS im Jahr 2012 versendet. Der Versuch der MNOs, die SMS mit der Multimedia-Erweiterung MMS zukunftsfähig zu machen, kann aus verschiedenen Gründen als gescheitert angesehen werden. MMS wurde nicht von der Anwenderperspektive aus entwickelt und war für den Nutzer technisch viel zu kompliziert. Bei SMS kam diese Schwäche nicht ans Tageslicht, da es als reines Text-Messaging ein einfaches Interface besaß. SMS war nur scheinbar günstig, denn die Netzbetreiber erzielten damit hohe Gewinnmargen. MMS wurde dann preislich als leistungsfähigere Erweiterung der SMS mit einem zu hohen Preis am Markt platziert. Nebenbei war der eigentliche Anlass zur Entwicklung von MMS ein defensiver: MMS sollte verhindern, dass das offene Internet in die mobile Welt einzog. Die Entwickler von WhatsApp haben bei allen kritikwürdigen Schwächen, insbesondere im Bereich des Datenschutzes, ein vergleichsweise attraktives und intuitiv handhabbares Produkt geschaffen, das für die Anwender zunächst kostenfrei daherkommt. Aktuell hat der WhatsApp-Dienst nahezu 60 Millionen Nutzer in Deutschland.

Doch mit der Profilierung der App Stores veränderte sich die Rolle der MNOs. In der Tat fürchteten diese nur wenige Szenarien so sehr wie die Degradierung zu sogenannten reinen *Bit-Pipes*. Mit diesem Begriff werden Service-Provider bezeichnet, welche im Kern

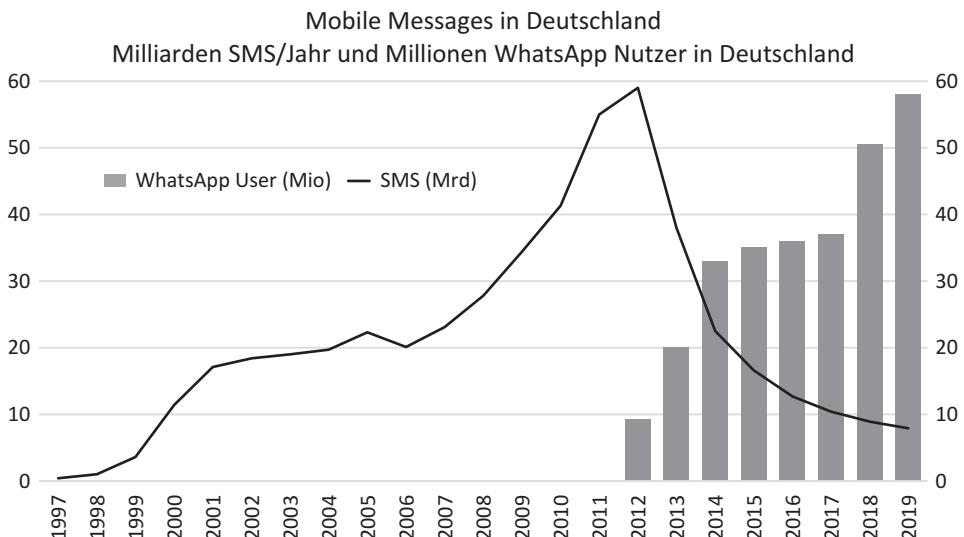


Abb. 7.10 Versandte SMS von 2000 bis 2019 und aktive WhatsApp Nutzer in Deutschland (Statista 2021g; Geschäftsberichte)

die Netzwerke mit der entsprechenden Bandbreite bereitstellen, ohne jedoch im Rahmen von Mehrwertdienstangeboten über die Nutzungsentgelte hinaus zu profitieren. Heutzutage haben die MNOs weitgehend genau diese Rolle inne. Die enge Verbindung zwischen Mobile Platform Providern und Endgeräteherstellern verdeutlicht dies und führte in der Vergangenheit zu umfangreichen gemeinsamen Wertschöpfungsaktivitäten zwischen diesen beiden Segmenten, mit negativem Einfluss auf die Bedeutung der MNOs.

Als Over The Top (OTT) werden Dienste im Internet bezeichnet, die über die vom Internet Service Provider bzw. MNO zur Verfügung gestellte Verbindung angeboten werden. Unter den mobilen OTT-Angeboten sind Messenger-Dienste und Social Media-Dienste besonders erfolgreich. Das Erfolgsrezept hierfür liegt in der ständigen Verfügbarkeit des Dienstes unabhängig vom jeweiligen Standort. Abb. 7.11 zeigt die Anteile der deutschen Mobilfunkkunden, die die populärsten OTT-Angebote nutzen.

Für die OTT-Anbieter ergeben sich aus der Kombination von örtlichen und zeitlichen Nutzungsprofilen mit den nachgefragten Inhalten interessante Verwertungsmöglichkeiten bei der zielgerichteten Platzierung von Werbung. Die damit erzielten Gewinne sind sehr hoch. Aufgrund der politisch gewollten und in den meisten Staaten gesetzlich fixierten Netzneutralität erfolgt die Durchleitung der OTT-Daten durch die Netzbetreiber für die OTT-Anbieter kostenfrei. Im Vergleich zu den OTT-Anbietern erscheinen die Umsätze und Gewinne der europäischen Netzbetreiber, die durch ihre Investitionen diese Services erst ermöglichen, geradezu bescheiden. Das gilt insbesondere in Europa. Abb. 7.12 zeigt

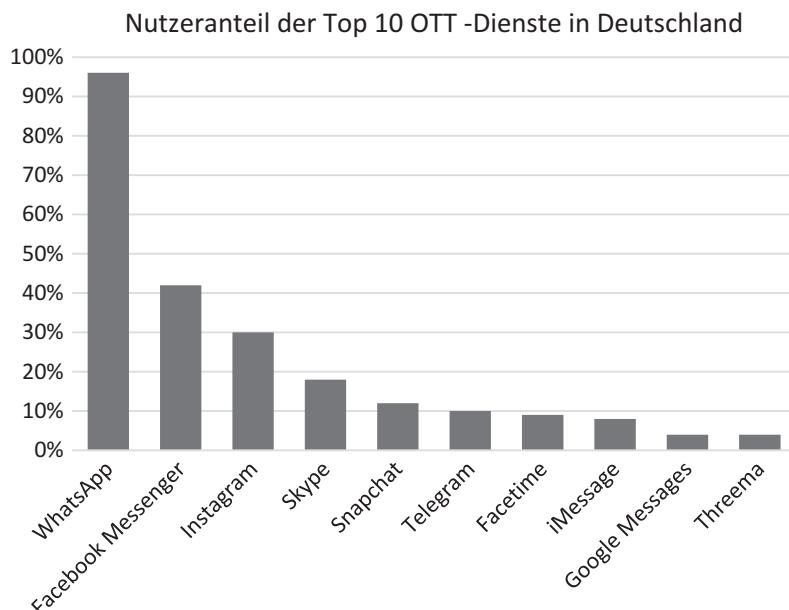


Abb. 7.11 Nutzeranteil der Top 10 Over The Top-Dienste in Deutschland (Bundesnetzagentur 2020b)

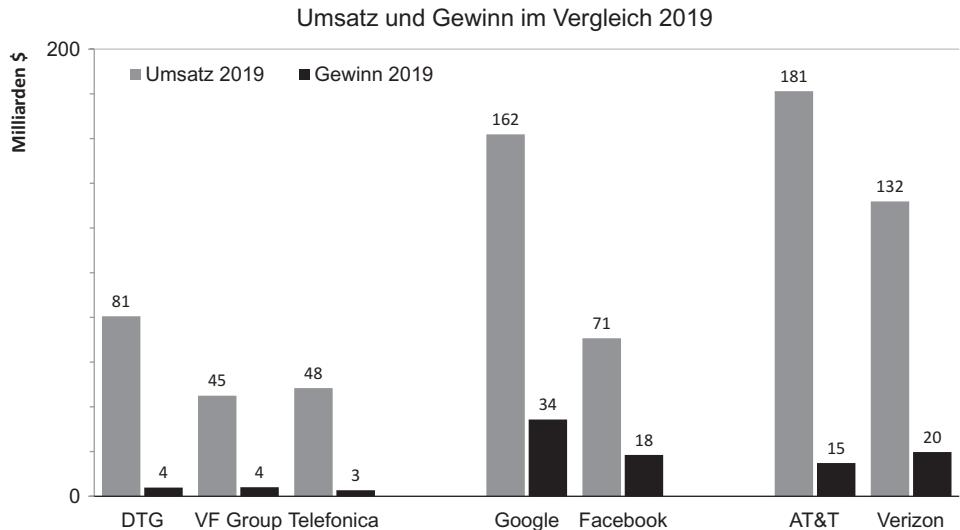


Abb. 7.12 Umsatz und Gewinn von europäischen und amerikanischen MNOs und Over The Top-Anbieter im Jahr 2019 im Vergleich laut Geschäftsberichten

einen Vergleich der Gesamtumsätze der drei großen europäischen MNOs, die in Deutschland aktiv sind, mit den bekanntesten OTT-Anbietern. Der Facebook-Konzern umfasst die drei meistgenutzten OTT-Angebote aus Abb. 7.11. Zum Vergleich sind die beiden führenden US-amerikanischen Mobilfunkbetreiber AT&T und Verizon aufgeführt, die durch die eigene Größe den OTT-Anbietern zumindest eine Skalenökonomie entgegensetzen können. Den europäischen Mobilfunkunternehmen fehlen sowohl die starke Position gegenüber den OTT-Anbietern als auch die Skaleneffekte eines großen einheitlichen Wirtschaftsraumes. Innerhalb der EU gibt es bei 27 Mitgliedsstaaten mehr als 100 Mobilfunknetze und MNOs. Dagegen haben die USA bei vergleichbarer Bevölkerungsgröße nur drei nationale Netze. Der gesättigte Privatkundenmarkt und die Kommoditisierung der zentralen Netzbetreiber-Dienstleistung erzeugen einen hohen Preisdruck, der bei der Zersplitterung der Netze nicht durch Skaleneffekte ausgeglichen werden kann. Beratungsunternehmen empfehlen den europäischen Mobilfunkunternehmen deshalb, ihr Angebot durch zusätzliche Dienste auszuweiten. Dazu können Anwendungen im Bereich Smart Home und Verkehrsmanagement gehören, aber auch eine Ausweitung der Aktivitäten im Bereich Entertainment (TV, Musik, Gaming) (Groene et al. 2017). Die Entwicklung des Internet of Things (IoT) im Mobilfunksektor bietet hier zusammen mit der Mobilfunkgeneration 5G eine neue Chance für Netzbetreiber, da für spezifische IoT-Anwendungen eine aktive Mitwirkung des Netzbetreibers durch eine geeignete Konfiguration des Netzes erforderlich ist. Die politische Unterstützung zur Überwindung der Zersplitterung des europäischen Mobilfunkmarktes durch EU-weite Regulierung, sowie durch Bildung länderübergreifender Betreiber und Netze ist nicht in Sicht.

Für die Nutzer der Endgeräte hat sich die Entscheidungssituation bezüglich einer geeigneten Kombination aus mobilem Gerät, Mobilfunknetzwerk und Plattform erheblich vereinfacht. Sie sind letztlich nicht unbedingt daran interessiert, welche Plattform in einem technischen Sinn sie nutzen. Jedoch ist für sie bedeutsam, welche Anwendungen verfügbar sind, wieviel diese kosten und wie integriert das gesamte Ecosystem ist. Natürlich spielen auch Aspekte des Marketings, z. B. Markenimage eine nicht unbedeutende Rolle. Das Mobilfunknetzwerk spielt jedoch lediglich noch in der Frage der Verfügbarkeit eine Rolle in dieser Entscheidungsfindung.

Unterschiede zwischen einzelnen mobilen Plattformen und ihren gekoppelten App Stores zeigen sich in mehreren wichtigen technischen und marketingbezogenen Merkmalen; insbesondere hinsichtlich der jeweiligen Anzahl an Installationen, der Zahl der verfügbaren Anwendungen, der Zahl der aktiven Entwickler, der für die Entwicklung notwendigen Lernkurve, der Anreize für Entwickler und schließlich in Bezug auf wichtige Aspekte wie Umsatzpotenzial und Erlösmodelle.

Plattform Ecosystem-Konzepte haben sich zu einem zentralen Merkmal vieler neuer Geschäftsmodelle entwickelt und sind insbesondere in der Mobilfunkbranche von Bedeutung. Der Erfolg einer mobilen Plattform ist untrennbar mit ihrem Mobile Platform Ecosystem verbunden. Zu diesem Ecosystem zählen die jeweils integrierten App Stores für Anwendungen und Inhalte. Daneben ist aber auch eine Integration von Desktop- und Cloud-Lösungen zu nennen. Des Weiteren legen Nutzer erfahrungsgemäß Wert auf eine benutzerfreundliche Lösung zur Datensicherung sowie eine nahtlose Integration von Social Media-Diensten. Die Verbindung mit gängigen Zahlungsmethoden ist insbesondere für die Betreiber der App Stores als elektronische Marktplätze von Bedeutung. Die Entwicklung von sicheren und preiswerten Zahlungsverfahren in den vergangenen Jahren hat hier bedeutend zur Akzeptanzsteigerung beigetragen. Zukünftig wird der Wert einer Plattform für den Nutzer insbesondere auch über die erreichbaren Medieninhalte (Spiele, Bücher, Musik, Filme, ...) definiert.

7.5 Fragen

1. Welche Arten von Unternehmen wirken am Aufbau eines Mobilfunknetzes mit?
2. Was ist die Bundesnetzagentur?
3. Warum gibt es Lizenzen für die Nutzung von Mobilfunkfrequenzen? Was würde ohne Lizenzen passieren?
4. Welche Arten von Betriebs- und Wartungsaufgaben entstehen in einem Mobilfunknetz? Wie heißen die Betriebsteile, die für die Wahrnehmung dieser Aufgaben verantwortlich sind?
5. Welche Typen von MVNO kennen Sie?
6. Erstellen Sie aus allgemein zugänglichen Quellen (Internet o. ä.) eine Liste der in Deutschland tätigen MVNOs und ihrer Geschäftsmodelle.
7. Was versteht wird unter der sogenannten „App Economy“ verstanden?

8. Wie war die Situation für Anwendungsentwickler vor der Entstehung der Mobile Plattform Ecosystems?
9. Welche mobilen Plattformen bedienen nahezu den gesamten Markt im Mobile Business Ecosystem?
10. Recherchieren Sie die Entwicklung der mobilen Plattformen Android OS (als Beispiel für Wachstum) und Symbian (als Gegenbeispiel).
11. Welche Rolle spielen App Stores beim rasanten Wandel der Wertschöpfung im Mobile Business Ecosystem?
12. Was wird unter Bit Pipes verstanden?
13. Was ist ein OTT-Anbieter? Nennen Sie Beispiele.
14. Welche Anforderungen stellen Nutzer an ein mobiles Endgerät/eine Plattform?

Literatur

- Basole RC, Karla J (2011) On the evolution of mobile platform ecosystem structure and strategy. Bus Inf Syst Eng 53(5):313–322. Springer. <https://doi.org/10.1007/s12599-011-0174-4>
- Bundesnetzagentur (2020a) Grafiken Jahresbericht 2019. Bonn. https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Allgemeines/Presse/Pressemitteilungen/JB2020_ZDF.pdf?__blob=publicationFile&v=4. Zugegriffen am 29.08.2021
- Bundesnetzagentur (2020b) Nutzung von OTT-Kommunikationsdiensten in Deutschland – Bericht 2020. Bonn. https://www.bundesnetzagentur.de/SharedDocs/Mediathek/Berichte/2020/OTT.pdf?__blob=publicationFile&v=5. Zugegriffen am 26.08.2021
- Bundesnetzagentur (2021) Teilnehmerentwicklung im Mobilfunk. Bundesnetzagentur. Bonn. https://www.bundesnetzagentur.de/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Marktbeobachtung/Mobilfunkteilnehmer/artikel.html?nn=268232. Zugegriffen am 29.08.2021
- Ericsson (2020) Ericsson mobility report – June 2020. Stockholm. <https://www.ericsson.com/en/mobility-report>. Zugegriffen am 24.06.2021
- Gottesman B (2020) Readers choice awards 2020. PCMag. <https://uk.pcmag.com/smartphones/125386/readers-choice-awards-2020-smartphones-carriers-and-mobile-operating-systems>. Zugegriffen am 29.08.2021
- Groene F, Navalekar A, Kramer Coakley M (2017) An industry at risk – commoditization in the wireless telecom industry. New York. <https://www.strategyand.pwc.com/gx/en/insights/2017/an-industry-at-risk/an-industry-at-risk.pdf>. Zugegriffen am 09.09.2021
- Legal Tribune Online (2021) EuGH gibt Klage der EU-Kommission statt: Bundesnetzagentur nicht unabhängig genug. Legal Tribune Online. https://www.lto.de/persistent/a_id/45906/. Zugegriffen am 09.09.2021
- Statista (2019) Marktanteile der Anbieter am Umsatz mit Netzwerktechnik im Bereich Mobilfunk weltweit im Jahr 2018. Statista. <https://de.statista.com/statistik/daten/studie/73663/umfrage/marktanteile-der-anbieter-von-netzwerktechnik-im-bereich-mobilfunk-weltweit/>. Zugegriffen am 29.08.2021
- Statista (2021a) Durchschnittlicher monatlicher Erlös pro Kunde (ARPU) von Telefonica Deutschland im Mobilfunk vom 1. Quartal 2009 bis zum 1. Quartal 2021. Statista. <https://de.statista.com/>

[statistik/daten/studie/162921/umfrage/arpu-von-telefonica-o2-germany-in-deutschland-nach-quartalen/](https://de.statista.com/statistik/daten/studie/162921/umfrage/arpu-von-telefonica-o2-germany-in-deutschland-nach-quartalen/). Zugegriffen am 29.08.2021

Statista (2021b) Durchschnittlicher monatlicher Erlös pro Kunde (ARPU) von Vodafone im Mobilfunk in Deutschland vom 2. Geschäftsquartal 2011/2012 bis zum 4. Geschäftsquartal 2020/2021.

Statista. <https://de.statista.com/statistik/daten/studie/163971/umfrage/arpu-von-vodafone-deutschland-im-mobilfunk/>. Zugegriffen am 29.08.2021

Statista (2021c) Durchschnittlicher monatlicher Erlös pro Kunde (ARPU) der Deutschen Telekom im Mobilfunk in Deutschland vom 1. Quartal 2009 bis zum 1. Quartal 2021. Statista. <https://de.statista.com/statistik/daten/studie/275502/umfrage/arpu-der-deutschen-telekom-im-mobilfunk-in-deutschland/>. Zugegriffen am 29.08.2021

Statista (2021d) Durchschnittliche monatliche Churn-Rate von Telefonica Deutschland im Mobilfunk vom 1. Quartal 2011 bis zum 1. Quartal 2021. Statista. <https://de.statista.com/statistik/daten/studie/326596/umfrage/monatliche-churn-rate-von-telefonica-o2-im-mobilfunk-in-deutschland/>. Zugegriffen am 29.08.2021

Statista (2021e) Annualisierte Churn-Rate von Vodafone im Mobilfunk in Deutschland vom 1. Geschäftsquartal 2010/2011 bis zum 4. Geschäftsquartal 2020/2021. Statista. <https://de.statista.com/statistik/daten/studie/237735/umfrage/annualisierte-churn-rate-von-vodafone-in-deutschland/>. Zugegriffen am 29.08.2021

Statista (2021f) Durchschnittliche monatliche Churn-Rate der Deutschen Telekom im Mobilfunk in Deutschland vom 1. Quartal 2009 bis zum 1. Quartal 2021. Statista. <https://de.statista.com/statistik/daten/studie/237715/umfrage/monatliche-churn-rate-der-deutschen-telekom-im-mobilfunk-in-deutschland/>. Zugegriffen am 29.08.2021

Statista (2021g) Anzahl der versendeten SMS in Deutschland von 2000 bis 2020. Statista. <https://de.statista.com/statistik/daten/studie/155052/umfrage/versendete-sms-in-deutschland-seit-2000/>. Zugegriffen am 29.08.2021



Mobile Anwendungssysteme

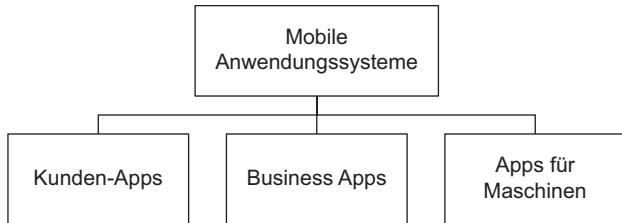
8

8.1 Einführung und Lernziele

In diesem Kapitel wird ein Überblick über mobile Anwendungssysteme gegeben (Abb. 8.1). Programme, die auf mobilen Endgeräten ausgeführt werden, werden als Apps bezeichnet. Anfangs waren es vor allem Privatpersonen und Konsumenten, die sich Apps über die App-Stores der einzelnen Hardware- bzw. Betriebssystem-Anbieter heruntergeladen haben und lokal installierten. Unternehmen versuchen, mit Hilfe dieser Apps Marketing und Werbung zu betreiben sowie die eigenen Produkte und Dienstleistungen zu verkaufen. Die Anwendungen dieser Gruppe werden als *Kunden-Apps* bezeichnet. Für die Unternehmen und deren Mitarbeiter stehen darüber hinaus zahlreiche *Business-Apps* zur Verfügung, die in die vorhandene IT-Infrastruktur integriert werden müssen. Im Mittelpunkt steht dabei die Unterstützung von Geschäftsprozessen durch mobile Endgeräte. Generell sind alle webbasierten betrieblichen Applikationen, z. B. Enterprise Resource Planning (ERP)-Systeme oder Customer Relationship Management (CRM)-Systeme auch mobil nutzbar. Als dritte Kategorie werden *Maschinen-Apps* behandelt, die beispielsweise zur Fahrassistenz oder in medizinischen Geräten genutzt werden (Verclas und Linnhoff-Popien 2012, S. 12 f.).

Aufgrund der besonderen Eigenschaften mobiler Endgeräte, also vor allem Ortsunabhängigkeit, Ortbarkeit, Identifizierbarkeit des Nutzers und Einfachheit der Nutzung, entstanden völlig neuartige Anwendungsfelder. Insgesamt ist das Angebot an mobilen Applikationen sehr groß. Es können daher in diesem Kapitel nur ausgewählte Beispiele vorgestellt werden. Während einige dieser Anwendungen in vielen Unternehmen nutzbar sind, konzentrieren sich andere Lösungen auf bestimmte Branchen. Ergänzend werden am Ende des Kapitels die wichtigsten Methoden zur Ortung mobiler Endgeräte und zur Identifikation der Nutzer durch Apps vorgestellt.

Abb. 8.1 Einsatzbereiche von mobilen Anwendungssystemen



► **Lernziele**

- Sie verstehen welche Chancen mobile Anwendungen für Marketingkommunikation und Werbung bieten
- Sie verstehen wie durch M-Shopping ein weiterer Verkaufskanal für den Handel entsteht
- Sie verstehen wie sich durch M-Ticketing und M-Payment Bezahlvorgänge vereinfachen lassen
- Sie verstehen welche Anwendungsmöglichkeiten sich innerhalb des Unternehmens durch Business Apps ergeben
- Sie verstehen wie durch Maschine-zu-Maschine-Kommunikation der Datenaustausch ohne menschliche Eingriffe erleichtert werden kann
- Sie verstehen wie die Position eines mobilen Endgerätes und die Identität des Nutzers bestimmt werden.

8.2 Kunden-Apps

Es handelt sich hierbei um Apps, die Kommunikation und geschäftliche Transaktionen zwischen Unternehmen und privaten Konsumenten ermöglichen. Bevor näher auf die verschiedenen Anwendungen eingegangen wird, gibt die nachfolgende Abb. 8.2 zunächst einen Überblick über beispielhafte Anwendungsbereiche:

8.2.1 Mobiles Marketing

Mobiles Marketing (M-Marketing) bedeutet die Nutzung von Mobilfunktechnik und mobilen Endgeräten im Rahmen von Marketingaktivitäten. Es umfasst sämtliche Kommunikationsmaßnahmen, die auf eine direkte und gezielte Beeinflussung der Einstellungen, Meinungen und Verhaltensweisen von Kunden abzielen und dem Aufbau bzw. der Sicherung von Wettbewerbsvorteilen dienen (Möhlenbruch und Schmieder 2002, S. 77; Steinhoff und Buse 2008, S. 440).

Die Marketingbotschaften zwischen Unternehmen und Konsument lassen sich auf unterschiedliche Weise austauschen. Beim mobilen Push-Marketing geht die Initiative vom Werbetreibenden aus; der Empfänger erhält die Werbeinformationen oder Angebote ohne eigenes Zutun. Hierbei besteht die Gefahr, dass unerwünschte Werbebotschaften verschickt

| Anwendungsbereich | Anwendungsbeispiele |
|----------------------|--|
| Marketing | <ul style="list-style-type: none"> - Mobile Werbekampagnen - Mobile Newsletter - Mobile Coupons - Mobile Gewinnspiele - Mobile Voting |
| Commerce | <ul style="list-style-type: none"> - Kauf von Gütern bzw. Diensten über mobile Netze und mobile Endgeräte |
| Ticketing | <ul style="list-style-type: none"> - Fahrscheine für öffentlichen Personennahverkehr, Bahn und Flugverkehr - Eintrittskarten für Sport- und Kulturveranstaltungen - Mobiles Parken |
| Payment | <ul style="list-style-type: none"> - Zahlung per Smartphone im stationären Handel - Zahlung per Smartphone für Online-Käufe - Zwei-Wege Identifikation für Online-Käufe - Mobile Geldübertragung |
| Entertainment | <ul style="list-style-type: none"> - Streaming/Download von Musik, Videos - Mobile Spiele |
| Fitness & Gesundheit | <ul style="list-style-type: none"> - Tracking von Sport-Aktivitäten - Trainingspläne - Austausch und Wettbewerb |

Abb. 8.2 Kunden-Apps im Überblick

werden, der Kunde sich belästigt fühlt und sich von dem Unternehmen abwendet. Beim mobilen Pull-Marketing fragt der Nutzer bestimmte Informationen gezielt beim Unternehmen nach. Die empfangenen Informationen können zwar für den Empfänger irrelevant sein, sie wurden jedoch auf seine Initiative übermittelt.

Sowohl die Push- als auch Pull-Strategie lassen sich nur mit dem Einverständnis des Adressaten erfolgreich betreiben. Rechtliche Vorgaben sind in jedem Fall zu beachten. Kunden sind verärgert, wenn sie unerwünschte Werbung erhalten. Für den Werbetreibenden gilt es, das daraus oftmals resultierende schlechte Image zu vermeiden. Die vorherige Zustimmung für den Empfang mobiler Werbebotschaften wird als *Opt-In-Verfahren* bezeichnet, die jederzeitige Widerrufung als *Opt-Out-Verfahren*. Das Opt-Out-Verfahren allein stellt keine rechtlich wirksame Einwilligung gemäß Datenschutzgrundverordnung (DSGVO) dar (Schreiber 2018). Beim einfachen Opt-In-Verfahren registriert sich ein Kunde z. B. auf einer Webseite oder per SMS und erteilt dem Unternehmen hiermit eine Zustimmung für den Empfang von Werbebotschaften. In der Regel bestätigt das Unternehmen diesen Vorgang. Beim doppelten Opt-In-Verfahren muss ein Interessent nach der Registrierung sein Einverständnis gegenüber dem Unternehmen nochmals bestätigen, beispielsweise durch Eingabe eines Kennwortes oder durch Anklicken eines Bestätigungslinks. Hierdurch wird verhindert, dass sich Dritte gegenüber dem Unternehmen mit falscher Identität anmelden (Sottek 2012, S. 24).

Obwohl der Schwerpunkt des mobilen Marketings in der Kommunikationspolitik liegt, sind auch in der Produkt-, Preis- und Distributionspolitik interessante Anwendungsmög-

lichkeiten gegeben (Weis 2018, S. 82). Die wichtigsten Einsatzbereiche von M-Marketing verdeutlicht Abb. 8.3, diese werden anschließend erläutert.

Mobile Werbung

Mobile Werbung ist eng verwandt mit dem Online Advertising bei Webseiten. Allerdings bietet es aufgrund der Eigenschaften mobiler Dienste ein deutlich erweitertes Spektrum der Einsatzmöglichkeiten und Verwendungszwecke. Die Zahl der verfügbaren mobilen Endgeräte zur Darstellung mobiler Werbung ist rapide gewachsen. Aufgrund des steigenden Leistungsumfangs der mobilen Geräte und der größeren verfügbaren Bandbreiten ist ein Trend zu multimedialer Werbung zu erkennen. Bedeutsam für die Werbeindustrie ist dabei die Möglichkeit der Zwei-Wege-Kommunikation. Dies bedeutet, dass der Nutzer über sein mobiles Endgerät unmittelbar auf die Werbung reagieren kann – ein deutlicher Unterschied zu Werbung in herkömmlichen Print- oder audiovisuellen Medien. Werbung in Printmedien integriert mittlerweile häufig eine Schnittstelle zu mobilen Endgeräten: QR-Codes in Printanzeigen können mit dem mobilen Endgerät gescannt werden und leiten zu einer Kampagnenseite oder weitergehenden Informationen weiter (Abschn. 5.5). Die Eins-zu-Eins-Beziehung zwischen Nutzer und Endgerät erlaubt der Werbeindustrie außerdem Einblicke in das Konsumentenverhalten, indem beispielsweise Daten getracked werden. Identifizierung eines Nutzers oder eines mobilen Endgerätes und Ortung sind dabei wichtige Elemente. Die gebräuchlichen Verfahren zu Ortung und Identifizierung mobiler Endgeräte werden in Abschn. 8.6 kurz dargestellt.

Bei mobiler Werbung werden verschiedene Werbemittel eingesetzt, beispielsweise Banner oder Poster, welche im Kopfbereich bzw. im Fußbereich einer mobilen Webseite eingeblendet werden. Daneben ist Werbung per SMS oder Messenger-Apps ein vielfach eingesetztes Werbemittel. Diese wird häufig über technische Partner abgebildet, welche ein geeignetes Gateway für den Versand großer Mengen von Nachrichten bereitstellen. Über Werbung finanzierte Nachrichtendienste per SMS waren die Vorreiter mobiler Werbung.

Der Effekt der Werbung wird im Mobile Advertising anhand der Impressions (oder Views), d. h. der Anzahl der Einblendungen auf dem mobilen Endgerät, oder anhand der Anzahl der Clicks auf mobile Werbemittel ermittelt. Entsprechend erfolgt auch die Abrechnung der Werbung über Cost-per-Impression oder Cost-per-Click. Ergänzende

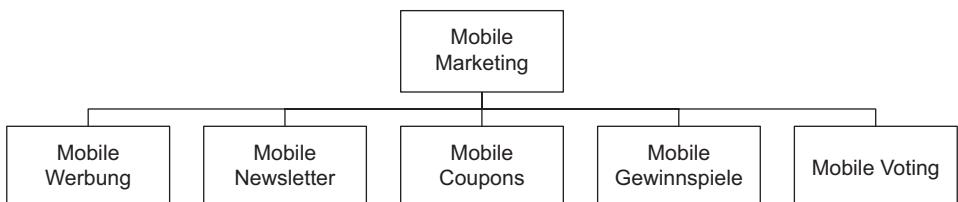


Abb. 8.3 Einsatzbereiche von Mobile Marketing

Kennzahl ist die Conversion Rate, anhand derer gemessen wird, ob sich ein Kunde aufgrund einer Werbung zum Kauf entschieden hat.

Mobile Newsletter

Mit Hilfe eines mobilen Newsletters werden Kunden in regelmäßigen Abständen über Angebote, Produktneuheiten und Verkaufsaktionen informiert. Die Werbebotschaft kann mit Fotos, Videos oder Musik untermauert werden. Wegen des kleineren Displays mobiler Endgeräte sollte der Newsletter responsiv bzw. adaptiv gestaltet werden. Responsives Webdesign passt das Layout der Website an die Displaygröße an.

Mobile Coupons

Bei mobilen Coupons handelt es sich um spezielle Angebote, Sonderaktionen oder Preisnachlässe, die nicht mehr in gedruckter Form als Gutscheine oder Rabattcoupons angeboten werden, sondern auf elektronischem Wege als E-Mail, SMS oder über eine App verteilt und vom Nutzer auf dem Smartphone gespeichert werden. Coupons enthalten häufig einen 2D-Barcode oder QR-Code und können an der Kasse mittels Scanner ausgelesen werden.

Mobile Gewinnspiele

Die Teilnehmer werden meistens über ein anderes Medium, wie Zeitschrift oder TV/Radio angesprochen, wobei die Rückmeldung zu dem jeweiligen Gewinnspiel mobil erfolgt. Oftmals wird dann eine SMS mit der Lösung oder dem Stichwort an eine Kurzwahlnummer geschickt. Über ein Gewinnspiel lassen sich Kundendaten, wie demografische Daten, Adressen und Präferenzen sammeln, um diese für einen zukünftigen Kundendialog zu speichern. Gemäß der Datenschutzgrundverordnung müssen die Teilnehmer eines Gewinnspiels allerdings eine separate Einwilligung abgeben, dass ihre Daten zu Werbezwecken verwendet werden dürfen.

Mobile Voting

Konsumenten haben hierbei die Möglichkeit, an Umfragen und Abstimmungen teilzunehmen. Wie bei mobilen Gewinnspielen kann die Abstimmung per SMS an eine Mehrwert-Kurzwahlnummer gesendet werden. Teilweise werden unter den Abstimmungsteilnehmern auch Gewinne ausgelost, um einen größeren Anreiz zur Teilnahme zu schaffen. Außerdem lassen sich gezielt Meinungsforschungsumfragen über das mobile Endgerät abwickeln.

8.2.2 Mobile Commerce

Als Mobile Commerce (M-Commerce) wird jede Art geschäftlicher Transaktionen bezeichnet, bei denen die Geschäftspartner im Rahmen von Leistungsanbahnung, -vereinbarung und -erbringung mobile Endgeräte und mobile Kommunikationsnetze einsetzen. Mobil wird ein Einkaufsvorgang dadurch, dass er nicht an ein festes Ladenlokal oder gar

Ladenöffnungszeiten gebunden ist. Mobil wird der Einkaufsvorgang ferner durch die Verwendung von Endgeräten, die ständig mitgeführt werden und über einen mobilen Internetzugang verfügen.

Der Verkäufer ermöglicht es seinen Kunden, einzelne oder sogar alle Phasen des Verkaufsprozesses mobil abzuwickeln. Hierunter fallen sämtliche Aktivitäten von der Geschäftsanbahnung über die Kaufvereinbarung, den Zahlungsvorgang bis hin zu Lieferung und Service (Abb. 8.4). Zumindest die ersten drei Schritte des Verkaufsprozesses können bei allen Online-Shops mobil abgewickelt werden, während die Auslieferung über Paketdienstleister oder durch persönliche Abholung des Käufers in einem Ladenlokal erfolgt. Bei digitalen Gütern wie z. B. Musik kann der gesamte Verkaufsprozess mobil erfolgen.

Mobile Kaufprozesse schmälern nicht automatisch die Erlöse des stationären Handels, sondern sie können das Einkaufserlebnis im Ladenlokal sogar fördern. Zu diesem Zweck stellen Händler mobile Shopping-Apps für verschiedene Service-Funktionen im Ladenlokal zur Verfügung. Beispielsweise können Navigations-Apps das Auffinden der nächsten Filiale ermöglichen. Innerhalb des Ladens können Apps die Suche nach bestimmten Artikeln erleichtern. Durch Scannen eines QR-Codes auf der Produktverpackung lassen sich weiterführende Informationen über Herkunft, Inhaltsstoffe und Verträglichkeit von Produkten, insbesondere von Lebensmitteln, abrufen. Ferner existieren Apps, die einen mobilen Preisvergleich ermöglichen sowie Produktbewertungen anderer Konsumenten anzeigen.

8.2.3 Mobile Ticketing

Mobile Ticketing ermöglicht Erwerb, Darstellung und die Kontrolle von Tickets über mobile Netze und mobile Endgeräte. Bedeutsame Anwendungen sind Fahrscheine für öffentliche Verkehrsmittel, Boarding Cards für Flugzeuge, Eintrittskarten für Sport- und Kulturveranstaltung sowie Parktickets.

Das elektronische Ticket ersetzt herkömmliche Tickets aus Papier. Zeitersparnis und Bequemlichkeit sind die wichtigsten Vorteile. Der Nutzer kann ein Ticket direkt bestellen und als Datei auf seinem mobilen Endgerät speichern. Die Kontrolle kann über einen mobilen Scanner erfolgen. Für die Realisierung mobiler Tickets existieren verschiedene Varianten:

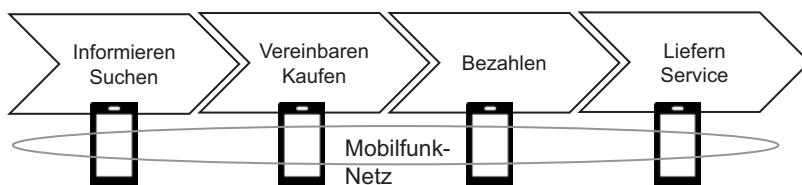


Abb. 8.4 Mobiler Verkaufsprozess

Ticketerwerb

Ein Ticket gilt entweder für eine bestimmte *Zeitdauer* oder für einen bestimmten *Anlass*. Im ersten Fall erfolgt der Erwerb des Tickets im Rahmen des *Check-In/Check-Out-Verfahrens*. Hierbei ist die Nutzungsdauer für den Preis des Tickets relevant. Der Kunde meldet sich zu Beginn der Nutzung in einem System an (Check-In). Wenn der Vorgang beendet wird, beispielsweise bei Verlassen eines Parkplatzes oder beim Ende einer Reise meldet sich der Nutzer wieder ab (Check-Out). Der Preis errechnet sich in diesem Fall aus der eingeloggten Zeit (beim Parken) oder aus der zurückgelegten Entfernung (bei einer Reise). Der Nachweis, dass ein Ticket ordnungsgemäß erworben wurde, ergibt sich, wenn zum Zeitpunkt einer Kontrolle der Check-In stattgefunden hat, jedoch noch nicht der Check-Out. Alternativ kann ein mobiles Ticket für eine allgemeine *Zugangs- oder Nutzungsberechtigung* erworben werden. Der Nutzer kauft eine Karte (Flug oder Konzertveranstaltung), anschließend wird ein personalisiertes Ticket in Form einer Datei auf das mobile Endgerät des Nutzers übertragen. Häufig werden die Ticketinformationen als zweidimensionaler Barcode auf dem Display dargestellt. Dieses Verfahren wird beispielsweise für die mobile Bordkarte bei Fluggesellschaften verwendet. Die Kontrolle erfolgt durch Einscannen des angezeigten Barcodes am Check-In-Schalter.

Kontrolle der Ticketgültigkeit

Die Kontrolle, ob ein gültiges Ticket erworben wurde, kann entweder im Online- oder im Offline-Prüfverfahren erfolgen. Beim Online-Prüfverfahren scannt der Kontrolleur das mobile Ticket und prüft über eine Mobilfunkverbindung in einem zentralen System, ob das Ticket gültig ist. Das Offline-Verfahren überprüft die Gültigkeit ohne bestehende Netzverbindung zu einem zentralen System, beispielsweise über ein mobiles Endgerät des Kontrolleurs. Zusätzlich lässt sich die Identität des Nutzers durch Vorlage von Ausweispapieren überprüfen.

Sicherheitsmaßnahmen

Zur Gewährleistung reibungsloser Nutzung und zur Verhinderung von Missbrauch werden an mobile Tickets hohe Sicherheitsanforderungen gestellt. Im Rahmen der Authentizitätsprüfung muss die Identität des Nutzers bewiesen werden können, um bei Verlust oder Diebstahl die missbräuchliche Verwendung des Geräts auszuschließen. Die einmal ausgegebenen mobilen Tickets dürfen nicht mehr modifiziert werden. Ansonsten besteht die Gefahr, dass der Nutzer die Tickets verändert oder dupliziert (Hülskamp und Buse 2008, S. 553).

Beispiel: Deutsche Bahn

Über die Ticket-App der Deutschen Bahn können von unterwegs Fahrkarten gebucht und Sitzplätze reserviert werden, sodass der Weg zum Schalter entfällt und Tickets direkt auf das Smartphone geladen werden können. Vorab muss sich ein Kunde registrieren und gibt hierzu seine Handynummer, das gewünschte Bezahlverfahren (Lastschrift, Kreditkarte, PrePaid) und die Nummer des Personalausweises als Kontrollmedium an. Je nach

Bezahlverfahren sind darüber hinaus Name, Adresse und Kontoverbindung bzw. Kreditkartennummer erforderlich. Bei der PrePaid-Zahlung sind keine weiteren Angaben nötig. Mit Abschluss der Registrierung verschickt die Bahn eine SMS mit der Handy Ticket-PIN. Diese wird für das Login im Handy-Ticket-Kundenportal und beim Ticketkauf benötigt.

Neben dem Erwerb von Tickets bietet die App Funktionen vor Reiseantritt wie z. B. eine integrierte Routenplanung, so dass die schnellste bzw. kostengünstigste Verbindung gefunden werden kann. Es können Informationen über die Auslastung des gebuchten Zuges und über die Wagenreihenfolge abgefragt werden. Im Fernverkehr besteht die Möglichkeit eines Check-Ins am Platz ohne weitere Ticket-Kontrolle; während der Fahrt gibt es per E-Mail oder Push-Nachricht Informationen über Verspätungen, Gleiswechsel oder Fahrplanänderungen. Möglich ist auch die Abfrage des Handy Ticket-Kontostandes und Ändern der PIN.

Beispiel Handyparken

Ein weiteres Beispiel für Mobile Ticketing ist das Handyparken, welches in vielen Städten angeboten wird. Hierbei kann über das mobile Endgerät ein Parkschein erworben werden. Es gibt verschiedene Anbieter, bei denen sich der Vorgang des Parkscheinerwerbs nur in Details unterscheidet. Zunächst ist bei allen Anbietern eine Registrierung nötig. In einigen Fällen wird daraufhin eine Vignette zugesendet, die gut sichtbar im Auto angebracht werden muss. Über den auf der Vignette enthaltenen Code kann die Gültigkeit des Parkvorgangs überprüft werden. Einige Anbieter realisieren ein Verfahren ohne Vignette. Hierbei gibt der Nutzer bei der Registrierung sein Kraftfahrzeugkennzeichen an, anhand dessen bei einer Kontrolle überprüft wird, ob ein gültiger Parkschein vorliegt oder nicht. Ein nicht unwesentlicher Vorteil des Handyparkens besteht in der Möglichkeit, die Parkzeit im Rahmen der Höchstparkdauer auch nachträglich oder aus der Entfernung zu verlängern.

Bei der Nutzung von Parkgaragen mit automatischer Kennzeichenerkennung kann mit Hilfe einer CameraPark-App der Parkvorgang automatisiert werden. Die Unterstützung dieser Funktion wird dem Nutzer bei der Einfahrt über ein Symbol signalisiert. Bei der Einfahrt wird das Kennzeichen automatisch erfasst. Der Parkvorgang wird in der App registriert. Während der normale Nutzer vor der Ausfahrt am Bezahlautomaten das Kennzeichen zur Abrechnung eingibt, kann der CameraPark-App-Nutzer direkt zum Fahrzeug gehen und ausfahren. Über die App und die hinterlegte Bezahlfunktion wird die Abrechnung der Parkzeit im Hintergrund durchgeführt. Die CameraPark-Funktion wird von üblichen Handy-Park Apps, aber auch von Apps der Garagenbetreiber angeboten.

Neben dem Lösen eines Parktickets kann mittlerweile auch das Verwarn geld für falsches Parken in manchen Städten über ein mobiles Endgerät bezahlt werden. Ein Beispiel hierfür ist das System „Bezahllotse“, welches in Kaiserslautern Falschparkern ermöglicht, ihre „Knöllchen“ unmittelbar am „Tatort“ mobil zu bezahlen.

Hierfür wird die Scheibenwischerverwarnung, die der Autofahrer erhält, zusätzlich mit einem QR-Code versehen. Wenn der Falschparker diesen mit seinem Mobilgerät einscannt, gelangt er zu einer mobilen Webseite, welche die Tatbestandsdaten inklusive einer



Abb. 8.5 Digitale Scheibenwischerverwarnung der Stadt Kaiserslautern (Bezahllotse 2021)

Begründung auflistet (Abb. 8.5). Über die PayPal-App kann der Nutzer nun den geforderten Betrag umgehend bezahlen, sofern er über ein Konto bei dem Bezahldienst verfügt. Für die Stadt ergeben sich hierdurch hohe Einsparpotenziale durch die unmittelbare Bezahlung, denn durch das Versenden von Mahnungen, Prüfen von Bankverbindungsdaten etc. entstehen Kosten, die die Höhe des Verwargeldes nicht selten übersteigen (Bezahllotse 2021).

8.2.4 Mobile Payment

Unter mobilem Bezahlen (M-Payment) wird die Initiierung, Autorisierung und Realisierung einer Zahlung verstanden, wobei zumindest der Zahlungspflichtige mobile Kommunikationstechnik oder ein mobiles Endgerät einsetzt. Der Einsatzschwerpunkt liegt im Bereich von B2C-Geschäften.

Generell läuft ein mobiler Bezahlvorgang wie folgt ab (Abb. 8.6):

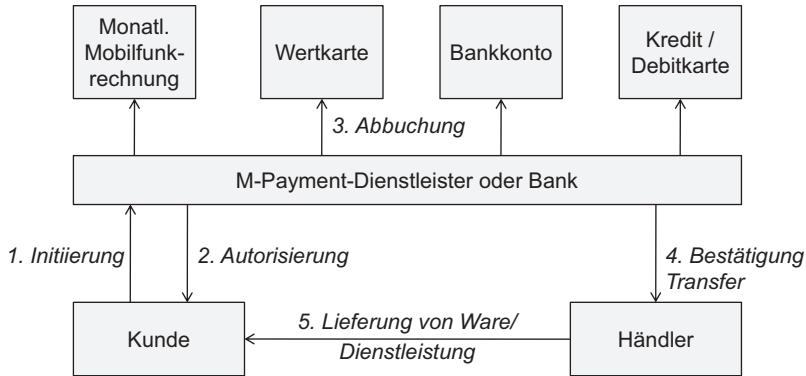


Abb. 8.6 Ablauf von M-Payment

- Der Kunde möchte ein Produkt oder eine Dienstleistung mobil bezahlen. Hierzu muss eine Verbindung zwischen Kunde, Händler und einem Vermittler (M-Payment-Dienstleister oder Bank) hergestellt werden. Das mobile Endgerät des Kunden und das Kassenterminal müssen mobil und sicher miteinander kommunizieren, d. h. Daten untereinander austauschen. Hierzu existieren derzeit verschiedene konkurrierende Zugangs- und Übertragungstechnologien.
- Das Kassenterminal übermittelt den Zahlungsbetrag über die sichere Schnittstelle an das mobile Endgerät.
- Im folgenden Schritt wird die Zahlung durch den Kunden autorisiert. Der Kunde bestätigt den Betrag und autorisiert durch Eingabe einer PIN oder durch biometrische Daten wie Fingerabdruck oder Gesichtserkennung.
- Die autorisierte Transaktion wird zurück an das Kassenterminal übermittelt, und von dort an den Zahlungsdienstleister übertragen, der dem Kassenterminal die Transaktion bestätigt.
- Der Händler kann die Ware ausliefern oder die Erbringung der Dienstleistung veranlassen.
- Durch den Payment-Dienstleister erfolgt die Buchung des Betrags. Hierbei existieren verschiedene Möglichkeiten:
 - Begleichung des Geldbetrages über die monatliche Mobilfunkrechnung des Mobilfunkanbieters;
 - Abbuchung über ein Prepaid-Verfahren, d. h. eine Karte oder ein Kundenkonto des M-Payment-Dienstleisters, welches vorher mit Geld aufgeladen wurde;
 - Abbuchung vom Bankkonto des Kunden;
 - Abbuchung über Kredit- oder Debit-Karten, wie es von bargeldlosen Bezahlvorgängen mit Kreditkarten oder Debitkarten (Girokarten) her bekannt ist.

Im einfachsten Fall ersetzt das Smartphone bei M-Payment Bargeld oder Kreditkarte. Generell lassen sich vier unterschiedliche Formen unterscheiden:

Peer-to-Peer-Payment

Hierbei erfolgt ein Geldtransfer direkt von Person zu Person bzw. von Smartphone zu Smartphone. Diese Form ist ein möglicher Ersatz für Bankgeschäfte, vor allem in Ländern, in denen kein allgemein zugängliches Bankensystem besteht.

Remote Payment

Diese Bezahlform umfasst sämtliche elektronischen Zahlungssysteme, die auch bei webbasierten Online-Shops angeboten werden, also beispielsweise Kreditkarte, Lastschrift, PayPal, wobei der Zahlvorgang hier nicht über einen PC abgewickelt wird, sondern über ein Smartphone mit Internet-Zugang.

Mobile Point of Sale

Ein Smartphone bzw. Tablet wird hierbei durch aufsteckbaren Dongle oder ein verbundenes Kartenlesegerät mit PIN-Eingabemöglichkeit zu einem mobilen Kassenterminal.

Proximity Payment

Im Mittelpunkt steht hierbei das mobile Bezahlen im stationären Handel, wobei verschiedene Möglichkeiten der Datenkommunikation zwischen dem Smartphone des Kunden und dem Point of Sale (kurz POS) existieren (Bleyh und Feser 2015, S. 383 f.):

NFC

- Für die Datenkommunikation zwischen mobilem Endgerät und POS kann Near Field Communication (Abschn. 5.4) genutzt werden (Abb. 8.6).

QR-Code

- Der QR-Code (Abschn. 5.5) dient hierbei als Daten-Schnittstelle zwischen Kassensystem und Smartphone. Die eine Seite erzeugt einen QR-Code mit den Daten zur Transaktion, während die Gegenseite diesen einscannt und verarbeitet.

BLE

- Über Bluetooth Low Energy (Abschn. 5.6) kann ein Einzelhändler an seine Kunden im Ladenlokal nicht nur gezielte Informationen verschicken, sondern es lassen sich hierüber auch mobile Zahlungen abwickeln.

Online-Legitimationsverfahren bei Kreditkarteneinkauf im Internet

Durch die EU-Richtlinie PSD2 wurden neue Regeln für das Bezahlen im Internet festgelegt. Statt der Eingabe des auf der Kreditkarte aufgedruckten Sicherheitscodes wird ein unabängiges Identifikationsmerkmal für eine Zwei-Wege-Absicherung gefordert. Dies wird in aller Regel durch eine registrierte Smartphone-App erbracht, über die die Anforderung zur Bestätigung der Kreditkartenzahlung übermittelt wird, und die es erlaubt, diese Bestätigung direkt zu geben.

ApplePay und Google Pay als Beispiele für Mobile Payment

Mit ApplePay trat der Smartphone-Hersteller Apple Inc. in den M-Payment-Markt ein. ApplePay ist mit den gängigen Kreditkarten nutzbar und ist eigentlich ein Angebot der Kreditkarten-Industrie. Das Smartphone emuliert eine Kreditkarte des jeweiligen Anbieters und fügt eine Reihe von Sicherheitsmerkmalen hinzu, die mit einer reinen Kartenlösung so nicht zu realisieren sind. Statt Kreditkarten können mittlerweile auch Giro-Karten bei ApplePay genutzt werden (Schmidutz 2020). Apple tritt als Vermittler bei der Einrichtung der ApplePay Funktion auf, spielt aber bei der Abwicklung der Zahlungen keine aktive Rolle. Der Zahlungsvorgang entspricht dem in Abb. 8.6 dargestellten Schema.

Mit einem Secure Element (SE) enthalten mobile Endgeräte von Apple Inc. eine sichere Plattform als System-on-a-Chip. Dort werden die vertraulichen Daten im Zusammenhang mit dem Dienst in verschlüsselter Form gespeichert. Ab dem Modell iPhone 5 ist das SE Teil des im Smartphone integrierten NFC Chips. Beim Einrichten des Dienstes wird ein Scan der Kreditkarte durch das Smartphone ausgeführt und über Apple verschlüsselt an die Kreditkartengesellschaft übermittelt. Die Kreditkartengesellschaft sendet eine Token-Version seiner Kreditkartendaten an das iPhone, die dort im Secure Element gespeichert wird. Der Token besitzt die Struktur einer Kreditkarten-Nummer mit Sicherheitscode und Gültigkeitsdatum. Die Daten der originalen Kreditkarte lassen sich aus dem Token aber nicht zurückrechnen. Innerhalb des Netzwerks der Kreditkartenunternehmen wird der Token wie ein normales Kreditkartendatum behandelt und an das ausgebende Unternehmen gesendet. Der Token wird dort entschlüsselt und die Identität des Nutzers geprüft; die weiteren Schritte entsprechen der Darstellung oben zum Mobile Payment.

Die Daten der originalen Karte sind auf dem Mobiltelefon gespeichert, bleiben aber beim Zahlungsvorgang für den Dienstleister und den Zahlungsempfänger verborgen. Sie können auch nicht aus dem Token zurückgerechnet werden. Der proprietäre und geheime Token-Algorithmus soll auch sogenannte Replay-Attacken sicher verhindern (Geuss 2014).

Das konkurrierende GooglePay nutzt mit dem als Host Card Emulation bezeichneten Verfahren einen vollständig anderen Weg zur Abwicklung von Kreditkartenzahlungen mittels Android-Endgeräten. Ursprünglich wollte auch Google ein Secure Element einführen, gab das Vorhaben allerdings wohl aufgrund der Schwierigkeiten mit den verschiedenen Herstellern, Software- und Hardware-Versionen wieder auf. Das GooglePay-Verfahren funktioniert mit allen Kreditkarten, ohne dass es einen Vertrag zwischen Google und dem

Kartenunternehmen geben muss. Mit Hilfe des Zahlungsdienstleisters TheBancorp Inc gibt Google bei der Einrichtung von GooglePay eine virtuelle Kreditkarte heraus, die auf dem Smartphone des Nutzers gespeichert wird. Der Kunde nutzt diese Karte für sein Mobile Payment. TheBancorp autorisiert die Zahlung und belastet dann die eigentliche Kreditkarte des Nutzers. Auch hier bleiben dem Verkäufer die Identität des Nutzers und seine Kreditkarten-ID verborgen. Im Unterschied zu Apple ist Google jedoch aktiver Teil jeder Transaktion. Google überwacht die Transaktionen mit einem eigenen Risiko-Monitoring, und gibt dem Nutzer durch die Auswertung von Transaktionsdaten ein zusätzliches Sicherheitsfeature.

Interessant ist ein Vergleich der Service-Gebühren für Zahlungsvorgänge. Bei Apple-Pay läuft die Transaktion direkt zwischen dem Nutzer, dem Bezahlterminal und der ausgebenden Kreditkartengesellschaft ab. Es fallen also keine zusätzlichen Gebühren an. Die Kreditkartengesellschaften beteiligen Apple an den Service-Gebühren und rechtfertigen dies mit der erhöhten Sicherheit und dem größeren Zahlungsvolumen durch das einfache Handling. Bei GooglePay fallen für jede Transaktion zwei Gebühren an: einmal für den Händler an TheBancorp, und danach für TheBancorp an die originale Kreditkartengesellschaft. Die Details des Gebührenmechanismus sind geheim; spekulativ ist aber davon auszugehen, dass Google einen Teil der Gebühren trägt. Dabei dürfte der Mehrwert für Google im Gewinn von hochwertigen Kundendaten für sein eigenes Werbegeschäft liegen. TheBancorp könnte von dem großen Transaktionsvolumen, und die Kreditkartengesellschaften von einem geringeren Anteil an „faulen“ Zahlungen durch die sicherheitsüberprüften Transaktionen profitieren

8.2.5 Mobile Entertainment

Das Smartphone wird von vielen Menschen zu Unterhaltungszwecken genutzt, und zwar vor allem für Spiele, zum Musikhören und Videokonsum.

Mobile Games

Mobile Endgeräte eignen sich deshalb hervorragend zum mobilen Spielen, weil unabhängig von Zeit und Aufenthaltsort spontan neue Spiele bezogen und Unterhaltungsbedürfnisse befriedigt werden können. Hinsichtlich der Bedienung und Interaktion sind die Spiele genau auf die Haptik und Eingabemöglichkeiten der mobilen Endgeräte abgestimmt. Die eingebauten Bewegungssensoren erlauben es, das ganze mobile Endgerät als frei beweglichen „Controller“ zu verwenden. Auch das Spieldesign ist überwiegend auf die Anforderungen der Mobilität abgestimmt, sodass sich Spielaufgaben in kurzen Zeittintenvalen abschließen lassen und nach Unterbrechungen eine sofortige Fortsetzung des Spiels möglich ist. Eine Sonderform bilden mobile Glücksspiele, bei denen der Spieler unter Einsatz realer Geldbeträge eine Wette (z. B. Sportereignis) mit Hilfe seines mobilen Endgeräts eingehet. Mobile Games treten in unterschiedlichen Formen auf. Sie werden

- vor Kauf des Endgeräts bereits vorab installiert oder
- müssen vor Spielbeginn vom jeweiligen App Store heruntergeladen und am mobilen Endgerät lokal gestartet oder
- über das Netzwerk als Streaming-Dienst genutzt, hierzu ist eine ständige Kommunikationsverbindung erforderlich;
- von einem einzelnen Nutzer gespielt oder
- von mehreren Nutzern gleichzeitig – gegeneinander bzw. miteinander – gespielt.

Es lassen sich verschiedene *Geschäftsmodelle* zur Finanzierung der in der Entwicklung teuren Unterhaltungssoftware unterscheiden. Bei der Variante *buy-to-play* wird ein einmaliger Preis beim Erwerb des Spiels im App-Store bezahlt, sodass es installiert werden kann und dem Anwender unbegrenzt zur Verfügung steht. Für etwaige Erweiterungspakete kann der Hersteller zusätzlich Geld verlangen. Dagegen wird beim *pay-to-play*-Prinzip die Zahlung einer regelmäßigen oder wiederkehrenden Gebühr verlangt, um das Spiel spielen zu können. Im mobilen Bereich besonders beliebt ist das Modell *free-to-play*. Hierbei wird das Spiel kostenfrei zum Download angeboten und kann auch kostenfrei gespielt werden. Finanziert werden solche kostenfreien Spiele zum Teil über Werbung, die sich durch Zahlung eines Premium-Zugangs ausblenden lässt oder über den Verkauf von Spielebeschleunigern, digitalen Gegenständen (z. B. besondere Kleidungsstücke für einen Avatar) oder speziellen Spielinhalten- bzw. Spielfunktionen. Bei Spielebeschleunigern handelt es sich um Funktionen, die u. a. Wartezeiten verkürzen, Limitierungen aufheben oder Spielerfolge schneller verfügbar machen. Die Möglichkeit, aus der App heraus zusätzliche Funktion oder Inhalte zu kaufen, muss der Anbieter bereits vor dem Download kenntlich machen (z. B. durch einen Vermerk „In-App Käufe“).

Aufgrund der Besonderheit mobiler Endgeräte, eine Ortung durchführen zu können, ergeben sich für den Spielesektor neue Potenziale, um besondere Spielmechanismen einzusetzen. Mobile Games lassen sich mit Location Based Services (Abschn. 8.6) verknüpfen. Die Positions- und die Bewegungsdaten der Spieler werden über das mobile Endgerät erfasst und in das Spielerlebnis eingebunden. Beim *Geocaching* geht es um das Auffinden von versteckten Gegenständen, deren Geopositionsdaten im Internet veröffentlicht werden. Als Hilfsmittel dient eine App, die die Navigation zum Versteck erleichtert und dem Finder das sofortige „Loggen“ eines gefundenen Geocachs (inkl. Fotoeinbindung) ermöglicht.

Mobile Musik- und Videoangebote

Mobile Endgeräte werden sehr häufig für den Musik- und Videokonsum genutzt. Download- und Streamingportale bieten interessierten Kunden eine große Bandbreite an Filmen und Musik an. Videostreaming gilt inzwischen als größter Wachstumstreiber im mobilen Internet. Die Medienangebote werden teilweise im Bündel mit Mobilfunkverträgen ohne Anrechnung der Streaming-Daten auf das Kontingent oder als Paket-Angebot unter Einchluss eines mobilen Prepaid-Vertrages vermarktet.

8.2.6 Mobile Health & Fitness

Als Mobile Health (M-Health) wird der Einsatz mobiler Technologien im Gesundheitssektor sowie in den Bereichen Sport und Fitness bezeichnet. Im Gegensatz zu E-Health werden hierbei Gesundheits- und Fitnessdienste über mobile Endgeräte angeboten. Insbesondere zählen hierzu die mobile Erfassung medizinisch relevanter Daten, die Speicherung und der Austausch bzw. die Weiterleitung dieser Daten an Ärzte, Trainer oder an Freunde und Sportkameraden. Dank verschiedener Ortungstechnologien (Abschn. 8.6) können im Freizeitsport die gelaufene oder gefahrene Strecke sowie Pulsfrequenz, Schritt-frequenz oder Geschwindigkeit erfasst und angezeigt werden. Die Fülle der erhobenen Daten nimmt stark zu und beinhaltet Vitaldaten (Blutdruck, Zuckerwerte, etc.), Sportdaten, wie gelaufene Kilometer oder Statusdaten von medizinischen Geräten (z. B. Herzschrittmacher). Neben Smartphones mit entsprechenden Gesundheits-Apps kommen Fitness-Armbänder sowie Smartwatches zum Einsatz.

M-Health kann zur medizinischen Vorsorge und zur Nachversorgung dienen. Patienten wird aufgrund der Verfügbarkeit mobiler Technologien ggfs. eine Rückkehr in den Alltag ermöglicht, ohne dass die medizinische Versorgung darunter zu leiden hat. M-Health-Ansätze versprechen also die Verbesserung gesunder Lebensstile, eine verbesserte Entscheidungsfindung durch medizinisches Fachpersonal und Patienten aufgrund einer erweiterten Datenbasis sowie die Erleichterung der Kommunikation zwischen Patienten und Fachpersonal. Auch die Durchführung präventiver Gesundheitsmaßnahmen soll ermöglicht werden. Ein weiteres Ziel ist die Absenkung der Kosten der medizinischen Versorgung.

Neben diesen positiven Wirkungen sind jedoch auch kritische Aspekte zu berücksichtigen. An erster Stelle rangiert dabei die Sorge um eine missbräuchliche Verwendung personenbezogener (Patienten-) Daten. Durch die zunehmende Vernetzung der Applikationen auf Server-Ebene verliert der Nutzer schnell die Kontrolle über die Verwendung seiner Daten. Rechtlich ist eine automatisierte Datenweitergabe z. B. an Krankenversicherungen kritisch zu hinterfragen. Daneben existieren Bedenken zur technischen Sicherheit und hochgradigen Verfügbarkeit der Systeme, die für eine kontinuierliche medizinische Versorgung notwendig sind.

8.3 Business Apps

Betriebliche Anwendungssoftware wie z. B. ERP- oder Office-Systeme sind heute zumeist über Webbrowser nutzbar und als Cloud-Anwendung von überall her erreichbar. Dank des mobilen Internet kann auf diese Anwendungen somit auch über Smartphone bzw. Tablet zugegriffen werden. An dieser Stelle werden diese Einsatzmöglichkeiten nicht weiter thematisiert, vielmehr sollen einige für die geschäftliche Nutzung relevante mobile Anwendungen vorstellt werden, die ihre Stärke erst durch die Eigenschaft der Mobilität offenbaren oder als herkömmliche Web-Anwendung gar nicht möglich sind.

8.3.1 Mobiles CRM

Von mobilen Customer Relationship Management (CRM) Systemen profitieren Nutzer im Bereich Kundenakquise und Außendienst. Sie erhalten Zugriff auf Kundendaten von unterwegs. Auf dem Weg zu einem Kundentermin lassen sich aktuelle Informationen über Produkte oder Kundenpräferenzen abrufen. Während des Kundengesprächs sind interaktive Präsentationen möglich und es kann auf Vertragsdokumente sowie auf zusätzliche Informationen zugegriffen werden. Nach Abschluss des Kundengesprächs können neue Daten zeitnah erfasst werden.

8.3.2 Mobiles SCM

Supply Chain Management (SCM) unterstützt die Auftragsabwicklung entlang der Wertschöpfungskette, also über das einzelne Unternehmen hinaus unter Einbeziehung von Kunden und Lieferanten durch untereinander abgestimmte Datenflüsse. Dies geschieht durch eine enge Abstimmung und Anbindung aller Akteure (Lieferanten, Hersteller, Logistik-Dienstleister und Händler). Alle Beteiligten müssen zeitnah mit relevanten Informationen für die rechtzeitige Planung, Herstellung und Lieferung der bestellten Waren versorgt werden. In der Praxis sind bislang aber keine vollständigen Wertschöpfungsketten, sondern lediglich Ausschnitte davon umgesetzt. Durch die Abstimmung der Prozesse kann der Wertschöpfungsprozess besser gesteuert werden und es kann schneller auf Planabweichungen und Lieferprobleme reagiert werden.

Mobile SCM-Systeme stellen ortsunabhängige Informationen entlang der Lieferkette auf mobilen Endgeräten zur Verfügung. Die Sendungsverfolgung (Abschn. 8.6) ermöglicht es, den Status einer Lieferung zu überwachen. Hierdurch kann beispielsweise ein Kunde Auskunft darüber erhalten, wo sich Waren zu einem bestimmten Zeitpunkt befinden. Es lässt sich die Planungssicherheit in der Produktion verbessern, und zwar gerade bei Just-in-Time-Anlieferungen seitens der Zulieferer, wodurch die Produktionsstätte in Echtzeit den voraussichtlichen Lieferzeitpunkt anpassen kann. Bei Abweichungen oder Verzögerungen kann so eine hohe Reaktionsgeschwindigkeit erreicht werden, insbesondere durch direkte Weiterleitung von Statusinformationen an den letztendlichen Warenempfänger.

Dies soll an folgendem Beispiel erläutert werden: Die mobile Sendungsverfolgung hat sich aus dem von Behörden und großen Unternehmen bekannten Laufzettel in Papierform entwickelt. Es müssen bestimmte Stationen angesteuert werden und am Ende sollte dokumentiert sein, dass auch alle Stationen durchlaufen wurden. Im Zuge der Digitalisierung der Unternehmensabläufe wird die Dokumentation durch elektronische Verfahren unter Einsatz von optischer Erfassung oder RFID durchgeführt (Abb. 8.7). Die globale Artikelnummer (Global Trade Number, abgekürzt GTIN), die European Article Number (EAN) oder eine betriebsindividuelle Kennung werden als optischer Barcode oder als RFID-Label auf dem Artikel angebracht. An jeder durchlaufenen Station werden sie durch einen

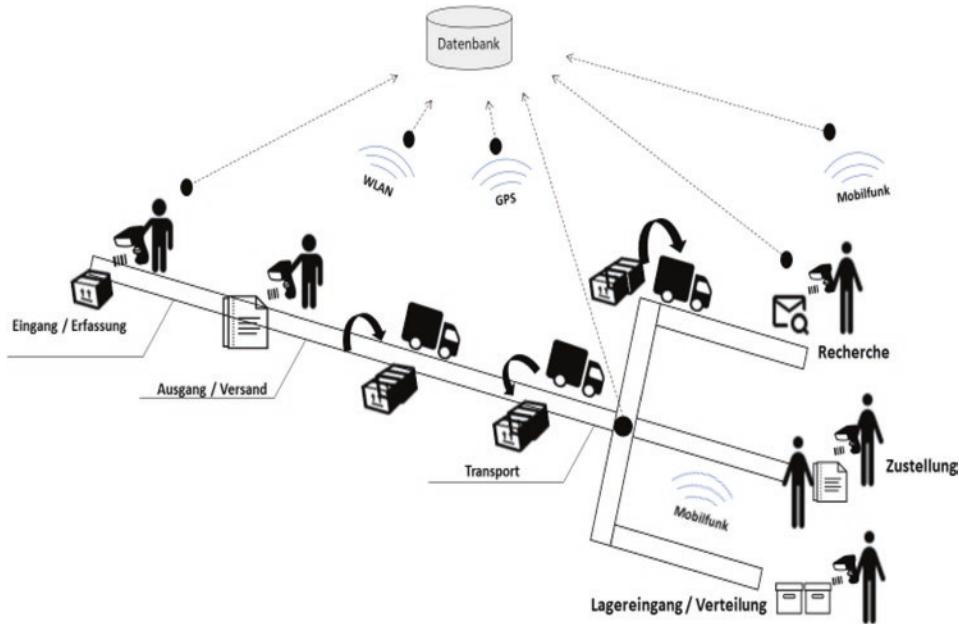


Abb. 8.7 Sendungsverfolgung

Scanner oder RFID-Lesegerät erfasst und mit dem aktuellen Aufenthaltsort in einer zentralen Datenbank gespeichert. Die Daten werden von den Teilnehmern der Supply Chain zur Sendungsabfrage oder Statusabfrage genutzt.

Unter Einsatz von Mobilfunktechnik kann die Kontrolle der Supply Chain deutlich verfeinert werden. Eine Tracking-Einheit, beispielsweise ausgestattet mit Positionierungs-Chips, Bewegungs- und Temperatursensoren meldet über ein IoT-Modem (Kap. 6) und ein Low Power Wide Area Mobilnetz (z. B. NB-IoT oder LoRaWAN, Kap. 5) fortlaufend die gespeicherte Artikel-ID, die Position und den Status an den zentralen Server. Je nach Problemlage und betriebenem Aufwand kann solch ein Gerät am transportierenden Lkw oder Eisenbahnwaggon, an der Palette oder am eigentlichen Paket angebracht sein. Durch die kontinuierliche und zeitnahe Information kann die Software genaue Vorhersagen über das Eintreffen der Ware am nächsten Kontrollpunkt oder am Ziel treffen. Dabei können zusätzlich Straßenzustandsmeldungen oder Wettervorhersagen einfließen. So können Unterbrechungen oder Verzögerungen in der Produktion effektiv reduziert werden. Zusätzlich können Risiken für die gelieferten Güter aktiv gemanaged werden. Melden zum Beispiel die Sensoren eine Störung an der Ladung, wie etwa eine Temperaturabweichung bei Kühlwaren, kann der Server einen Alarm auslösen und automatisch oder durch die Disposition geeignete Maßnahmen einleiten.

Der Vergleich von Barcode/QR-Code, RFID und Mobilfunk in Abb. 8.8 zeigt, dass deutlich größere Einsatzmöglichkeiten mit erhöhten Kosten verbunden sind. Es ist daher immer zu prüfen, ob der benötigte Leistungsumfang die Kosten rechtfertigt.

| Technologie | Identifizierung | Nachverfolgung | Ortung | Überwachung | Echtzeit-Reaktion | Optimierung Datenanalyse | Kosten |
|--------------------|-----------------|----------------|--------------|-------------|-------------------|--------------------------|--------------|
| Barcode | Ja | Beschränkt | Nein | Nein | Nein | Nein | Sehr Niedrig |
| RFID | Ja | Ja | An Stationen | Nein | Nein | Nein | Niedrig |
| Mobilfunk-Sensoren | Ja | Ja | Ja | Ja | Ja | Ja | Hoch |

Abb. 8.8 Leistungsfähigkeit und Kosten von IoT-Lösungen im SCM

Durch die internationale Standardisierung, globale Verfügbarkeit und bestehende Roaming-Abkommen eignet sich das auf LTE basierende NB-IoT (Kap. 4) besonders für solche Lösungen. Dies gilt insbesondere für internationale Lieferketten. Die weltgrößte Frachtreederei Maersk verwendet zusätzlich Satellitenverbindungen, um Kühlcontainer auf ihren Frachtschiffen zu überwachen. Dabei besitzt jedes Frachtschiff eine eigene Mobilfunk-Basisstation, die über einen Satellitenlink mit dem Service-Zentrum verbunden ist. Die Tracking-Einheiten an den Kühlcontainern verbinden sich mit dieser bordeigenen Station (Ericsson 2012).

8.3.3 Mobiles Human Resource Management

Das stärkste Interesse an mobilen HR-Apps haben diejenigen Nutzer, die orts- und zeitunabhängig arbeiten. Mobile HR-Applikationen lassen sich in vier Gruppen zusammenfassen (Abb. 8.9). Beispielsweise können Stellensuchende von unterwegs mit ihrem Smartphone direkt auf eine Stellenanzeige reagieren (Mobile Recruiting). Mitarbeiter eines Unternehmens können mobil lernen. Führungskräfte mit hoher Reisetätigkeit können unterwegs wichtige Kennzahlen und Analysen abrufen (Mobile Business Intelligence) oder Urlaubsanträge der eigenen Mitarbeiter genehmigen (Mobile Self Services).

Mobiles Lernen

Mobiles Lernen (Mobile Learning, M-Learning) kann als Weiterentwicklung von E-Learning betrachtet werden. Hierbei sind die Lerninhalte zu jeder Zeit und an jedem Ort über ein mobiles Endgerät zugänglich. Der Lernende kann selbst entscheiden, wann und wo er lernt. Aufgrund der begrenzten Darstellungsmöglichkeit von Lerninhalten infolge der kleineren Displays und wegen der eher beiläufigen Nutzung mobiler Geräte kommt es ganz besonders darauf an, Lernangebote attraktiv und die einzelnen Lerneinheiten nicht zu umfangreich darzustellen. Auch wird versucht, das spielerische und aktivierende Lernen in den Mittelpunkt zu stellen.

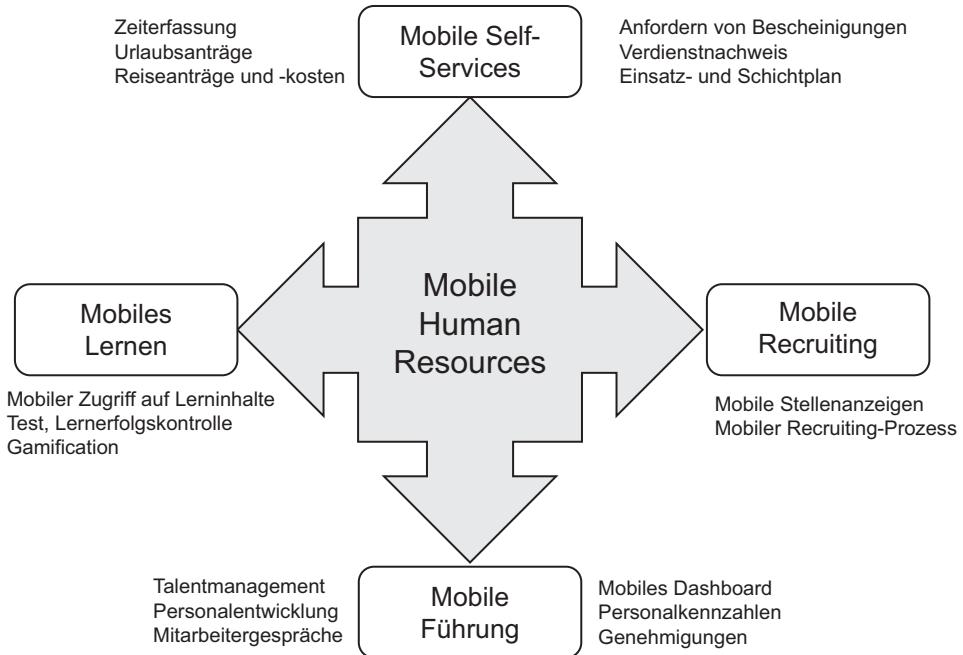


Abb. 8.9 Anwendungsschwerpunkte von mobile HRM (Mülder 2016, S. 53)

Ambient Learning bedeutet, situativ und spontan zu lernen. Der Lernende bezieht seine Umgebung in den Lernprozess mit ein. Ein Beispiel hierfür sind mobile Apps, die in der Lage sind, mittels eines Fotos ein Gebäude zu erkennen und dem Nutzer genaue Informationen über das Bauwerk zu liefern. Andere Möglichkeiten zur Ortung ergeben sich über die in allen Smartphones mittlerweile vorhandene GPS-Ortung oder über das Fotografieren eines QR-Codes am Objekt.

Mobile Recruiting

Mobile Recruiting unterstützt die Kommunikation des Unternehmens mit potenziellen Bewerbern unter Verwendung von mobilen Endgeräten. Die Ortung mobiler Endgeräte kann auch im Zusammenhang mit Rekrutierung genutzt werden, beispielsweise wenn dem Nutzer in einer Stadt angezeigt wird, welche Unternehmen aktuell Jobs anbieten.

Mobile Recruiting ermöglicht Bewerbern den mobilen Zugriff auf Stellenanzeigen und erleichtert auch den Bewerbungsprozess. Beispielsweise kann während des Bewerbergesprächs der Recruiter auf Bewerberakten und Ergebnisse eines Assessment Centers zugreifen. So können Bewerbungsgespräche auch an eher untypischen Orten wie Hotels oder Restaurants stattfinden, da Bewerberdaten mobil verfügbar sind.

Neben den eher traditionellen Job- und Karriereinformationen können auch vorhandene Social-Media-Präsenzen über den mobilen Kanal erreicht werden. Außerdem lässt

sich hierdurch eine Schwäche von mobilem Recruiting beseitigen: die eigentliche Durchführung des Bewerbungsvorgangs. Webbasierte E-Recruiting-Systeme verlangen vom Bewerber in der Regel eine umfangreiche Eingabe von persönlichen Daten, Qualifikationen und Zeugnissen, die auch als Datei hochgeladen werden können. Ein Umstand, der sich auf mobilen Endgeräten wegen einer fehlenden physischen Tastatur nicht ohne weiteres realisieren lässt. Aushilfe schaffen hier Karriere- und Lebenslaufprofile, wie sie von Nutzern in Business Netzwerken (z. B. Xing) angelegt werden. Per Link lässt dieses Profil an eine vom Smartphone initiierte Bewerbung „anheften“.

Mobile Self Services

Employee Self Services (ESS) ermöglichen allen Mitarbeitern einen Zugriff auf ihre persönlichen, vom Arbeitgeber gespeicherten Daten. Hierdurch können die meisten Routine-Aufgaben, die früher ein Formular erforderten oder von der Personalabteilung erledigt wurden, jetzt vom Arbeitnehmer selbst ausgeführt werden, beispielsweise Abruf von Verdienstnachweisen oder die Beantragung von Urlaub. Führungskräfte erhalten einen mobilen Zugriff auf personenbezogene Informationen der eigenen Mitarbeiter und können beispielsweise Genehmigungen, etwa von Urlaubsanträgen über das mobile Endgerät erteilen.

Mobile Business Intelligence

Führungskräfte mit Personalverantwortung erhalten hierbei mobil den Zugriff auf Kennzahlen und Reports, beispielsweise Profile der eigenen Mitarbeiter-Gehaltsentwicklung. Im Rahmen von Zielvereinbarungsgesprächen können über die App die Gespräche organisiert und wichtige Ergebnisse festhalten werden.

8.4 Apps für Maschinen

Internet of Things oder Industrie 4.0 basieren unter anderem auf dem Einsatz von Maschinen, die über geeignete Technologien Daten austauschen müssen.

8.4.1 Maschine zu Maschine Kommunikation

Bei Maschine-zu-Maschine-Kommunikation (M2M) tauschen technische Objekte wie beispielsweise Maschinen oder Fahrzeuge Daten direkt untereinander oder über eine Leitstelle aus. Zu den relevanten Daten zählen *Zustände* der Objekte, wie z. B. Temperatur, die über Sensoren ermittelt werden, sowie *Positionen*, die über Ortung (Abschn. 8.6) bestimmbar sind. Die Übermittlung kann über ein Festnetz oder ortsunabhängig über mobile Kommunikationsverbindungen erfolgen. Es werden bei M2M drei unterschiedliche Anwendungsmöglichkeiten unterschieden:

- a) Die kommunizierenden Objekte sind selbst mobil. Dabei kann es sich um Personen handeln, die Sensoren am Körper als Kleidung („Wearables“) oder Accessoires tragen. Das Spektrum reicht von Fahrzeugen über Haustiere und Vieh bis zu versendeten oder transportierten Gütern.
- b) Die Objekte sind nicht dauerhaft mobil, müssen aber oft den Standort verändern, so dass eine Anbindung über Kabel mit ständigen Baumaßnahmen verbunden wäre. Dies ist eine interessante Option für flexible Fabrikationsstraßen, die schnell an sich verändernde Produktionsanforderungen angepasst werden müssen.
- c) Die Objekte sind nicht mobil, jedoch durch Kabelverbindungen nicht oder nur zu sehr hohen Kosten zu erreichen. Beispiel hierfür ist das *Smart Metering*. Dabei handelt es sich um das Ablesen von Stromzählern und die Kontrolle des Verbrauchs (z. B. private Ladestationen für e-Mobilität) über das Netz. Stromzähler befinden sich häufig in Kellerräumen, die weder durch Kabelverbindungen noch durch WLAN-Lösungen einfach und kostengünstig angeschlossen werden können. Mit LTE-M und NB-IoT hat das 3GPP hier Lösungen erarbeitet, mit denen die schlechte Netzabdeckung in diesen Räumen überwunden werden kann. Auch Low Power Wide Area Lösungen können hier zum Einsatz kommen. Voraussetzung ist dabei ein Verkehrsmodell, bei dem nur eine geringe Daten-Nutzlast ausgetauscht wird. Das Verkehrsmodell stellt zusammen mit der Netztechnologie auch eine lange Lebensdauer der Mobilfunkkomponenten sicher. Von der Anwenderseite wird ein 10-Jahres Betrieb mit einer Batterieladung gefordert (LTE-M, Kap. 4).

Die Funktionsweise einer M2M-Applikation wird in Abb. 8.10 verdeutlicht. Hierbei ist die Kaffeemaschine mit Sensoren ausgestattet und meldet ihren Wartungsbedarf über Funk an die Plattform des Herstellers. Von hier aus kann automatische eine E-Mail oder SMS an einen freien oder in der Nähe bereits tätigen Wartungstechniker versandt werden, dieser führt die Reparatur rechtzeitig aus. In ähnlicher Weise melden die Kaffeemaschinen ihren Verbrauch oder ihre Nutzungsdauer an die Plattform und der Hersteller erzeugt regelmäßig eine Abrechnung für den Kunden. Früher musste sich der Kunde selbst um die Anschaffung und Wartung der Kaffeemaschine kümmern, jetzt wird die Maschine vorausschauend gewartet und die Kosten hängen ausschließlich vom Verbrauch ab. Der Hersteller von Kaffeemaschinen hat sein Geschäftsmodell verändert: während er sich ursprünglich auf den Verkauf von Kaffeemaschinen konzentrierte, bietet er seinen Kunden nun „Coffee as a Service“ (Noggler 2016).

Als Beispiel für eine Anwendung der Gruppe b) lassen sich Geldautomaten, die mit Funktechnik ausgestattet sind, kurzfristig und unabhängig von Kabelanschlüssen aufstellen, z. B. auf Messen oder bei Veranstaltungen. Manipulationen und Einbrüche können unmittelbare Alarmierungen beim Sicherheitspersonal auslösen. Snack- und Getränkeautomaten, die mobil mit dem Warenwirtschaftssystem des Serviceunternehmens verbunden sind, können Auskunft über ihren Füllstand geben. Hierdurch erfolgen Servicefahrten gezielter, weil ein Automat nur dann nachgefüllt wird, wenn er auch tatsächlich leer ist. Bei Bedarf meldet der betreffende Automat sich selbstständig. Die mobile Anbindung ermög-

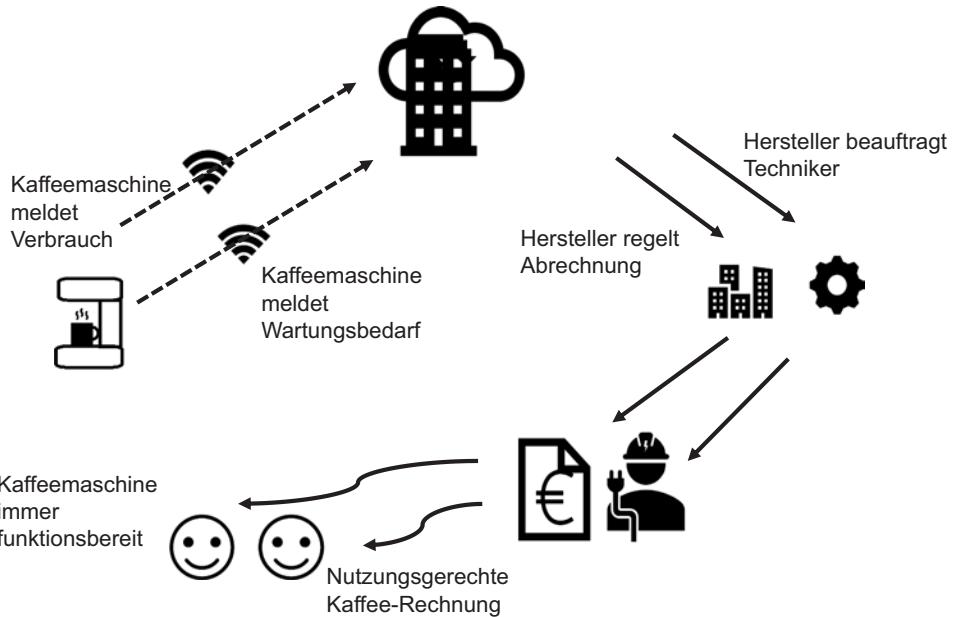


Abb. 8.10 M2M-Lösung

licht auch einen größeren Schutz vor Vandalismus und Einbrüchen. Entsprechende Sensoren registrieren eine unsachgemäße Handhabung oder einen Einbruchversuch und lösen einen Alarm aus.

8.4.2 Gebäudemanagement und Smart Metering

M2M-Apps werden beim Gebäudemanagement vielseitig genutzt. Durch Sensoren lassen sich z. B. die Temperatur und Luftfeuchtigkeit von Mietwohnungen oder Büroräumen zentral überwachen und bei Bedarf regeln. Die verschiedenen Anlagen wie z. B. Heizung, Klimaanlage, Licht, Fenstersteuerung lassen sich über Personal Area oder Local Area Networks wie Bluetooth, Zigbee oder WLAN an eine Steuerungseinheit koppeln und aus der Ferne überwachen (Abb. 8.11). Befindet sich der Hauseigentümer auf einer Urlaubsreise, ist eine Fernüberwachung und Steuerung per Smartphone möglich. Per SMS kann eine Benachrichtigung erfolgen, ob beispielsweise ein Fenster geöffnet wurde oder die Heizungsanlage gestört ist. Verschiedene Systeme werden hierzu unter Bezeichnungen „Smart Home“ angeboten. In Hochhäusern können Aufzüge mittels mobiler M2M-Technologie überwacht werden. Eine Störung kann sofort an die zuständige Service-Zentrale und ggfs. an den Hausmeister weitergeleitet werden. Durch die Möglichkeit der Ferndiagnose können drohende Ausfälle frühzeitig erkannt und die Komponenten repariert oder ausgetauscht werden. Sensoren an Fenstern und Türen des Hauses melden darüber hinaus einen

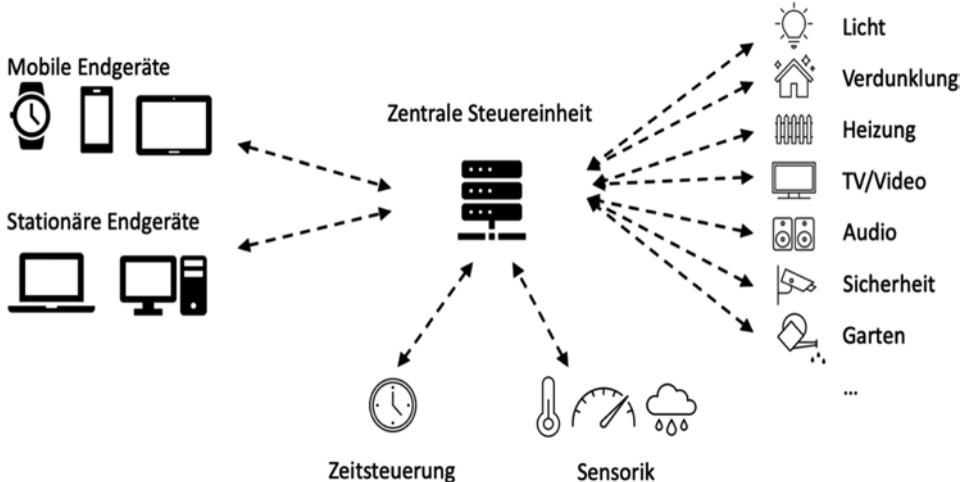


Abb. 8.11 Smart Home

Einbruch, wobei automatisch die Polizei verständigt werden kann. Ebenso ist die Verbindung mit einer Videoüberwachung möglich. Der abwesende Hausbesitzer kann hierdurch in Echtzeit ausgewählte Bereiche seines Hauses aus der Ferne kontrollieren, abends eine Sicherheitsbeleuchtung einschalten oder Rollläden an den Fenstern herunterlassen.

Mit M2M-Funktion ausgestattete Strom- und Gaszähler erlauben die Echtzeiterfassung von Stromverbrauch und die Beeinflussung von stromverbrauchenden Geräten zum Ausgleich von Verbrauchsspitzen – ein kritisches Thema der Energiewende. Da diese Geräte in der Regel in Bereichen sehr schlechter Funkabdeckung installiert sind, kommen hier die stromsparenden und abdeckungserweiternden Techniken wie LTE-M und NB-IOT (Abschn. 4.5.4) zum Einsatz. Mit öffentlichem Mobilfunk sind in Deutschland nur etwa 75 % der Standorte erreichbar, mit Einsatz von LTE-M im dafür vorgesehenen 450 MHz-Frequenzband und den in Abschn. 4.5.4 beschriebenen Anpassungen kann diese Quote stark verbessert werden. Die Endgeräte für diese Anwendung sind nicht wirklich mobil; sie sind fest z. B. an einem Stromzähler angebracht. Ihr Charakteristikum ist die drahtlose Anbindung. Hierdurch wird der Installationsprozess vereinfacht. Auch die Datenraten sind gering. Es wird lediglich mehrmals täglich eine kurze, nur wenige Bytes lange Meldung abgesetzt. Dafür müssen die Geräte eine extrem lange Laufzeit, typischerweise 10 Jahre mit handelsüblichen AA-Batterien, haben. Sie müssen Fernwartung und Software-Upgrades zulassen, um die Wartungskosten gering zu halten (Arzberger et al. 2017).

8.4.3 Umwelt- und Katastrophenschutz

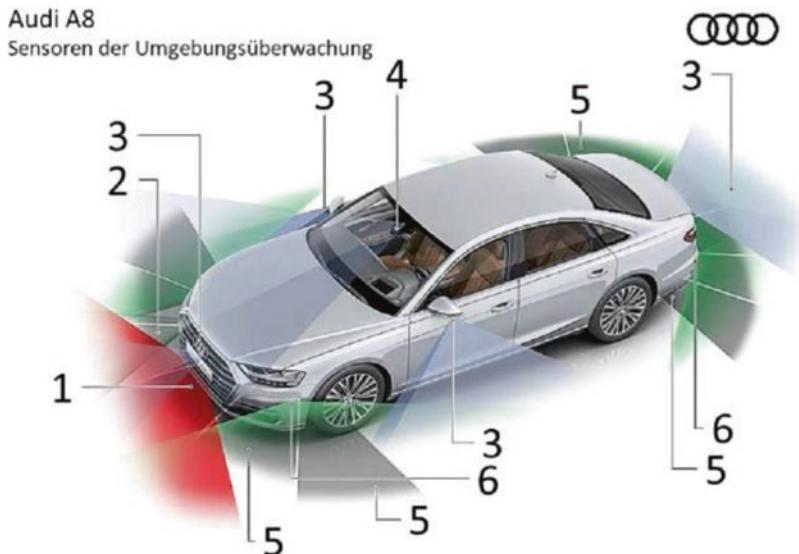
Der Umweltsektor bietet zahlreiche Einsatzmöglichkeiten für die M2M-Technologie. Eine dieser Einsatzmöglichkeiten ist die Übermittlung von Messdaten. Entsprechende Messstationen (Wetterstationen, See- oder Flussmessstationen etc.) übermitteln bei Bedarf oder bei Erreichen kritischer Werte die gesammelten Daten an eine Zentralstelle, wo die Daten gespeichert oder in einem Anwendungssystem verarbeitet werden (Alarmierung, Unwetterwarnung etc.). M2M-Module können auch bei der Wasseranalyse in Flüssen oder Seen genutzt werden, um z. B. eine Kontaminierung zu melden. In Schwimmbädern ist analog dazu eine permanente Prüfung der Wasserqualität möglich; bei entsprechend schlechten Werten kann ein Hinweis (z. B. per SMS) an einen Servicetechniker verschickt werden. Im Bereich der Entsorgungswirtschaft können Abfallcontainer, ausgestattet mit entsprechenden Sensoren und M2M-Modulen, den aktuellen Füllstand an die Zentrale des Entsorgungsunternehmens melden. Damit könnten Fahrten zu leeren Containern verhindert werden. Grundsätzlich könnte anstatt periodisch geplanter Entsorgungsfahrten ein bedarfsoorientierter Service (d. h. Leerung der Container nur bei Bedarf) angeboten werden.

Sensoren, die Bewegungen von Erdreich oder Schneemassen detektieren, können – mit energiesparenden Funkmodems ausgestattet – zur Warnung von Naturkatastrophen oder bei Lawinengefahr dienen. Aufgrund der Erfahrungen mit Erdrutschen als Folge von starken Erdbeben haben das China Geological Survey Institute gemeinsam mit dem Mobilfunkbetreiber China Mobile und der Mobilfunkhersteller Ericsson ein Erdrutsch-Warn und Detektionssystem konzipiert. (Ericsson 2017a). Bei diesen Anwendungen kommen aufgrund der benötigten Reichweiten Technologien aus dem Low Power Wide Area Bereich wie NB-IoT oder LoRaWAN zum Einsatz.

8.4.4 Autonomes Fahren

Autonomes Fahren bedeutet, dass ein Fahrzeug die Fahreraufgaben (Lenken, Bremsen, Beschleunigen) im vollen Umfang übernimmt. Die Automobilindustrie beschäftigt sich weltweit mit dieser Thematik. Die Society of Automotive Engineers (SAE) hat mit Level 0 bis Level 5 sechs Stufen autonomen Fahrens definiert (ISO 2021). Level 2 wird als Teilautomatisierung beschrieben und ist heute in Neufahrzeugen gebräuchlich. Die Funktionen umfassen Spurhalte-Assistenten, Geschwindigkeits- und Abstandsassistenten, sowie automatisches Einparken. Erst ab Level 4 wird von autonomem Fahren gesprochen. Die Entwicklung schreitet von Level zu Level fort; ein neues Level muss jeweils vom Gesetzgeber freigegeben werden. Die derzeitige Freigabe in Deutschland umfasst die Level 1 bis 3. Autonomes Fahren beschränkt sich hierbei nicht nur auf PKW, sondern umfasst ebenfalls gewerbliche LKW, Busse, Schienenfahrzeuge, Flugzeuge und landwirtschaftliche Nutzfahrzeuge.

Um Daten aus der Umgebung aufnehmen zu können, werden in autonomen Fahrzeugen unterschiedliche Sensoren eingebaut. Die Abb. 8.12 zeigt am Beispiel eines Audi A8, welche Sensoren an welchen Stellen vorgesehen sind.



| | Sensorart | Distanz (m) | Richtung | Einbauplatz |
|---|---------------------|-------------|-----------------|------------------------|
| 1 | Laserscanner | 100 | Vorn | Unter Kennzeichen |
| 2 | Long Range Radar | 200 | Vorn | Stoßstange |
| 3 | 360 Grad Kameras | 8 | Rundum | Seitenspiegel und Heck |
| 4 | Frontkamera | 100 | Vorn | Windschutzscheibe |
| 5 | Ultraschallsensoren | 8 | Vorn und hinten | Spoiler, Kotflügel |
| 6 | Mid Range Radar | 70 | Schräg außen | Kotflügel |
| 7 | Innenraumkamera | Innen | Innen | Konsole |

Abb. 8.12 Sensoren im PKW (Audi 2017)

Der Laserscanner erkennt sowohl dynamische als auch statische Objekte. Das Long-Range-Radar erkennt Hindernisse weit im Voraus. 360-Grad-Umgebungskameras erkennen den Nahbereich rund um das Auto. Die an der Windschutzscheibe angebrachte Frontkamera erkennt z. B. Fahrzeuge, die sich vor dem eigenen Fahrzeug bewegen. Vorn und hinten am Kotflügel angebrachte Ultraschallsensoren überwachen den Nahbereich des eigenen PKW schräg vorn oder schräg hinten und erkennen Radfahrer und Fußgänger. Der kreuzende oder einscherende Verkehr wird durch Mid-Range-Radar erkannt. Eine Kamera im Fahrzeuginnenraum beobachtet den Fahrer und erkennt, ob dieser das Fahrzeug wieder selbst steuern kann oder ggf. eingeschlafen ist (Viehmann 2017).

Für autonomes Fahren sind eine Reihe von Kommunikationsbeziehungen nötig und möglich, die in Abb. 8.13 illustriert werden:

V2V Fahrzeug zu Fahrzeug (Vehicle to Vehicle). Hier können Informationen über Verkehrshindernisse oder Gefahrenstellen vom vorausfahrenden an die folgenden Fahrzeuge übermittelt werden. Auch plötzliche Ausweichmanöver oder Bremsvorgänge können ver-

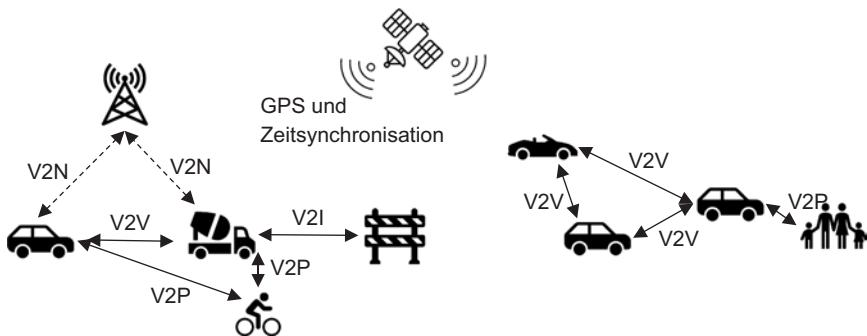


Abb. 8.13 Kommunikationsbeziehungen beim vernetzten und autonomen Fahren

zögerungsfrei als Warnung gegeben werden. Bei V2V erkennt z. B. das erste Auto nach einer unübersichtlichen Kurve ein Hindernis und warnt die nachfolgenden Fahrzeuge, damit diese rechtzeitig ein Bremsmanöver einleiten können.

V2I Fahrzeug zu Infrastruktur (Vehicle to Infrastructure). Verkehrszeichen, Lichtzeichenanlagen und geplante Hindernisse wie etwa Baustellen können aktiv über Präsenz und ihren Status informieren. Ein Beispiel für V2I sind Ampeln in einer Großstadt, die mitten in der Nacht für eine „grüne Welle“ einzelner vorbeifahrender PKW sorgen.

V2R Fahrzeug zu Straße (Vehicle to Road). Kommunikation mit intelligenten Straßenmarkierungen und Reaktion auf sich verändernde Straßeneigenschaften

V2P Fahrzeug zu Verkehrsteilnehmer (Vehicle to Person). Fußgänger und Radfahrer können mit Wearables auf sich aufmerksam machen und die automatisierte Erkennung durch die Fahrzeugsensoren ergänzen oder absichern.

V2N Fahrzeug zu Netzwerk (Vehicle to Network). Über das Mobilfunknetz empfängt das Fahrzeug Informationen zur Verkehrslage und zum Straßenzustand, Navigationshinweise, und kann auch eigenen Nachrichten absetzen (eCall, technische Defektmeldungen).

Die Entwicklung der entsprechenden Kommunikationsstandards erfolgt derzeit in zwei verschiedenen Linien, die teilweise in Konkurrenz stehen. Unter der Standard-Bezeichnung 802.11p entwickelt die IEEE WLAN-Arbeitsgruppe einen aus 802.11ac abgeleiteten Standard für automobile Vernetzung, insbesondere für die Kommunikationsbeziehungen V2V, V2P und V2I. Das 3GPP arbeitet an einem allgemeinen Standard V2X, der auch die Beziehung zum Mobilfunknetz berücksichtigt. Für die direkte Kommunikation zwischen Fahrzeugen, Personen und Infrastruktur ist auf Vorschlag der ITU-R ein einheitlicher internationaler

Frequenzbereich bei 5,9 GHz für Verkehrstelematik eingerichtet worden (Abb. 5.2). Während die 3GPP-Version zusätzlich die Kommunikation über das Mobilfunknetz nutzen kann, bleibt die Kommunikation bei 802.11p auf direkte Kommunikationsbeziehungen über wenige Hundert Meter beschränkt. Welcher Standard sich am Ende durchsetzen wird hängt wesentlich von den Ambitionen der Politik und der Hersteller zum vernetzten Fahren ab. Zusätzlich werden Satellitensignale (GPS) zur Ortsbestimmung und Zeitsynchronisation genutzt.

In einem „Connected Mobility“ Feldversuch testet ein Konsortium von Netzbetreibern, Infrastruktur-Herstellern, Fahrzeugherstellern und Forschungsinstituten unter Beteiligung der Deutschen Bahn und des Bundesverkehrsministeriums auf der Autobahn A9 zwischen Nürnberg und München sowie der parallel verlaufenden ICE-Strecke die Möglichkeiten der 5G-Technologie für Applikationen in fahrenden Automobilen und Zügen. Das Interesse der beteiligten Parteien gilt insbesondere den Anwendungen mobiler Applikationen in Fahrzeugen für V2V- und V2X-Kommunikation für neue Methoden der Verkehrsinformation in Echtzeit sowie herstellerübergreifende Verkehrskontrolle für autonome Fahrzeuge. (Ericsson 2017b)

8.5 Mobile Geschäftsprozesse

Durch Nutzung von IT konnten die Geschäftsprozesse in Unternehmen vereinfacht, teilweise auch automatisiert werden. Die Nutzung mobiler Technologien und mobiler Anwendungssysteme bietet die Chance, vorhandene Prozesse erneut zu überprüfen und zu verbessern.

Ein *Geschäftsprozess* besteht aus mehreren, logisch und zeitlich zusammenhängenden Aktivitäten, die in einer festgelegten Reihenfolge ablaufen, um ein bestimmtes Ziel zu erreichen. Jeder Geschäftsprozess hat einen eindeutigen Beginn und ein eindeutiges Ende. In der Regel beginnt ein Geschäftsprozess durch Eintritt eines Ereignisses, beispielsweise eine Kundenanfrage und endet mit dem Erreichen eines bestimmten Ergebnisses, beispielsweise Versand der gekauften Produkte an den Kunden. Die Ergebnisse stellen für den Kunden einen Nutzen dar. Geschäftsprozesse sind nicht an organisatorische Strukturen, z. B. Abteilungsgrenzen, gebunden (Mülder 2010, S. 238 f.).

Das Neuartige bei mobilen Geschäftsprozessen besteht zunächst einmal in der Einbindung und Nutzung mobiler Endgeräte und mobiler Apps im Unternehmen. Aktivitäten, die früher unterbrochen werden mussten oder bei denen es zu Medienbrüchen kam, weil Zwischenergebnisse auf Formularen festgehalten wurden, können heute direkt und unverzüglich erledigt werden. Hiervon profitieren zunächst einmal all jene Mitarbeiter, die überwiegend mobile Tätigkeiten verrichten, also vor allem:

- Fachkräfte, die mobil auf dem Unternehmensgelände unterwegs sind, wie beispielsweise Lagerarbeiter, die an verschiedenen Stellen Waren annehmen, prüfen und ausgeben oder Sicherheitskräfte, die regelmäßig die Unternehmensgebäude sowie ein- bzw. ausfahrende Fahrzeuge überwachen
- Mitarbeiter, die außerhalb des Unternehmensgebäudes ihre Arbeit verrichten, wie z. B. Fahrer, Kundenberater, Handwerker, Verkäufer im Außendienst

- Fachkräfte, die ihre tägliche Arbeit von unterwegs aus durchführen. Hierzu gehören Speditionsfahrer, Einsatzkräfte der Polizei und von Rettungsdiensten
- Manager, die sich häufig extern in Niederlassungen oder bei Kunden aufhalten.

8.5.1 Kundenzentrierte Geschäftsprozesse

Im Bereich Customer Relationship Management steht der Kunde im Fokus. Die damit verbundenen Geschäftsprozesse werden allerdings aus Unternehmenssicht und nicht primär aus Kundensicht optimiert: alle kundenbezogenen Daten und alle Interaktionen zwischen Kunde und Unternehmen werden gespeichert, der Kunde soll möglichst nicht abwandern. Durch das Internet ist allerdings die Informationsasymmetrie zwischen Kunden und Unternehmen in vielen Branchen längst nicht mehr so groß wie früher, die Bereitschaft, den Stromanbieter, den Mobilfunkbetreiber oder die Bank zu wechseln ist stärker vorhanden, teilweise aus wettbewerbspolitischen Gründen auch gewollt: Kunden sind nur noch einen Klick vom Wettbewerber entfernt.

Durch mobile Geschäftsprozesse besteht die Chance, die Leistungen des Unternehmens an den Kundenprozessen auszurichten und hierdurch einen Mehrwert für die Kunden zu schaffen und letztlich eine langfristige Kundenbindung zu erreichen. Unter Kundenprozess wird hierbei der komplette Prozess, den ein Kunde durchläuft, um sein spezifisches Bedürfnis zu erfüllen oder sein Problem zu lösen, bezeichnet (Moermann und Dohmen 2010, S. 31). Ausgangspunkt ist das Kundenbedürfnis. Es ist eher unwahrscheinlich, dass dieses Bedürfnis, und somit dieser Prozess, von einem einzelnen Unternehmen ausgeführt werden kann, vielmehr besteht die Herausforderung darin, Dienstleistungen und Apps von verschiedenen Anbietern zu integrieren. Kundenzentrierte Geschäftsprozesse sind vor allem im Bereich B2C von Bedeutung, beispielsweise:

- Bankkunden, die sich für die Themenkomplexe „Erwerb von Wohnungseigentum“, „Kreditaufnahme“, „Geldanlage“ oder „Vererben“ interessieren;
- Ältere Menschen mit ihren Bedürfnissen nach „Sicherheit“, „Gesundheit“ und „Notfall“;
- Sportler, die sich für die Themen „Training“, „Gesundheitsüberwachung“ und „Sportveranstaltungen“ begeistern.
- Touristen, die sich in einer fremden Stadt orientieren möchten, die sich für Sehenswürdigkeiten interessieren, die Restaurantempfehlungen suchen und Kulturveranstaltungen buchen möchten.

Beispielhaft soll der Kundenprozess „Erwerb von Wohnungseigentum“ betrachtet werden. Dieser hat auf den ersten Blick nur teilweise einen Bezug zu Bankprodukten. Aus Abb. 8.14 wird deutlich, dass das Bedürfnis des Kunden im Mittelpunkt steht. Angelehnt an den Customer Buying Cycle mit den Phasen Informationsbeschaffung, Alternativen-Bewertung, Kauf und After Sales werden mehrere Teilprozesse durchlaufen, wobei an

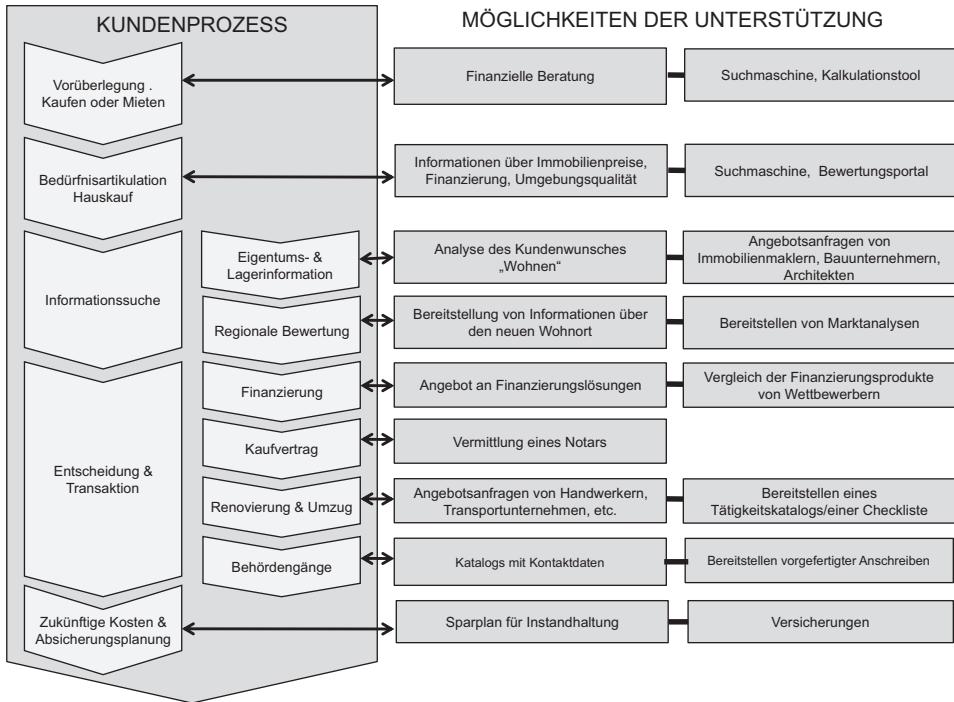


Abb. 8.14 Mobiler Kundenprozess: Erwerb von Wohnungseigentum (Moermann und Dohmen 2010, S. 31)

verschiedenen Stellen Bankprodukte eingebettet sind. Zusätzlich sind jedoch auch bankfremde Dienstleistungen, etwa von Immobilienmaklern, Handwerkern und Meldebehörden in diesen Kundenprozess eingebettet. Es gibt keinen zentralen Anbieter zur Unterstützung des gesamten Prozesses. Das mobile Endgerät dient als zentrales Verbindungselement zwischen Kunde, Bank und den übrigen Lieferanten. Hierdurch wird eine ganzheitliche Prozessunterstützung ermöglicht; dabei müssen sich die einzelnen Beteiligten nicht auf fremden Geschäftsfeldern bewegen, sondern können sich über ihre jeweiligen Apps in den Kundenprozess einbringen. Aus Kundensicht ist zumindest der Datenaustausch zwischen den einzelnen Dienstleistern erforderlich, idealerweise erfolgt die Bündelung der verschiedenen Dienste über ein mobiles Portal (Moermann und Dohmen 2010, S. 31 ff.).

8.5.2 Mitarbeiterzentrierte Geschäftsprozesse

Hierbei steht nicht der Kunde, sondern der Mitarbeiter mit seinem mobilen Endgerät im Mittelpunkt der Prozessgestaltung. Verdeutlicht wird dies am Beispiel des Prozesses *Geschäftsreise*. In vielen Unternehmen existieren zwar Softwarelösungen, die die Beantragung und Reisekostenabrechnung unterstützen, allerdings ist der administrative Aufwand

für den Reisenden und für das Unternehmen nach wie vor relativ hoch. Im Regelfall müssen unterschiedliche Buchungen (Hotel, Flug, Mietwagen) im Voraus erfolgen, mehrere Tickets und Quittungen (meistens in Papierform) sind aufzubewahren, Beträge für Reisemittel und Hotel müssen vorgestreckt werden.

In Abb. 8.15 wird dargestellt, dass ein mobiler Geschäftsreiseprozess nicht von einem einzelnen Dienstleistungsunternehmen unterstützt werden kann. Auch reicht es nicht aus, verschiedene, isolierte Apps zu installieren, weil hierdurch die Fokussierung auf den Benutzer und seine spezifischen Bedürfnisse („seine“ Geschäftsreise) verloren geht. Realisierbar ist der Prozess jedoch mit verschiedenen Apps, die allerdings teilweise untereinander Daten austauschen müssen.

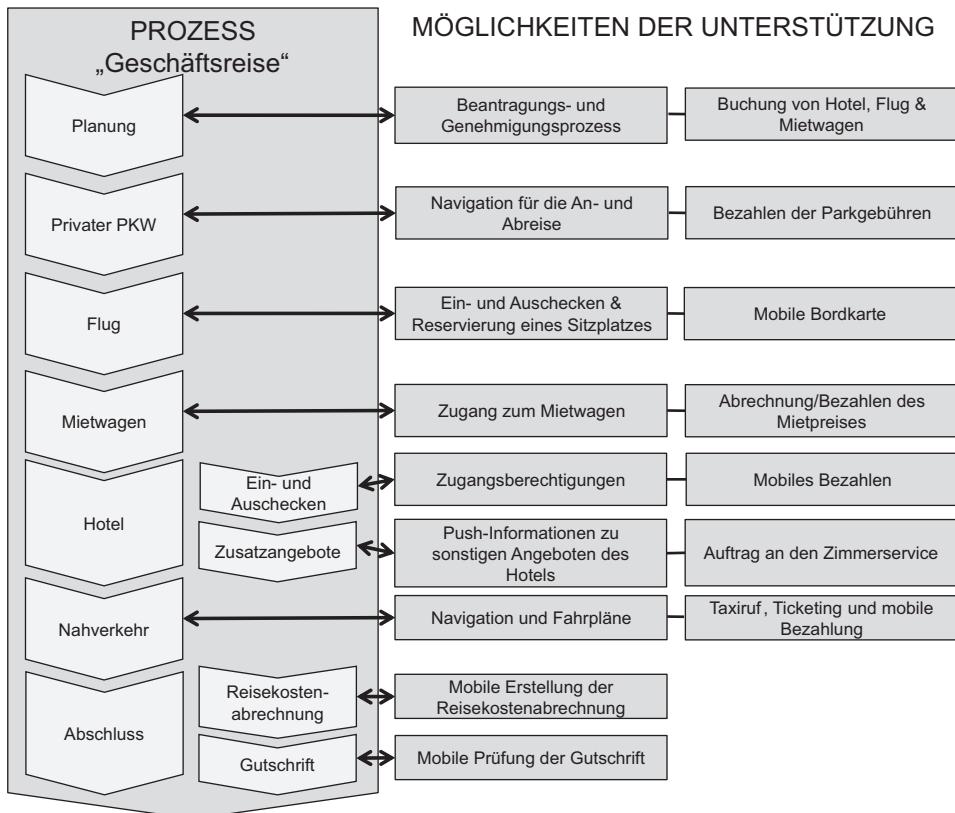


Abb. 8.15 Mobiler Prozess Geschäftsreise

Das mobile Endgerät bildet das zentrale (und möglicherweise sogar einzige) technische Hilfsmittel für den kompletten Geschäftsreiseprozess. Im Einzelnen werden folgende Funktionen benötigt:

- App zur Planung und Buchung der Reise
Der Nutzer sollte während des gesamten Prozesses unterstützt werden. Für reservierte Verkehrsmittel sind mobile Tickets vorgesehen, ferner müssen sämtliche Bestätigungen und Reservierungen abrufbar und vorzeigbar sein.
- Bezahlung mittels M-Payment
Hierdurch kann der Reisende seine laufenden Reiseausgaben, auch im Ausland, bezahlen.
- Einrichtung verschiedener Konten
Durch das Einrichten verschiedener Konten erfolgt schon beim Bezahlen eine Trennung zwischen geschäftlichen Ausgaben, die nachher über die Reisekostenabrechnung erstattet werden, und privaten Ausgaben.
- Aktueller Informationsstatus
Sämtliche getätigten Zahlungen werden aufgelistet und können vom Nutzer jederzeit kontrolliert werden.
- Mobile Navigation
Zur Orientierung im Ausland relevant, insbesondere bei fremden Schriftzeichen.
- Fotografieren von Quittungen
Für Reisekostenabrechnungen werden sämtliche Quittungen benötigt. Anstatt Papierbelege zu sammeln besteht die Möglichkeit, diese mit dem Smartphone zu fotografieren.
- Erstellung der Reisekostenabrechnung
Da die meisten Zahlungen mit dem Smartphone vorgenommen wurden, kann über die entsprechende App später auch die Reisekostenabrechnung erstellen werden, die elektronisch zur Personalabteilung übermittelt wird.
- Identifizierung und Zutritt
Um für Schließfächer, Mietwagen oder Hotelzimmer nicht immer verschiedene Schlüssel zu nutzen kann sich der Nutzer über NFC-Chip und PIN-Eingabe in einer App identifizieren, um damit das Hotelzimmer oder den Mietwagen zu öffnen.

8.6 Technologien zur Identifikation und zur Ortung von mobilen Endgeräten

Ortung bedeutet die räumliche Standortbestimmung eines Objekts. Diese ist häufig eine bedeutsame Voraussetzung für das Zustandekommen einer mobilen Kommunikationsverbindung. Darüber hinaus können den Nutzern ortsabhängig Informationen, Werbebotschaften oder Produktangebote vermittelt werden. Im Industrie- und Dienstleistungsbereich ist die Ortung essenzielle Voraussetzung von drahtloser Steuerung ortsveränderlicher Maschinen und Fahrzeuge.

8.6.1 Ortung von mobilen Endgeräten

Bei der Ortung wird zwischen Tracking, Positioning und Tracing unterschieden. In der Logistik werden diese Begriffe für die Sendungsverfolgung verwendet. Tracking bezeichnet hierbei die Ermittlung des aktuellen Standorts in Echtzeit (z. B. wo befindet sich eine Lieferung gerade?). Positioning liegt dann vor, falls ein mobiles Endgerät aktiv seinen Standort bestimmt. Tracing beschreibt hingegen die zeitliche Rückverfolgung (Wo war die Lieferung in der Vergangenheit, welchen Weg hat sie genommen, welche Stationen passiert?).

8.6.2 Netzbasierte Ortung (Tracking)

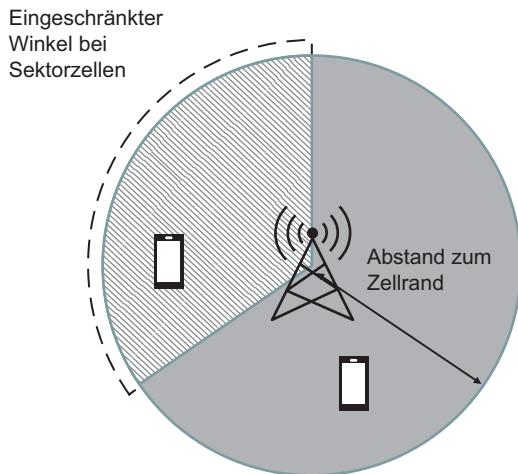
Es sind eine Reihe von netzbasierten Ortungstechniken entwickelt worden. Sie zeichnen sich dadurch aus, dass der Nutzer des Endgerätes bei der Ermittlung der Position keine Rolle spielt. Das Endgerät muss lediglich für Netz-Nachrichten empfangsbereit sein. Es empfängt die Referenzsignale und wertet sie aus. Die Ergebnisse werden an die Basisstation übertragen und im Gerät selbst gespeichert. Damit kann grundsätzlich jedes Endgerät, das sich in Betrieb befindet, geortet werden. Die netzbasierten Verfahren kommen in verschiedenen Fällen zum Einsatz.

- Die Mitwirkung des Nutzers kann nicht vorausgesetzt werden. Hier kann es sich um die Ortung des Gerätes in einem Notfall handeln. Bei dem eCall Notrufsystem in Kfz wird ein automatischer Notruf im Fall eines Unfalls abgesetzt. Die Angabe des Ortes ist hier von höchster Bedeutung.
- Die Ortung soll unbemerkt stattfinden. Dies ist in erster Linie der Fall bei Strafverfolgungsmaßnahmen. Auch ohne aktives Zutun einer observierten Person muss ihre Position ermittelt werden können, falls – und nur dann – eine entsprechende richterliche Anordnung vorliegt.
- Bei M2M-Kommunikation, zum Beispiel in der Logistik (Abschn. 8.3.2). Die Positionsdaten werden von einer Applikation auf dem Gerät ausgelesen und können so über das Netz an eine Zentrale übertragen werden.

Das einfachste Verfahren besteht in der Bestimmung der Mobilfunkzelle, in der sich das gesuchte Endgerät gerade befindet (Cell of Origin). Ist das Endgerät gerade aktiv, steht die Angabe im Netz unmittelbar zur Verfügung. Befindet sich das Endgerät in einem Ruhemodus, kann es durch eine Stille SMS (Abschn. 2.5.3) in den aktiven Zustand versetzt werden, ohne dass dies durch den Teilnehmer bemerkt wird. Die Koordinaten der Basisstation und die Größe der Zelle sind dem Netzbetreiber genau bekannt. Die Genauigkeit der Ortsangabe des Endgerätes ist wegen der Größe der Zellen allerdings begrenzt. Für eine rundstrahlende Antenne liefert die Zell-ID-Angabe lediglich den Radius der Zelle als den maximal möglichen Abstand zur Basisstation. Eine Sektorantenne mit 120 Grad Sektorwinkel liefert zusätzlich eine grobe Richtungsangabe (Abb. 8.16).

Basisstationen bestimmen laufend für jeden aktiven Teilnehmer die sogenannte Timing Advance (TA). Damit werden die Laufzeitunterschiede der Signale von verschieden weit

Abb. 8.16 Ortung mittels Cell of Origin bei Sektorzelle und 360 Grad-Zelle



entfernten Endgeräten ausgeglichen. Die TA ist der Zeitversatz, um den ein Endgerät früher senden muss, damit seine Signale im richtigen Zeitabschnitt bei der Basisstation ankommen. Da die Basisstation gewisse Ungenauigkeiten eliminieren kann, wird die TA in ganzzahligen Stufen, den TA-Intervallen, angegeben. Jede solche Stufe entspricht einem Entfernungsbereich. Bei GSM ist ein TA-Intervall ca. 3,7 µs lang, entsprechend einer Entfernungsdifferenz von ca. 550 m; bei LTE sind es 1282 TA-Intervalle von ca. 0,5 µs entsprechend einer Entfernungsdifferenz von etwa 80 m.

Falls diese Information zusätzlich für eine Ortung herangezogen werden kann, wird der Standort des mobilen Endgeräts wesentlich genauer bestimmbar. In Abb. 8.17 wird die Situation am Beispiel einer 120 Grad-Sektorzelle illustriert.

In modernen LTE- und 5G-Netzen wird das Verfahren Observed Time Difference of Arrival (OTDOA) verwendet. Dabei senden die Basisstationen einer ganzen Region synchrone Referenzsignale eingebettet in die Datenblöcke für ein bestimmtes Endgerät. Das Endgerät zeichnet die Laufzeitunterschiede der empfangenen Signale der Stationen auf und überträgt sie zurück an das Netz. Empfängt das Endgerät die Referenzsignale von wenigstens drei Basisstationen, kann das Netz aus einer Triangulation, einem geometrischen Messverfahren, den Benutzerstandort errechnen. Abb. 8.18 illustriert das Verfahren. Messungen können innerhalb von Sekunden einige hundert Mal durchgeführt werden, so dass mittels statistischer Methoden die Genauigkeit bis in den Bereich weniger Meter gesteigert werden kann. Die Auswertung und Rückmeldung der Laufzeitdifferenzen ist Teil des LTE-Protokolls und wird von der Endgeräte-Hardware automatisch bei Empfang dieser Signale ausgeführt. Eine Zustimmung oder Mitwirkung des Nutzers ist auf der Seite des Endgerätes nicht vorgesehen. Da diese Ortungsfunktion Netzressourcen bindet, wird sie nicht regelhaft, sondern nur bei Bedarf und ggfs. nach Genehmigung durchgeführt.

In der Mobilfunkgeneration 5G ist eine schnelle und hochgenaue Ortsbestimmung von Endgeräten ein zentrales Feature. Dies ergibt sich bereits aus wichtigen Anwendungsgebieten wie Industrie 4.0, Internet of Things und Autonomes Fahren. So soll eine Genauigkeit von deutlich unter 1 m gewährleistet sein.

Abb. 8.17 Ortung mittels Cell-of-Origin und Timing Advance (TA) in einer Sektorzelle

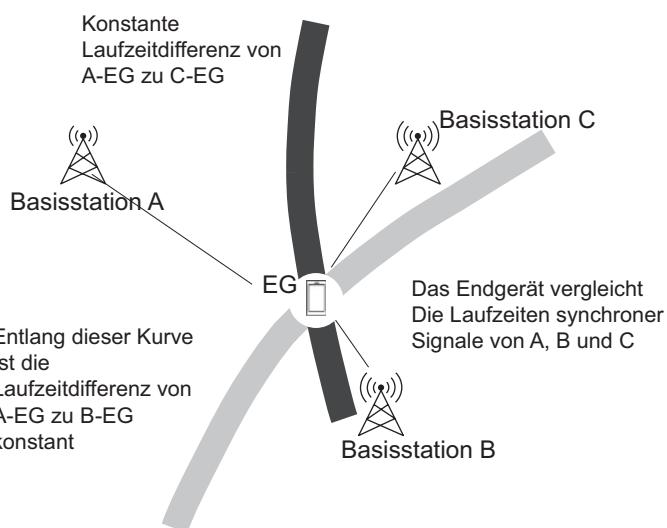
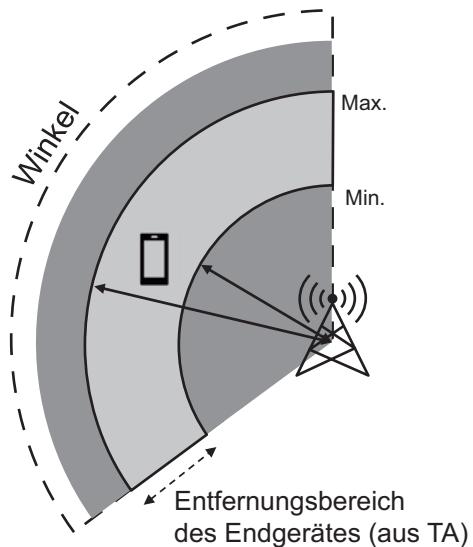


Abb. 8.18 Ortsbestimmung mittels Observed Time Difference of Arrival

8.6.3 Terminalbasierte Ortung (Positioning)

Bei diesem Verfahren führt das mobile Endgerät (Terminal) die Ortung selbst durch. Im einfachsten Fall erfolgt die Eingabe von Standordaten manuell durch den Benutzer, beispielsweise in Form von Postleitzahl, Ortsname oder Straßennamen.

Weit verbreitet ist die Ermittlung einer geografischen Position durch die Verarbeitung von Funksignalen der Satelliten eines Global Navigation Satellite Systems (GNSS). GNSS Systeme sind zum Beispiel das bekannte amerikanische Global Positioning System (GPS), das von der Europäischen Union betriebene GALILEO oder das russische GLONASS. Die Darstellung konzentriert sich hier auf das am weitesten verbreitete GPS. Über den Empfang der Referenz-Signale von einigen (typischerweise 4–12) der insgesamt 32 GPS-Satelliten und durch ein im mobilen Endgerät verbautes GPS-Modul lässt sich der Standort errechnen. Die GPS-Satelliten senden in einem lizenzierten Frequenzband im 1,6 GHz-Bereich laufend die eigene Position und den durch eine Atomuhr hochgenau ermittelten Zeitstempel. Das Endgerät empfängt die Positionssignale der Satelliten und errechnet hieraus den aktuellen Standort (Abb. 8.19). Dabei werden, ähnlich wie bei der OTDOA-Methode bei LTE, die Laufzeitdifferenzen der Signale verschiedener Satelliten verwendet. Die Verwendung der Laufzeitdifferenzen an Stelle der absoluten Laufzeiten eliminiert eine ungenaue Eigenzeit des Endgerätes aus der Rechnung. Mit dem Verfahren ist eine Genauigkeit der Ortung von bis zu wenigen Metern erzielbar. Die im Einzelfall tatsächlich erzielte Genauigkeit hängt allerdings stark von der Anzahl der empfangenen Satelliten und der Möglichkeit der Korrektur von Satelliten-Bahndaten ab. Die Zeitstempel auf dem verschlüsselten militärischen Frequenzband von GPS werden zusätzlich enger getaktet und erlauben dadurch eine höhere Genauigkeit. Dieses Frequenzband wird für militärische Anwendungen und für die Navigation im Luftverkehr verwendet.

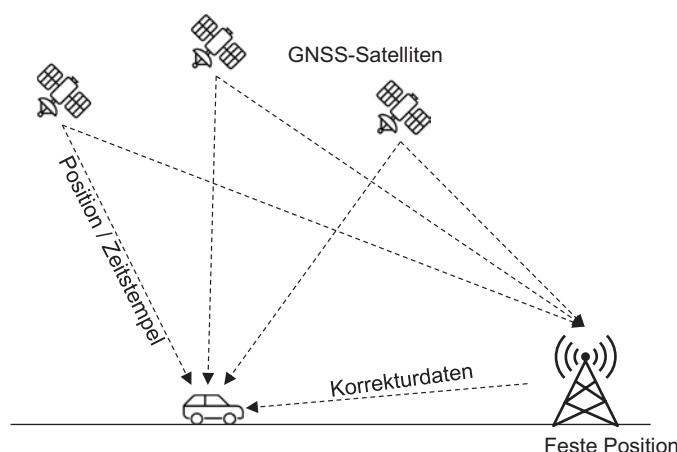


Abb. 8.19 Grundprinzip der Satellitenortung

Eine Nebenanwendung des GPS-Systems besteht in der Zeitsynchronisation von örtlich verteilten Anwendungen. Räumlich entfernte technische Systeme können mittels GPS-Empfängern in synchronem Takt laufen. Dies wird in Glasfaser-Weitverkehrsnetzen, für Bahnhofsuhrnen, aber auch für die Kommunikationssteuerung von vernetzten Fahrzeugen beim autonomen Fahren (8.4.4) genutzt.

Die Nutzung der Ortung per Satellit vereint verschiedene Vor- und Nachteile. Zu den Vorteilen zählt die nahezu unbeschränkte Ortung auf einem großen Teil der Erdoberfläche. Außerdem erlaubt die Ortung per Satellit im Grunde eine hohe Genauigkeit. Das rein satellitengestützte Verfahren hat in der Praxis allerdings auch deutliche Schwächen: Die Satellitenbahnen unterliegen Schwankungen und das Signal ist durch die lange Laufstrecke verzerrt. Unter Umständen kann das Auffinden einer ausreichenden Anzahl von Satellitensignalen durch den Empfänger mehrere Minuten in Anspruch nehmen. In Städten mit tiefen Straßenschluchten gelingt dies häufig nicht. In Gebäuden und geschlossenen Räumen ist der Empfang der sehr schwachen Signale so gut wie ausgeschlossen.

Die von den Schwankungen der Bahnen und den Verzerrungen der Signale erzeugten Fehler werden durch das Differenzial GPS-Verfahren (DGPS) weitgehend eliminiert. Ortsfeste Stationen mit genau bekannten Positionen bestimmen laufend ihre Position aus den empfangenen Satellitendaten. Aus dem Vergleich der berechneten Positionen mit den bekannten eigenen Koordinaten ergeben sich Korrekturen, die über Radiosender an Endgeräte mit entsprechenden Antennen verteilt werden. Bei Smartphones mit GPS-Funktion kommt hier zusätzlich das Mobilfunknetz ins Spiel. Beim Assisted GPS (A-GPS) werden die Satellitendaten und Korrekturen über das Mobilfunknetz geladen. Bei GPS-Navigationssystemen, die in Fahrzeugen eingebaut sind, wird eine zeitliche Abfolge von Positions punkten mit dem vorhandenen Kartenmaterial abgeglichen, um Straßen anhand markanter Punkte wie Kurven oder Kreuzungen zu erkennen.

Stehen weder Mobilfunk-Netzwerk noch GPS zur Verfügung, können unter Umständen WLAN-Signale zur Ortung genutzt werden. Dazu muss das Smartphone die SSIDs von möglichst vielen WLAN-Netzwerken, die es im Augenblick empfängt, an den Betreiber einer WLAN-Datenbank senden. Aus den bekannten Daten zu den Positionen der WLAN Access Points kann auf die Position des Smartphones zurückgeschlossen werden. Solche Datenbanken bestehen zum Beispiel bei den Betriebssystem-Herstellern Google und Apple. Da diese Datenbanken automatisch erstellt werden, gibt es allerdings nur ungefähre Angaben über die Positionen der Access Points.

8.6.4 Ortung mittels Personal Area Networks

Die Verfügbarkeit von GNSS Signalen oder Mobilfunknetzwerken im Innenbereich ist in der Regel schlecht oder gar nicht gegeben. Es gibt jedoch eine Reihe von Gründen, auch in geschlossenen Räumen Ortung durch Funk vorzunehmen:

- Points of Interest (Abschn. 5.6.3 – iBeacon)
- Auffinden von Gegenständen
- Tracking von Objekten
- Orientierung und Navigation in Gebäuden

Genutzt werden dafür Personal Area Networks (PAN). Die beiden in Kap. 5 besprochenen PAN-Technologien Bluetooth und Zigbee erlauben es, eine Ortung vorzunehmen. Sie verwenden primär die Messung der Signalstärke (Received Signal Strength Indicator, RSSI) durch einen oder mehrere Empfänger als Basis für die Bestimmung von Entfernung oder Position. Bei Bluetooth besteht seit der Veröffentlichung des Bluetooth Standards 5.1 zusätzlich die Möglichkeit, Richtungen zu bestimmen.

Je nach Anwendungsfall kann das mobile Gerät in einer aktiven oder passiven Rolle sein. Es kommt darauf an, die aktuelle Position eines mobilen Gerätes durch das Netz mittels ortsfester Sender zu bestimmen (Tracking), oder das Gerät seine eigene Position durch Hilfssignale der ortsfesten Netzstationen finden zu lassen (Positioning).

Bluetooth

Die einfache RSSI-Messung kann die Entfernung zwischen dem Mobilgerät und der ortsfesten Netzstation („Anker“) mit einer Toleranz von 2 bis 3 Metern innerhalb einer Reichweite von 10 m bis zu 30 m bestimmen. Bei mehreren Ankern, die die Signale des Endgerätes empfangen, kann die Position durch Triangulation analog zu GPS und Mobilfunknetzen genauer bestimmt werden. In Abb. 8.20 sind die jeweiligen Bluetooth-Sender als Sendeantennen dargestellt.

Durch Verwendung der Signale von zwei Bluetooth-Referenzstationen ist mit Bluetooth 5.1 die Bestimmung von Richtungen und Winkeln relativ zur Verbindungsline der beiden Stationen möglich. Dabei werden die Laufzeitunterschiede der vom Endgerät ausgesendeten Signale von den ortsfesten POI ausgewertet (Angle of Arrival, AoA), oder das

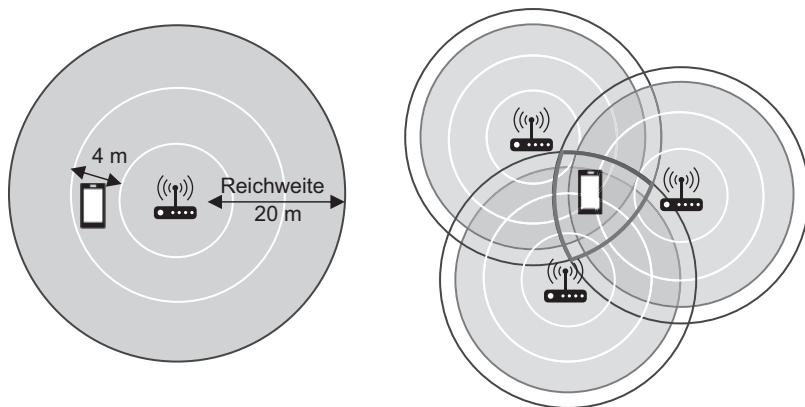


Abb. 8.20 RSSI-Messung bei Bluetooth zur Entfernungsbestimmung und Ortung

Endgerät wertet die Laufzeitunterschiede von synchron ausgesendeten Signalen der POI aus (Angle of Departure, AoD). Mit AoA lässt sich ein Tracking eines Objektes im Raum durchführen, AoD kann von einem intelligenten Bluetooth-Endgerät, wie etwa einem Smartphone, zur Navigation im Innenbereich genutzt werden.

8.6.5 Personalisierung

Neben ortsbezogenen Werbungs- und Marketingbotschaften ist für die Werbeindustrie auch der Zuschnitt auf die persönlichen Interessen des Kunden bedeutsam. Die aus dem Festnetz-Internet bekannten Cookies, die eine Identifikation des Kunden ermöglichen, sind allerdings im Mobilfunknetz nur von eingeschränktem Wert. Der Zugriff auf Anbieter-Seiten erfolgt nicht über Browser, sondern weitgehend über Apps, deren Speicherbereiche durch die Software-Architektur geschützt sind. Eine App kann in der Regel nicht auf Cookies zugreifen, die durch den Browser oder eine andere App geladen wurden.

Durch den Zugriff auf die Endgeräte-ID IMEI (Abschn. 2.3) könnten werbetreibende Unternehmen aussagefähige Nutzerprofile für Werbezwecke erstellen. Da sich aus der IMEI aber die Identität des Endgerätes und damit auch des Nutzers ermitteln lässt, ist diese Möglichkeit mit Datenschutz-Grundsätzen nicht mehr kompatibel. Die dominierenden mobilen Betriebssystemhersteller Apple und Google haben daher schon frühzeitig den Zugriff auf die IMEI durch Apps eingeschränkt. Statt der IMEI wurden der Werbeindustrie anonyme bzw. pseudonyme Identifier zur Verfügung gestellt.

Apple führte 2012 mit der Betriebssystemversion iOS6 den Identifier for Advertisers (IDFA) ein. Das Äquivalent für Android wurde von Google 2014 unter dem Namen Google Play Services ID for Android (GPS-ADID) eingeführt. Mit Hilfe einer vom Betriebssystem erzeugten zufälligen ID wird App-Entwicklern und der werbetreibenden Wirtschaft ermöglicht, auf einer anonymen Basis das Nutzerverhalten zu beobachten und gezielt Werbung zu schalten. Trotz der anonymen bzw. pseudonymen Basis bleiben die datenschutzrechtlichen Bedenken jedoch bestehen.

Bei einer hinreichend umfänglichen Sammlung von gewonnenen Daten ist auch der hinter einer IDFA oder GPS-ADID stehende Nutzer persönlich identifizierbar. Daher gab es, wenn auch versteckt, die Möglichkeit des Opt-Out per Software-Einstellung durch den Nutzer. Mit iOS 14.5 setzte Apple die IDFA per Voreinstellung auf inaktiv, und ermöglichte den Nutzern stattdessen das Opt-In per Software-Einstellungen. Bei Google ist GPS-ADID per Voreinstellung weiter aktiv. Da die wenigsten Nutzer jemals Änderungen in den tieferen Schichten der Software-Einstellungen ihres Mobiltelefons vornehmen, kann davon ausgegangen werden, dass diese Default-Werte in der Praxis unverändert beibehalten werden. Entsprechend aufgeregt reagierte die Werbebranche auf den Schritt von Apple. Es wird erwartet, dass bis zu 90 % der Nutzer die Online-Identifikation per IDFA ablehnen werden (NDION 2021).

8.7 Fragen

- 1) Nennen Sie vier Anwendungsbeispiele für mobile Marketing.
- 2) Wie unterscheidet sich das mobile Ticket der Bahn vom mobilen Ticket der Lufthansa?
- 3) Diskutieren Sie über Vor- und Nachteile von M-Ticketing.
- 4) Diskutieren Sie über Vor- und Nachteile von M-Payment.
- 5) Wie unterscheidet sich der klassische Geschäftsprozess von dem mobilen Geschäftsprozess?
- 6) Wie unterscheiden sich Opt-In-Verfahren und Out-out-Verfahren beim mobilen Marketing?
- 7) Welche zusätzliche Sicherheit bietet das doppelte Opt-In-Verfahren?
- 8) Nennen und erläutern Sie verschiedene Einsatzszenarien von mobile HRM.
- 9) Welche Geschäftsmodelle werden für die Monetarisierung von mobilen Spielen maßgeblich genutzt?
- 10) Erläutern Sie das Grundprinzip der M2M-Kommunikation.
- 11) Die Anwendung von M2M in der Logistik setzt die Anbindung an ein Mobilfunknetz voraus. Diskutieren Sie die Optionen NB-IoT und LPWA unter den Aspekten Verfügbarkeit, internationale Lieferketten, zeitnahe Statusupdates und Kosten (optional).
- 12) Unter dem Begriff „Ambient Assisted Living“ (AAL) werden verschiedene Technologien und Assistenzsysteme zusammengefasst, die Menschen bei ihren täglichen Abläufen und Lebenssituationen unterstützen. Bislang existieren vorwiegend Stand-Alone-Systeme, wie beispielsweise Pulsarmbanduhren, die den Pulsschlag und andere wichtige Körperparameter messen und an ein medizinisches Zentrum weiterleiten. Skizzieren Sie den mobilen kundenzentrierten Prozess zur Unterstützung alter Menschen, die weiterhin in ihrer vertrauten Wohnung leben möchten.
- 13) Welche Funktion hat die Messung der Timing Advance im Rahmen der netzbasierten Ortsbestimmung?
- 14) Aus welchen Gründen kann eine netzbasierte Ortung eines Mobilfunkgerätes angebracht sein? Welche rechtlichen Beschränkungen gibt es?
- 15) Wie viele Satelliten muss ein Mobiltelefon empfangen können, um eine zuverlässige GNSS-Ortsbestimmung durchzuführen?
- 16) Wozu werden Korrekturdaten zu GPS benötigt, und wie werden sie dem Endgerät zugänglich gemacht?
- 17) Welche Messung wird bei einer Ortsbestimmung durch Personal Area Networks durchgeführt?
- 18) Erläutern Sie IDFA und GPS-ADID.

Literatur

- Arzberger M, Bleckmann A, Cwik A, Fischer E, Koch M, Mengi A, Wolski T (2017) Datenkommunikation. In: Arzberger M, Zayer P, Kahmann M (Hrsg) Handbuch Elektrizitätsmesstechnik, 3. Aufl. VDE Verlag, Offenbach, S 391–444. 978-3-8022-1160-7
- Audi (2017) Fahrassistsysteme. Audi-mediacenter.de. <https://www.audi-mediacenter.com/de/technik-lexikon-7180/fahrerassistenzsysteme-7184>. Zugegriffen am 04.01.2019
- Bezahllotse (2021) Der Lotse für die Bezahlung von öffentlichen Gebühren. <https://bezahllotse.de/img/info-bezahllotse.pdf>. Zugegriffen am 26.09.2021
- Bleyh M, Feser C (2015) Zukunft des Bezahlens – Mobile Payment. In: Linnhoff-Popien C, Zadach M, Grahl A (Hrsg) Marktplätze im Umbruch. Springer, Berlin, S 379–388. <https://doi.org/10.1007/978-3-662-43782-7>
- Ericsson (2012) Maersk Line and Ericsson bring mobile connectivity to the oceans. Ericsson. <https://www.ericsson.com/en/press-releases/2012/1/maersk-line-and-ericsson-bring-mobile-connectivity-to-the-oceans>. Zugegriffen am 12.09.2019
- Ericsson (2017a) Ericsson demonstrates how massive IoT saves lives. Ericsson. <https://www.ericsson.com/en/news/2017/9/ericsson-demonstrates-how-massive-iot-saves-lives>. Zugegriffen am 28.11.2018
- Ericsson (2017b) Ericsson initiates 5G motorway project with cross-industry consortium in Germany. Ericsson. https://www.ericsson.com/news/161117-ericsson-initiates-5g-motorway-project-with-cross-industry-consortium-in-germany_244039853_c. Zugegriffen am 12.09.2019
- Geuss M (2014) How Apple Pay and Google Wallet actually work. Ars Technica. <https://arstechnica.com/gadgets/2014/10/how-mobile-payments-really-work/>. Zugegriffen am 01.09.2021
- Hülskamp G, Buse S (2008) Mobile ticketing. In: Buse S, Tiwari R (Hrsg) Perspektiven des Mobile Commerce in Deutschland. Shaker, Aachen, S 545–646. 978-3-8322-7048-3
- ISO (2021) Taxonomy and definitions for terms related to driving automation systems for on-road motor vehicles, ISO/SAE PAS 22736:2021. <https://www.iso.org/standard/73766.html>. Zugegriffen am 15.09.2021
- Möhlenbruch D, Schmieder U-M (2002) Mobile Marketing als Schlüsselgröße für Multichannel-Commerce. In: Silberer G, Wohlfahrt J, Wilhelm T (Hrsg) Mobile commerce. Gabler, Wiesbaden, S 67–89. https://doi.org/10.1007/978-3-322-90464-5_4
- Moermann J, Dohmen A (2010) Smartphone-Applikationen: Innovationspotenzial für das Retail Banking. Wirtschaftsinformatik und Management 2(4):30–35. <https://doi.org/10.1007/BF03248270>
- Mülder W (2010) Geschäftsprozessmodellierung. In: Mülder W, Abts D (Hrsg) Masterkurs Wirtschaftsinformatik. Vieweg Teubner, Wiesbaden, S 237–277. 978-3-8348-0002-2
- Mülder W (2016) Mobile human resource management. In: Barton T, Müller C, Seel C (Hrsg) Mobile Anwendungen in Unternehmen. Springer, Berlin, S 51–64. https://doi.org/10.1007/978-3-658-12010-8_4
- NDION (2021) Apple sorgt mit „Anti-Tracking-Funktion“ für Wirbel in der Werbeindustrie. <https://ndion.de/de/apple-sorgt-mit-anti-tracking-funktion-fuer-wirbel-in-der-werbeindustrie/>. Zugegriffen am 15.09.2021
- Noggler S (2016) Von der Idee zum IoT-Geschäftsmodell. www.funkschau.de/telekommunikation/artikel/133596/1/. Zugegriffen am 01.09.2016
- Schmidtz T (2020) Sparkassen: Apple Pay für die Girocard – So funktioniert der neue Bezahl-dienst. <https://www.merkur.de/wirtschaft/sparkasse-apple-pay-girocard-news-start-probleme-einrichten-fail-cupertino-90032678.html>. Zugegriffen am 15.12.2020

- Schreiber M (2018) Apps und die Datenschutz-Grundverordnung (DSGVO). <https://www.adzine.de/2018/03/apps-und-die-datenschutz-grundverordnung-dsgvo/>. Zugegriffen am 15.09.2021
- Sottek C (2012) Mobile Marketingkampagnen – Einsatz und Erfolgsfaktoren der mobilen Kundenakquise. Diplomica, Hamburg, S 978-3842879249
- Steinhoff C, Buse S (2008) Mobile marketing. In: Buse S, Tiwari R (Hrsg) Perspektiven des Mobile Commerce in Deutschland. Shaker, Aachen, S 431–544. 978-3-8322-7048-3
- Verclas S, Linnhoff-Popien C (2012) Mit Business-Apps ins Zeitalter mobiler Geschäftsprozesse. In: Verclas S, Linnhoff-Popien C (Hrsg) Smart mobile apps. Springer, Berlin, S 3–15. https://doi.org/10.1007/978-3-642-22259-7_1
- Viehmann S (2017) Echte Roboter-Funktionen statt Mogelpackung: Neuer A8 im Autobahn-Test. Focus. https://www.focus.de/auto/fahrberichte/audi-a8-stau-pilot-im-test-echte-roboter-funktionen-statt-mogelpackung-neuer-a8-im-autobahn-test_id_7539414.html. Zugegriffen am 15.09.2021
- Weis HC (2018) Marketing, 18. Aufl. Kiehl, Ludwigshafen. 978-3-470-51278-5



Sicherheit und Gesundheit

9

9.1 Einführung und Lernziele

Sicherheit stellt ein elementares menschliches Bedürfnis dar und ist auch bei Mobilfunk und im Mobile Business von zentraler Bedeutung. Die Sicherheit wird unter anderem gefährdet durch aktive und passive Angriffe Dritter, wie beispielsweise das Abhören von Datenübertragungen oder die Manipulation vertraulicher Daten durch Infizierung eines Endgerätes mittels einer Schadsoftware. Aber auch ein unbewusster Umgang mit mobiler Kommunikation durch den Nutzer, z. B. bei Telefonaten im öffentlichen Raum, kann zu Risiken führen. Daneben findet sich oftmals eine öffentliche Diskussion zur Auswirkung der Mobilfunknutzung auf die menschliche Gesundheit.

Im Folgenden soll auf ausgewählte Aspekte eingegangen werden, ohne dabei die Literatur zur IT-Sicherheit oder zu gesundheitsschädlichen Folgen bei einer intensiven Nutzung von mobilen Endgeräten ersetzen zu wollen.

► Lernziele

- Sie lernen welche Sicherheitsziele bei mobiler Kommunikation und im Mobile Business verfolgt werden.
- Sie lernen welche Sicherheitsprobleme und Gefährdungen auftreten können.
- Sie lernen welche organisatorischen Schutzmaßnahmen getroffen werden sollten.
- Sie lernen welche Gestaltungsmöglichkeiten für den Einsatz mobiler Endgeräte im Unternehmen gegeben sind.
- Sie lernen ob eine Nutzung des Mobilfunk und mobiler Endgeräte gesundheitsschädlich ist oder nicht.

9.2 Schutzziele

Zur gezielten Abwehr von Angriffen ist in Unternehmen ein Konzept für die mobile IT-Sicherheit erforderlich. Hierbei stehen die folgenden Schutzziele im Mittelpunkt (Abb. 9.1).

Vertraulichkeit bedeutet, dass nur autorisierte Benutzer einen Zugriff auf Systeme und Daten erhalten. Ein Verlust der Vertraulichkeit entsteht, falls Daten an die falschen Adressaten gelangen, z. B. Kundendaten an Konkurrenzunternehmen übermittelt werden.

Integrität bedeutet, dass zu übermittelnde Daten nicht unautorisiert und unbemerkt manipuliert werden können. Hierzu zählen das Löschen, die Vervielfältigung oder die Änderung von Daten.

Verfügbarkeit bedeutet, dass das System für befugte Benutzer zum gewünschten Zeitpunkt im richtigen Umfang zugänglich und funktionstüchtig ist. Es sollen vor allem der Ausfall von Servern und Netzwerk sowie der Verlust gespeicherter Daten verhindert werden.

Authentizität soll die Echtheit der Kommunikationspartner und der ausgetauschten Daten garantieren, die anhand einer eindeutigen Identität und charakterisierender Eigenschaften festgestellt wird.

Verbindlichkeit meint, dass ein Benutzer von ihm durchgeführte Aktionen, insbesondere wirtschaftliche Transaktionen, nachträglich nicht abstreiten kann.

Datenschutz umfasst insbesondere den Schutz geschäftskritischer sowie personenbezogener Daten.

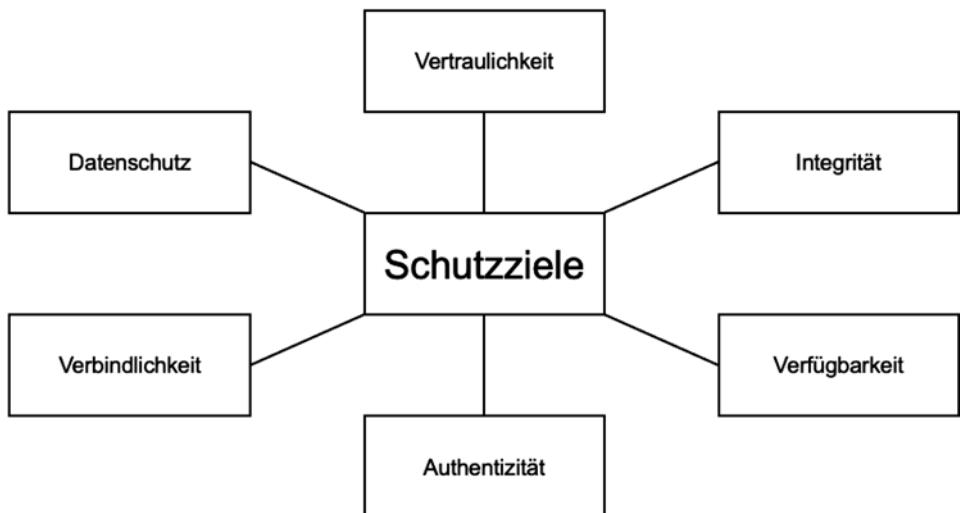


Abb. 9.1 Schutzziele der IT-Sicherheit

Im Rahmen der IT-Sicherheit werden diese Schutzziele mitsamt den bestehenden Risiken für Nutzer und Unternehmen ausgiebig diskutiert. In der Literatur hierzu finden sich zahlreiche Maßnahmen, die zur Erreichung der Schutzziele getroffen werden können.

9.3 Angriffsmöglichkeiten im Mobilfunksystem

Die Funkschnittstelle kann von niemandem exklusiv genutzt werden und ist umgekehrt für jedermann frei zugänglich. Während diese im Nahbereich, z. B. bei NFC, nur wenige Zentimeter und bei WLAN meistens nur wenige Meter ausmacht, beträgt die Distanz bei Mobilfunk zwischen mehreren hundert Metern und einigen Kilometern. Beispielhaft sollen hier zwei mögliche Angriffswege genannt werden: Bei einer Man-in-the-Middle-Attacke gibt ein Angreifer sich als Bestandteil der Mobilfunknetzwerkinfrastruktur aus, hört so Daten ab (passiver Angriff) oder versucht, eigene Daten einzuschleusen oder Daten zu manipulieren (aktiver Angriff). Bei einer Denial-of-Service-Attacke verursacht der Angreifer eine Überlastung des Kommunikationskanals, um hierdurch die Funktionsfähigkeit des Systems außer Kraft zu setzen.

Mobile Endgeräte sind über Funksignale mit anderen Geräten und dem Netz verbunden. Eine Funkverbindung ist zunächst grundsätzlich angreifbar. Wer über eine passende Antenne verfügt, kann die Signale empfangen. Es stellt sich damit die Frage, ob und wie diese Funkstecken und die verbundenen Netze durch Betreiber und Technologie abgesichert werden können und wie sie tatsächlich abgesichert sind. Diese Frage wird im Folgenden für den öffentlichen Mobilfunk und WLAN diskutiert.

9.3.1 Sicherheit im öffentlichen Mobilfunk

Die Entfernung eines mobilen Endgeräts zu den Antennenanlagen des öffentlichen Mobilfunknetzes kann zwischen wenigen hundert Metern und 30 Kilometern variieren. Entsprechend unübersichtlich würde sich für den Nutzer die Sicherheitslage darstellen, falls diese Funkstrecken nicht besonders gesichert wären. Jede in ein mobiles Endgerät eingebaute Antenne ist ein perfekt abgestimmter Empfänger für alle Signale und Daten, die über die Funkschnittstelle ausgetauscht werden. Daher wurde seit Beginn des digitalen Mobilfunks Anfang der 1990er-Jahre großen Wert auf die Authentifizierung der Teilnehmer am Mobilfunksystem und die Verschlüsselung der übertragenen Daten gelegt.

Die Mechanismen haben sich im Laufe der nun vier Generationen (2G bis 5G) verändert und stark verbessert, so dass der Funkverkehr in Mobilfunknetzen heute als weitgehend sicher gelten kann. Nachfolgend werden einzelne Sicherheits-Maßnahmen und die verbleibenden Risiken kurz erläutert.

SIM-Karten als Sicherheitsmerkmal Das in Kap. 2 beschriebene Subscriber Identification Module (SIM) ist ein zentrales Sicherheitsmerkmal seit der zweiten Generation des Mobilfunks. Durch das SIM werden Teilnehmer und mobiles Endgerät logisch voneinander getrennt. Das Recht zum Netzzugang gehört zum Teilnehmer und zur SIM-Karte. Wechselt der Teilnehmer die SIM-Karte auf ein neues Endgerät, greift dieses auf dasselbe Mobilfunknetzwerk zu. Zusammen mit der allgemeinen Teilnehmerdatenbank auf Seiten des Mobilfunknetzwerkbetreibers identifiziert das SIM bzw. seine Weiterentwicklung Universal SIM (USIM) durch die im gesicherten Speicherbereich der Karte enthaltenen Algorithmen und Schlüsseldaten den Teilnehmer eindeutig gegenüber dem Mobilfunknetzwerk und erstellt einen mit dem Netz gemeinsam genutzten symmetrischen Schlüssel, der die Daten auf der Funkschnittstelle gegen Abhören schützt. Das USIM verlangt im Rahmen der Authentifizierung zusätzlich eine Identifikation des Mobilfunknetzwerks gegenüber dem Teilnehmer – eine Funktionalität, welche unten noch angesprochen wird.

SIM-Karte im GSM Durch das in Kap. 2 beschriebene Challenge-Response Verfahren vereinbaren das mobile Endgerät und das Netz einen individuellen Code, mit dem der Funkverkehr nach dem Data Encryption Standard (DES) verschlüsselt werden kann. Diese Vereinbarung verlangt lediglich den Austausch eines zufälligen Zahlen-codes; die Verifikation der ID und die Berechnung des Schlüssels erfolgen auf beiden Seiten unabhängig voneinander. Mit Ausnahme der zu Beginn vom Teilnehmer über-sandten Identifikations-Nummer sind alle ausgetauschten Daten bereits verschlüsselt. Ohne Kenntnis des Codes ist es Außenstehenden unmöglich, die Schnittstelle abzu-hören. Durch den Einsatz eines IMSI Catchers kann beim GSM und UMTS-Netzen jedoch eine Sicherheitslücke ausgenutzt werden, die es erlaubt, eine Man-in-The-Middle-Attacke durchzuführen.

IMSI Catcher IMSI Catcher wurden in den 1990er-Jahren durch das Unternehmen Rohde und Schwarz zur Nutzung durch Aufsichtsbehörden und Strafverfolgung ent-wickelt. Heute sind international verschiedene Modelle erhältlich. Der Betrieb solcher Geräte außerhalb des engen berechtigten Personenkreises ist illegal und wird strafrech-tlich verfolgt. IMSI Catcher simulieren eine Mobilfunk-Basisstation. Durch räumliche Nähe zum Endgerät und hohe Sendeleistung werden sie zur bevorzugten Basisstation bei der Kontaktaufnahme zu einem Netz. Ihre eigentliche Anwendung besteht darin, die un-verschlüsselt übertragene IMSI beziehungsweise die temporäre TMSI eines mobilen End-geräts zu ermitteln. Der weitergehende Verbindungswunsch wird dann abgelehnt, so dass das Gerät sich erneut auf Netzsuche macht. Mit Hilfe dieses Datums können dann über Netzbetreiber Abhörmaßnahmen, Ortungen und Fangschaltungen realisiert werden. Der Hintergrund ist, dass für kriminelle Zwecke vorwiegend anonyme Prepaid SIM-Karten

genutzt werden. Ist ihre IMSI bekannt, können sie allerdings genauso abgehört werden, wie normale Telefongespräche. Das Abhören erfolgt dann in der Regel nicht über die Funkschnittstelle, sondern komfortabel über eine Schnittstelle im Kern-Netz.

UMTS Mit dem UMTS System wurde die verbesserte USIM Anwendung eingeführt. Die Algorithmen sehen jetzt eine beidseitige Authentifizierung von mobilem Endgerät und Netz vor. Zusätzlich wurde der genutzte Verschlüsselungsalgorithmus verbessert.

LTE und 5G Mit dem 4G Standard LTE wurde endgültig die Unterstützung des SIM eingestellt und grundsätzlich das USIM mit der beidseitigen Authentifizierung eingeführt. Die Funktion eines IMSI Catchers beschränkt sich dann auf die Gewinnung der IMSI. Der an IMSI Catchern interessierte Personenkreis schränkt sich automatisch auf Strafverfolger und Personenkreise ein, die mittels der IMSI weitergehende Daten erhalten können.

Sicherheitslücken im Kern-Netz Der Verbindungsaufbau im Kern-Netz eines Mobilfunknetzes beruht auf dem weltweit in der Telekommunikation eingesetzten und von der ITU standardisierten Signaling System Number 7 (SS7). Die Sicherheit dieser Protokollsuite aus den 1980er-Jahren ergab sich historisch durch die Tatsache, dass die genutzte Technologie in einem abgeschlossenen Netz durch Außenstehende überhaupt nicht zugänglich war. Heute wird im Kern-Netz auch zum Signal-Austausch IP eingesetzt. Dabei ist die Applikationsschicht nach wie vor kompatibel mit SS7. An der Netzgrenze und im Übergang zu anderen Netzen entsteht so eine Angriffsfläche für Angreifer. Durch einen Zugriff auf SS7 kann ein Angreifer zum Beispiel Telefongespräche oder SMS umleiten. Solche Angriffe sind tatsächlich als Demonstration durchgeführt worden (Engel 2014). Durch Umleiten von SMS konnte ein Angriff auf ein Bankkonto durchgeführt werden, bei dem der Kontoinhaber das sogenannte mTAN Verfahren, also die Übertragung der TAN Nummer in einer SMS, nutzte. Auch moderne 2-Wege Verfahren, bei denen eine zusätzliche Sicherheit über einen per SMS an ein Mobilgerät zugesandten Autorisierungscode geschaffen werden soll, können so kompromittiert werden. Datenverbindungen sind von dieser Sicherheitslücke nicht betroffen, da die entsprechende Software keine SS7 Elemente nutzt.

9.3.2 Sicherheit im WLAN

Über drahtlose Netzwerke können im Unternehmen und im privaten Haushalt mobile Endgeräte mit einem Router und somit mit dem Internet verbunden werden. Falls das WLAN von einem Angreifer „geknackt“ wurde, erhält dieser Zugriff auf unterschiedliche Geräte

und gespeicherte Daten. Im Gegensatz zum öffentlichen Mobilfunk steht es um die Sicherheit im Wireless Local Area Network (WLAN) nicht zum Besten. Das liegt zum Teil an der Technik selbst; viel häufiger ist es aber auch der vielfach sorglose Umgang mit der Technik, der die Möglichkeit für Angriffe und Lauschaktionen schafft.

WLANs sind lokale Netze, die in den meisten Fällen einen Access Point haben. In Unternehmensnetzen oder Hotels finden sich alternativ eine Reihe von vernetzten WLAN Access Points mit identischen Zugangsdaten (ein sogenanntes Mesh), um trotz der kurzen Reichweite der einzelnen Access Points einen größeren Bereich zu überdecken.

WLANs erlauben eine Verschlüsselung des Funkverkehrs; allerdings in der Regel nur durch einen gemeinsamen Schlüssel aller im lokalen Netz angeschlossenen Teilnehmer. Damit sind Lauschangriffe innerhalb des lokalen Netzes ohne weiteres zu realisieren. Die in Hotels und vielen freien Hotspots geforderte Anmeldeprozedur mit Passwort dient entgegen einem häufigen Missverständnis nicht etwa der Verschlüsselung, sondern ist lediglich eine Registrierung und Autorisierung der Teilnehmer. Da der Funkverkehr in diesen Netzen somit gänzlich unverschlüsselt ist, können auch nicht angemeldete Geräte von außerhalb auf den gesamten Datenaustausch zugreifen.

Das Spektrum der möglichen Angriffe geht von Denial-of-Service über Identitätsdiebstahl (Identity-Theft), Man-in-the-Middle-Angriffe bis zur Übernahme des Netzes im Administrator-Modus. Für Unternehmen mit WLANs besteht auch das Risiko, dass ein Angriff auf einen angeschlossenen PC oder ein angeschlossenes mobiles Endgerät dazu führt, diese als WLAN-Brücke ins Unternehmensnetz zu benutzen. Ein so angeschlossener Angreifer hat wenige Hindernisse für einen Angriff zu befürchten. Der initiale Angriff kann auch in einem ungeschützten Netz, zum Beispiel während eines Hotelaufenthalts bei einer Geschäftsreise erfolgen.

Die Kommunikation über ein WLAN ist daher mit einem gewissen Risiko verbunden. Deshalb ist der erste Sicherheitshinweis, WLAN nach Möglichkeit nicht zu benutzen, wenn es Alternativen gibt. Fast überall stellt der mobile Zugang durch die öffentlichen Netze einen sehr viel sichereren Weg ins Internet dar. Ist WLAN-Nutzung unvermeidlich, sollte nach Möglichkeit ein verschlüsseltes Virtual Private Network (VPN) genutzt werden. In jedem Fall sollten Netz-Transaktionen jeglicher Art, inklusive Onlinebanking und Einkauf in Online-Shops über eine auf Transport-Level gesicherte Transport Layer Security (TLS) Verbindung durchgeführt werden. TLS Verbindungen mittels Hypertext Transfer Protocol lassen sich erkennen an der Zeichenkette *https*. Es muss allerdings an dieser Stelle darauf hingewiesen werden, dass *https*-Verbindungen allein keine Sicherheitsgarantie darstellen. Die umgeleitete Verbindung zu einem Malware-Server kann ohne weiteres über *https* laufen.

Für die WLAN-Verschlüsselung existieren die Standards WPA2 und WPA3 (Wifi Protected Access). Sowohl Router als auch Endgeräte müssen dieses Verfahren unterstützen. WPA2 gilt trotz einiger bekannter Lücken als relativ sicher. WPA3 schließt die Sicherheitslücken von WPA2 und ist damit derzeit der Standard mit der höchsten Sicherheit, allerdings verfügen (noch) nicht alle Geräte über dieses Verfahren. Es ist auch nicht zu

erwarten, dass der Wettkampf um die Entdeckung und Behebung von Schwachstellen damit beendet werden kann. Die Verschlüsselung erweist sich jedenfalls als wirkungslos, wenn ein Angreifer Zugriff auf das Passwort erhält oder dieses errät. Ab Werk voreingestellte Passwörter lassen sich oftmals auf der Unterseite eines Routers ablesen und sollten geändert werden. Falls möglich, ist eine MAC-Addressfiltrierung anzuraten, die nur Geräte mit bekannten MAC-Adressen zulässt. Bei allen angeschlossenen Endgeräten sollte sichergestellt sein, dass sie nicht selbst als WLAN Access Point mit Brückenfunktion missbraucht werden können. Die vereinfachte Anmeldeprozedur per WPS mit PIN sollte ausgestellt sein, denn sie öffnet ein Sicherheits-Fenster: Am Ende muss ein Angreifer per WPS lediglich drei oder vier Dezimalziffern der PIN erraten; alle anderen Stellen dienen der Fehlerkorrektur.

Unternehmensweite WLANs müssen professionell geschützt werden. Neben den beschriebenen Maßnahmen gehört dazu eine engmaschige Zugangskontrolle durch den Access Point nach dem IEEE 802.1X Authentifikations-Standard mit einem Enterprise Authentication Server. Bei dieser Prozedur verlangt das Netz nach erfolgtem Zugriff auf den Access Point eine Authentifizierung mittels Zertifikats, bevor der Zugriff auf Netz-Ressourcen freigegeben wird.

9.4 Schutzmaßnahmen

Die mobilen Nutzer sind in erheblichem Maße selbst für die Sicherheit verantwortlich. Daher sind verschiedene Maßnahmen zu ergreifen.

9.4.1 Organisatorische Schutzmaßnahmen

Organisatorische Regelungen sind daher insbesondere für Unternehmen bedeutsam, deren Mitarbeiter mobile Endgeräte einsetzen. Die Bewusstmachung von Schwachstellen ist jedoch auch in der rein privaten Nutzung mobiler Endgeräte hilfreich. Aufklärung und Schulung können unterstützen, bedeutsame Verhaltensregeln einzuhalten. In Unternehmen können diese im Rahmen einer *Sicherheitsrichtlinie* oder Betriebsvereinbarung festgelegt werden. Bedeutsam sind beispielsweise folgende Fragestellungen:

- Welche (sensiblen) Daten werden auf dem mobilen Endgerät gespeichert?
- Welche Apps werden auf dem mobilen Endgerät installiert und welche nicht?
- Welche Freigaben werden Apps für Zugriffe auf Daten erteilt?
- Wie wird ein unbefugter Zugriff verhindert (z. B. Passwort)?
- Wird ein mobiles Endgerät auch privat genutzt (falls ein Unternehmen die Hardware bereitstellt)?
- Wird das Gerät in lokale Netzwerke eingebunden?
- Gibt es zeitliche Nutzungsbeschränkungen (nachts, im Urlaub)?

- Werden durch Ortung Persönlichkeitsrechte des Einzelnen tangiert?
- Wird eine Fern sperre (Lock Down) oder die Datenlöschung aus der Ferne (Remote Wipe) für Smartphones eingerichtet?
- Kann das Gerät bei unzulässiger Nutzung (z. B. Umgehung herstellerseitig vorgesehener Sicherheitsmaßnahmen) dennoch zentral gesperrt werden?

Für das Unternehmen ist die kontinuierliche Schulung und Erinnerung der Mitarbeiter zu den Risiken essentiell. Die bekannten Social Engineering Angriffe wie Phishing, Smishing etc. können durch technische Maßnahmen kaum verhindert werden. Sie sind mit bei Mobilgeräten besonders effektiv. Durch die kleinen Bildschirme von Mobiltelefonen fällt eine sorgfältige Prüfung eines Links in einer empfangenen Message oft aus. Und gerade erfolgreich auf Mobiltelefonen platzierte Spyware kann dem Angreifer tiefe Einblicke in betriebliche Abläufe und Daten geben, da das Mobiltelefon fast immer am Körper getragen wird.

Die Nutzung mobiler Endgeräte in Berufs- und Privatleben birgt die Gefahr, dass die Grenzen zwischen Arbeitszeit und Freizeit verschwinden. Daraus kann ein Ungleichgewicht der Work-Life-Balance entstehen. Dieses Problem wird inzwischen von vielen mobil arbeitenden Beschäftigten erkannt. Manche Unternehmen erwarten, dass Mitarbeiter ständig erreichbar sind und auch in ihrer Freizeit kurzfristig geschäftliche Aufgaben übernehmen. Für Unternehmen bedeutet mobiles Arbeiten daher oftmals eine Ausweitung der Ansprech- und Arbeitszeiten. Für die Mitarbeiter bringt diese Form der Arbeit ein höheres Maß an Flexibilität, denn viele Bürotätigkeiten lassen sich dank mobiler Endgeräte zuhause, im Hotel oder im Zug erledigen. Viele Unternehmen haben für mobiles Arbeiten inzwischen klare Regeln vereinbart. Beispielsweise kann die Nutzung von E-Mails über mobile Endgeräte nach Feierabend im Rahmen einer Betriebsvereinbarung zeitlich geregelt werden.

9.4.2 Mobile Device Management

Zunehmend setzen Unternehmen gesonderte Software ein, die eine sichere Nutzung von mobilen Endgeräten ermöglichen. Diese Lösungen werden als Mobile Device Management-Systeme bezeichnet. Hierbei handelt es sich um Software, die sämtliche administrativen Maßnahmen für die sichere Nutzung mobiler Endgeräte umfasst. Bereits seit längerem existieren Systeme für Device-, Client- oder Asset Management, womit die Verwaltung von Endgeräten und Client-Software von der Beschaffung über Installation und Betrieb bis zur Entsorgung ermöglicht wird.

Bei Inventarisierung und Lizenzmanagement steht die Frage im Vordergrund, welche Geräte im Unternehmen vorhanden sind und welche Software darauf installiert wurde. Konkret sollten die IMEI, das installierte Betriebssystem mit Versionsnummer, die installierten Apps sowie die verwendete SIM-Karte inventarisiert werden. Lizenzverträge regeln die bestimmungsgemäße Verwendung von Software auf den Endgeräten. Aus rechtlichen Gründen dürfen nicht zu wenige Lizenzen gekauft werden, aus ökonomischen Gründen sollten auch keine unnötigen Nutzungsrechte existieren. Bei mobilen Endgeräten ist Lizenzmanagement bislang noch von geringerer Bedeutung, weil das Betriebssystem

in der Regel bereits installiert ist. Die Apps werden zumeist gezielt über Marktplätze (Stores) gekauft und nicht wie bei Desktop-Anwendungen als Lizizenzen in größerer Stückzahl. Eine Besonderheit ergibt sich für die Vertragsgestaltung mit den Mobilfunknetzwerkbetreibern. Vielfach haben Unternehmen Volumenverträge abgeschlossen und bezahlen einen festen Preis für die Kommunikation in Mobilfunknetzen. Mobile Device Management berücksichtigt daher die Gestaltung von Mobilfunkverträgen.

Betriebssystem und Anwendungssoftware müssen auf den mobilen Endgeräten erstmalig installiert werden, ferner müssen Updates und Backups nachträglich überspielt werden können. Schadprogramme nutzen oftmals Schwachstellen bei Betriebs- und Anwendungssystemen aus. Die Hersteller schließen diese Lücken durch sogenannte Patches, die jedoch zeitnah auf allen Endgeräten installiert werden müssen. Die Installation von mobilen Anwendungsprogrammen erfolgt über Marktplätze. Allerdings war dieses Verfahren ursprünglich nicht für Unternehmen und nicht für Business Apps vorgesehen. Im geschäftlichen Umfeld kann die Installation von Apps nicht jedem einzelnen Nutzer überlassen werden. Die Business Apps müssen den Sicherheitsstandards des Unternehmens entsprechen und das Unternehmen muss darüber entscheiden, welche Apps von welchen Nutzern verwendet werden dürfen. Als Lösung kann ein eigener Unternehmensmarktplatz aufgebaut werden, auf dem nur Apps angeboten werden, die vom Unternehmen geprüft und zugelassen wurden. Neben Bereitstellung der möglichen Apps (Positivliste bzw. Whitelist) können umgekehrt Applikationen aufgelistet werden, deren Nutzung ausgeschlossen wird, weil sie ein zu großes Risiko darstellen (Negativliste bzw. Blacklist). Beide Prinzipien haben Vor- und Nachteile. Die Positivliste kann von den Nutzern als zu starke Reglementierung empfunden werden und muss deswegen häufiger um neue Apps erweitert werden, wodurch der administrative Aufwand steigt. Andererseits wurde jede Business App vorher überprüft und bewusst zugelassen. Bei der Negativliste ist es genau umgekehrt. Unsichere oder unerwünschte Apps werden regelmäßig erst dann in die Liste aufgenommen, wenn bereits ein Schaden eingetreten ist. Somit ist dieses Prinzip risikanter, wird dennoch aufgrund der größeren Wahlfreiheit für die Benutzer oftmals bevorzugt.

Bei Verlust oder Diebstahl eines mobilen Gerätes müssen schnellstmöglich Vorrkehrungen getroffen werden, um Schäden vom Unternehmen abwenden. Beispielsweise können die Fernlöschung und die Sperrung von mobilen Endgeräten vorgenommen werden. Fernlöschung stellt sicher, dass keine sensiblen Daten in unautorisierte Hände gelangen.

Alternativ kann der Zugriff von mobilen Endgeräten auf Unternehmensnetze und -daten grundsätzlich über eine einzige, durch Passwort und andere Maßnahmen (z. B. biometrische Absicherung) gesicherte Zugriffs-App gestattet werden, die dem Nutzer einen Enterprise-Desktop über ein VPN zur Verfügung stellt. Die Unternehmens-IT braucht dann nur noch einige wenige Zugriffs-Apps verwalten. Als Bedingung für die Nutzung von privaten mobilen Endgeräten muss dann die Kompatibilität mit einer Zugriffs-App verlangt werden.

9.4.3 Nutzungsformen privater mobiler Endgeräte in Unternehmen

Mobile Endgeräte setzen sich für die private Nutzung schneller durch als für den geschäftlichen Einsatz. Durch die intensive private Nutzung entstand der Wunsch, die priva-

ten Endgeräte auch im Unternehmen zu nutzen. In der Konsequenz entstanden Konzepte zur sicheren Integration privater Endgeräte im Unternehmen unter der Bezeichnung „bring your own device“ (BYOD). Ein Nutzer verwendet also privat angeschaffte mobile Endgeräte für dienstliche Zwecke, wobei die Geräte in die Infrastruktur des Unternehmens eingebunden werden müssen, also beispielsweise den Zugriff auf interne Datenbanken ermöglichen. Das Unternehmen erspart sich die Anschaffungs- und Schulungskosten, da sich die Nutzer regelmäßig sehr gut mit ihren eigenen Geräten auskennen. Die Benutzer arbeiten motivierter und sind zufriedener, weil sie sich ihr Arbeitsgerät nach ihren eigenen Bedürfnissen ausgewählt haben. Aufgrund der ständigen Erreichbarkeit und Nutzung werden die Mitarbeiter allerdings auch in der Freizeit oder während des Urlaubs Informationen abrufen und geschäftliche Aufgaben erledigen. Die Trennung zwischen Beruf und Freizeit wird hierdurch aufgehoben.

Bei BYOD entstehen auch erhebliche Nachteile und Risiken. An erster Stelle muss die Sicherheit genannt werden. Bei mitgebrachten Privatgeräten handelt es sich nicht um vor-konfigurierte Geräte des Unternehmens. Die Funktionen der privaten Geräte sind nicht eingeschränkt, die Nutzer haben bei ihrem Gerät die vollständige administrative Berechtigung und können somit lokal auf ihren Geräten z. B. neue Apps installieren oder Eingaben konfigurieren. Hierdurch kann Schadsoftware in die allgemeine IT-Infrastruktur eindringen. Neben dem erhöhten Sicherheitsrisiko lässt sich eine heterogene IT-Landschaft, bei dem jeder Nutzer sein bevorzugtes Endgerät einsetzt, wesentlich schwerer administrieren. Die von den Nutzern mitgebrachten Geräte ersparen dem Unternehmen auch keine nennenswerten Kosten. Der Anschaffungspreis macht lediglich einen kleineren Anteil aus, die Kosten für Support und Service müssen zusätzlich berücksichtigt werden. Schwierig ist die Feststellung, welchen Anteil Service- und Wartungskosten eines mobilen Endgeräts haben. Weitere Probleme entstehen durch Haftungsfragen, z. B. bei illegaler Nutzung von Apps oder missbräuchlichem Datenzugriff.

Aufgrund der Risiken von BYOD entwickelten Unternehmen alternative Konzepte, um die produktivitätsfördernde Nutzung eigener Endgeräte mit begrenzbarem Risiko zu ermöglichen. Unter der Firmierung „choose your own device“ (CYOD) wird den Nutzern eine Wahl zwischen wenigen mobilen Endgeräten überlassen, welche im Unternehmen genutzt werden dürfen. Der IT-Bereich behält hierbei vollständig die Kontrolle über die eingesetzte Hardware und geht trotzdem auf die Wünsche der Mitarbeiter ein. Hierdurch wird eine homogene IT-Infrastruktur aufgebaut, ohne sich von vornherein auf ein einziges Gerät zu beschränken. Vor allem wird hierdurch ein hohes Maß an Sicherheit ermöglicht. Das Unternehmen übernimmt die vollständigen Kosten und da sich die Endgeräte im Eigentum des Unternehmens befinden, ist auch eine Fernlöschung (Wipe) im Falle von Verlust oder Diebstahl möglich, während bei Geräten, die sich im Privatbesitz von Mitarbeitern befinden, bei einer derartigen Fernlöschung auch private Daten verloren gehen könnten. Im Grunde existieren also ähnliche Regelungen wie beim privaten Gebrauch von Dienstwagen: Es werden unternehmenseigene mobile Geräte verwendet, wobei die private Nutzung gestattet ist und durch entsprechende Richtlinien geregelt wird.

9.5 Mobilfunk und Gesundheit

Seit Beginn der breiten Verfügbarkeit von Mobilfunk wird vor elektromagnetischer Strahlung und den damit zusammenhängenden Erkrankungen gewarnt. Gerüchte über angeblich krankmachende Mobilfunkstrahlung haben vereinzelt zur Zerstörung von Funktürmen und Sendeanlagen geführt (DNN 2019). Die Einführung der 5G-Technologie gab erneut Anlass zu Protesten, vor allem in den Sozialen Medien, und führte wiederum zu Vandalismus gegenüber technischen Anlagen (Erhardt 2020; Tremmel 2020). Vielfach beruht die Ablehnung auf mangelnder Information.

Im Zusammenhang mit den von Mobilfunkgegnern vorgebrachten Bedenken wird häufig der Begriff „Elektrosmog“ verwendet. Der darin enthaltene Begriff „Smog“ bezeichnet im allgemeinen Sprachgebrauch gesundheitsschädliche Konzentrationen von Luftschadstoffen. In Bezug auf die künstlichen elektrischen, magnetischen und elektromagnetischen Felder wird der Begriff „Smog“ verwendet, um deren allgegenwärtiges Vorkommen in der Umwelt des Menschen und die in diesem Zusammenhang befürchteten gesundheitlichen Beeinträchtigungen zu beschreiben. Obwohl die Wortwahl nicht sehr glücklich ist und eher zur allgemeinen Verunsicherung beiträgt, wird der Begriff „Elektrosmog“ vielfach in den Medien und in der öffentlichen Diskussion verwendet.

Elektromagnetische Felder in der Umwelt gehen von zahllosen natürlichen und künstlichen Quellen aus. Dazu gehören Rundfunk- und Fernsehsender, Satelliten, alle Arten von elektrischen Geräten, sowie die Strahlung der Sonne, natürliche Wärmequellen oder das Magnetfeld der Erde. Die Wechselwirkung von elektromagnetischen Feldern mit Materie ist seit Jahrzehnten wissenschaftlich geklärt. Die Art der Wechselwirkung hängt ausschließlich von der Frequenz und der Intensität der elektromagnetischen Welle ab. Bei einer Welle mit niedriger Frequenz, die auf ein Objekt trifft, wird Energie auf ganze Moleküle oder Molekülgruppen übertragen. Diese geraten in stärkere Bewegung oder Schwingung, die sich dann als Temperaturerhöhung des Objektes zeigt. Die Erwärmung ist die einzige mögliche und nachgewiesene Wirkung von Wellen niedriger Frequenz. Im Gegensatz dazu wirken Wellen hoher Frequenz auf Elektronen und Atomkerne und sind in der Lage, Elektronen aus Molekülen und Atomen zu lösen (Ionisation). In biologischen Geweben verhalten sich diese Ionen chemisch aggressiv und schädigen ihre Umgebung. Krebserkrankungen sind eine mögliche Folge der Exposition durch solche Strahlung, vor allem bei intensiver und häufiger Einwirkung. Die Grenze zwischen niedrigen und hohen Frequenzen mit Bezug auf diese Wirkung ist klar gezogen: Alle Frequenzen unterhalb der des sichtbaren Lichtes sind niedrige Frequenzen. Dazu gehören Radiofrequenzen, Mikrowellen und Wärmestrahlung. Alle elektromagnetischen Wellen mit Frequenzen vom ultravioletten Licht aufwärts sind hohe, ionisierende Frequenzen (Abb. 3.2). Bekannt ist die krebsverregende Wirkung von hohen Dosen von UV-Strahlung (Risiko von Hautkrebs), Röntgenstrahlung oder radioaktiver Gammastrahlung.

Eine Datenbank der RWTH Aachen University bietet eine Übersicht zur internationalen Forschung über die Auswirkungen elektromagnetischer Felder auf den Menschen. Sie um-

fasst heute mehr als 33.500 Veröffentlichungen, wovon mehr als 6000 die Wirkung von Mobilfunkfrequenzen untersuchen (RWTH Aachen University [2021](#)). Die Weltgesundheitsorganisation WHO verfolgt die wissenschaftlichen Untersuchungen der gesundheitlichen Auswirkungen von elektromagnetischer Strahlung und beauftragt selbst die Durchführung von Studien zu diesen Themen. Auf ihrer Internetseite führt sie aus: „A large number of studies have been performed over the last two decades to assess whether mobile phones pose a potential health risk. To date, no adverse health effects have been established as being caused by mobile phone use.“ (World Health Organization [2014](#))

Die elektromagnetische Strahlung, die im Mobilfunk genutzt wird, dringt kaum in den menschlichen Körper ein. Sie wird von der Haut und anderen oberflächlichen Geweben absorbiert, und führt nur zu vernachlässigbaren Temperatur-Erhöhungen im Körper. Durch Studien wurden die Auswirkungen auf Hirnfunktionen, Kognition, Schlaf, Herzfrequenz und Blutdruck von Probanden untersucht. Es gibt keinen konsistenten Hinweis auf problematische Auswirkungen. Auch konnte kein Hinweis auf einen kausalen Zusammenhang zwischen der gelegentlich behaupteten elektromagnetischen Hypersensitivität und Mobilfunk gefunden werden.

Ein möglicher Zusammenhang zwischen Krebserkrankungen und der Einwirkung von Mobilfunkwellen wurde in einer Reihe von groß angelegten internationalen Studien untersucht. Hier macht die WHO die Einschränkung, dass Krebserkrankungen auch noch Jahrzehnte nach der verursachenden Einwirkung auftreten könnten. Aufgrund dieser Einschränkung kommt die Klassifikation „möglichweise kreberregend“ (2B) der International Agency for Research on Cancer (IARC) zustande. Für den überblickten Untersuchungs-Zeitraum von bis zu 10 Jahren konnte die Entstehung von Gliomen, das sind bösartige Hirntumore, als Folge von Mobilfunk ausgeschlossen werden. Auch Tierversuche konnten keinen konsistenten Hinweis auf eine höhere Bildungsrate von Tumoren nach langfristiger Mobilfunk-Exposition geben. Seit 1990 gibt es national und international keine Erhöhung von Hirntumorfällen trotz massiver Nutzung von Mobilfunk und mobilen Endgeräten. Abb. [9.2](#) illustriert dies anhand der Inzidenzen von Gliomen in Deutschland im Vergleich mit der Entwicklung des Gesprächsvolumens im Mobilfunk.

Im Internet kursierende Studien mit gegenteiligen Ergebnissen zeigen oft ein unlässiges Studiendesign, eine nicht randomisierte Auswahl von Studienteilnehmern oder eine fehlerhafte statistische Analyse ([LGL 2005](#); [Toxicology 2009](#)). In Tierversuchen wird häufig eine viel zu hoch dosierte Exposition angewandt.

Da auch starke Wärme-Einwirkung durch Felder hoher Intensität unerwünschte Folgen für Organismen und Geweben haben kann, gibt es weltweit verbindliche Regelungen für die erlaubte Stärke der vom Mobilfunk genutzten elektromagnetischen Felder. Die zulässigen Grenzwerte für die Leistungsabgabe von Mobilfunkstationen orientieren sich an den Empfehlungen der internationalen Strahlenschutzkommission (ICNIRP). Diese betragen bei 900 MHz für die Leistungsdichte 37,5 dBm (Feldstärke 41 V/m), für 1800 MHz 39 dBm (Feldstärke 58 V/m) und für Frequenzen über 2000 MHz 40 dBm (Feldstärke 61 V/m). Die Messungen erfolgen nach einem standardisierten Verfahren mit definierten

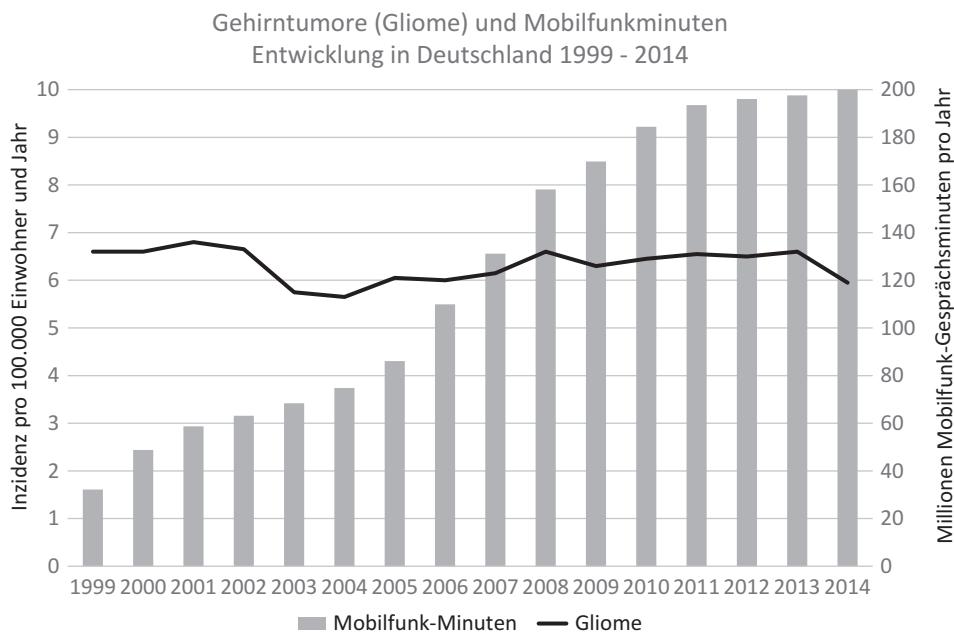


Abb. 9.2 Gliome und Mobilfunkminuten von 1999 bis 2014 (Hofer et al. 2021; Bundesnetzagentur 2011; Bundesnetzagentur 2015)

Abständen von der zu messenden Antenne (Reg TP 2003). Die leicht höheren Werte für die höheren Frequenzen sind durch die frequenzabhängige stärkere Dämpfung dieser Wellen begründet.

Die Grenzwertempfehlungen werden nicht nur von der Internationalen Strahlenschutzkommission selbst, sondern auch durch zahlreiche nationale und internationale Expertengremien wie die Deutsche Strahlenschutzkommission (SSK), das europäische Scientific Committee on Emerging and Newly Identified Health Risks (SCENIHR) und die WHO regelmäßig überprüft. Die einwirkende Leistung der Mobilfunkwellen liegt bei einem Abstand des Nutzers von 10 m von der Antenne bereits bei Milliwatt-Bereich, wie in Kap. 3 beschrieben. Bei realem Nutzungsverhalten wird die empfangene Leistung -50 dBm, also 1/100.000 eines Milliwatts, nicht überschritten.

Die Nutzung eines Mobiltelefons (100 mW) für 10 Minuten resultiert in einer viel höheren Strahlendosis im Vergleich zu einer Exposition mit -50 dBm über 24 Stunden. Die Einwirkung von Mobilfunkwellen auf den Körper des Mobilfunkteilnehmers geht also praktisch ausschließlich vom selbst genutzten mobilen Endgerät aus. Bei am Körper gehaltenen Geräten ist es unvermeidlich, dass ein Teil der abgestrahlten Leistung vom Körper aufgenommen wird. Entsprechend gibt es regulatorische Beschränkungen, deren Einhaltung von den Herstellern bei der Zulassung des Gerätes gegenüber der nationalen Zulassungsbehörde nachgewiesen werden muss. Neben der maximalen Leistungsabgabe

von 200 mW ist die Spezifische Absorptionsrate (SAR) zu messen und zu dokumentieren. Das SAR-Verfahren modelliert die Situation eines am Kopf gehaltenen Mobiltelefons mittels einer Nachbildung des menschlichen Schädels gefüllt mit einer dem Körpergewebe vergleichbaren Gelatine sowie zahlreichen Messpunkten im Inneren. Das Modell wird als Specific Anthropomorphic Mannequin (SAM) bezeichnet. Gemessen wird mit der höchsten zulässigen Sendeleistung (200 mW), wobei die tatsächlichen Sendeleistungen abhängig von den Sende- und Empfangsbedingungen und in der Regel um Größenordnungen geringer sind.

Die SAR-Grenzwerte sind mit 2 Watt/kg (bzw. 1,5 Watt/kg in den USA) festgelegt. Da mobile Endgeräte heutzutage für den Weltmarkt entwickelt werden, sind auch in Europa keine Geräte mit einem SAR-Wert von über 1,5 Watt/kg erhältlich. Im Gegenteil erreichen heute 40 % aller mobilen Endgeräte einen SAR von unter 0,5 Watt/kg (Bundesamt für Strahlenschutz 2021). Eine Strahlungsleistung von 1 Watt/kg während einer Stunde bewirkt einen lokalen Temperaturanstieg im isolierten bestrahlten Gewebe von weniger als 1 Grad Celsius. Durch die Ausbreitung der Wärme in das umgebende Gewebe ergeben sich nochmals deutlich geringere Werte.

9.6 Fragen

1. Erläutern Sie die wichtigsten Schutzziele bei IT-Systemen.
2. Welche Angriffsmöglichkeiten gibt es bei Mobilfunk und mobilen Endgeräten?
3. Welche Schutzmaßnahmen existieren für die Sicherheit im Mobilfunk?
4. Warum ist die Nutzung von IMSI Catchern nur bestimmten Personengruppen vorbehalten?
5. Warum werden im Unternehmen Mobile Device Management Systeme eingesetzt?
6. Häufig wünschen Mitarbeiter im Unternehmen die Nutzung ihrer privaten mobilen Endgeräte für geschäftliche Zwecke. Vergleichen Sie die Konzepte „bring your own device“ und „choose your own device“. Berücksichtigen Sie hierbei die Kriterien „Kostensparnis“, „Komfort“/Bequemlichkeit und „Kontrolle/Sicherheit“.
7. Nehmen Sie Stellung zu der These „Mobiles Arbeiten bedeutet eine Gefahr für die Work-Life-Balance“.
8. Können im Mobilfunk genutzte elektromagnetische Wellen Strahlenschäden (also Ionisation von Gewebemolekülen) hervorrufen?
9. Welche Grenzwerte für die Leistungsabgabe von Mobilfunkgeräten kennen Sie?
10. Was ist der SAR-Wert und wie wird er gemessen?

Literatur

- Bundesamt für Strahlenschutz (2021) Blauer Engel: so viele Mobiltelefone könnten damit ausgezeichnet werden. <https://www.bfs.de/DE/themen/emf/kompetenzzentrum/mobilfunk/schutz/blauer-engel.html>. Zugegriffen am 27.08.2021
- Bundesnetzagentur (2011) < i>Tätigkeitsbericht 2010/2011 Telekommunikation. https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Allgemeines/Bundesnetzagentur/Publikationen/Berichte/2011/TaetigkeitsberichtTK20102011pdf.pdf?__blob=publicationFile&v=2. Zugegriffen am 11.05.2022
- Bundesnetzagentur. (2015) Tätigkeitsbericht Telekommunikation 2014/2015. https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Allgemeines/Bundesnetzagentur/Publikationen/Berichte/2015/TB_TK_2015.pdf?__blob=publicationFile&v=3. Zugegriffen am 11.05.2022
- DNN (2019) Brennender Mobilfunkmast in Trachau – Polizei geht von Brandstiftung aus. Dresdner Neueste Nachrichten, 25. Februar 2019.
- Engel T (2014) Locate. Track. Manipulate. 31C3: a new dawn. Chaos Computer Club. https://media.ccc.de/v/31c3_-_6249_-_en_-_saal_1_-_201412271715_-_ss7_locate_track_manipulate_-_to-bias_engel. Zugegriffen am 27.08.2021
- Erhardt C (2020) Corona: Falschmeldungen über 5G Masten verbreiten sich weltweit. Kommunal. Berlin. <https://kommunal.de/corona-funkmaste>. Zugegriffen am 27.08.2021
- Hofer S, Bullinger L, Dierlamm J, Grosu A-L, Hau P, Hense J, Hoffmann J, Proescholdt M, Pflugshaupt T, Preusser M, Pukrop T, Rushing EJ Wörmann B (2021) Gliome im Erwachsenenalter. Berlin. <https://www.onkopedia.com/de/onkopedia/guidelines/gliome-im-erwachsenenalter/@@guideline/html/index.html>. Zugegriffen am 27.08.2021
- LGL (2005) Mobilfunk: Ein Gesundheitsrisiko? Studien – kontrovers diskutiert. Erlangen. <https://repository.publisso.de/resource/frl:3247777-1/data>. Zugegriffen am 27.08.2021
- Reg TP (2003) Messvorschrift für bundesweite EMVU-Messreihen der vorhandenen Umgebungsfeldstärken (Reg TP MV 09/EMF/3). Bonn. https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Telekommunikation/Verbraucher/ElektromagnetischeFelder/EMF-Messreihen/messvorschrift-emf-messreihe.pdf?__blob=publicationFile&v=4. Zugegriffen am 27.08.2021
- RWTH Aachen University (2021) EMF Portal. RWTH Aachen University. Aachen. <https://www.emf-portal.org/de>. Zugegriffen am 27.08.2021
- Toxicology (2009) RETRACTED: evaluation of basal DNA damage and oxidative stress in Wistar rat leukocytes after exposure to microwave radiation. Toxicology 259(3). <https://doi.org/10.1016/j.tox.2009.02.008>
- Tremmel M (2020) Mobilfunkmasten wegen Corona-Verschwörungstheorie angezündet. Golem. Berlin. <https://www.golem.de/news/grossbritannien-mobilfunkmasten-wegen-corona-verschwoerungstheorie-angezuedet-2004-147720.html>. Zugegriffen am 27.08.2021
- World Health Organization (2014) Electromagnetic fields and public health: mobile phones. Geneva. <https://www.who.int/news-room/fact-sheets/detail/electromagnetic-fields-and-public-health-mobile-phones>. Zugegriffen am 27.08.2021