Drahtlose Kommunikation

https://iuk.one/1010-1017

Clemens H. **Cap**
ORCID: 0000-0003-3958-6136

Department of Computer Science
University of **Rostock**
Rostock, Germany
clemens.cap@uni-rostock.de

3. 1. 2021 Vers. 3

Ziel

Drahtlose Kommunikation löst die Probleme

- der Verkabelung
- der Erreichbarkeit außer Haus
- der mobilen Erreichbarkeit

Wir sehen und die physikalischen Grundlagen an.

Wir erarbeiten weitere Konzepte anhand konkreter Systeme.

1. Elektromagnetische Wellen

1.1. Erzeugung

1.2. Ausbreitung

Ziele: Wie erzeugen wir elektromagnetische Wellen? Wie kommen diese vom Sender zum Empfänger?

Antenne

Antennen: Zur Erzeugung oder Aufnahme elektromagnetischer Wellen.

Isotrope Antenne: Modellvorstellung einer idealisierten Antenne.
Abgestrahlte Leistung ist in jede Raumrichtung gleich.

Reale Antenne: Hat meist Vorzugsrichtung in bestimmte Raumrichtungen.

Antennendiagramm: Vergleich realer Antenne mit isotroper Antenne.
Für jede Raumrichtung: Angabe des Faktors in der Leistungsdichte in [dB].

Auswahl der Antenne: Je nach spezifischer Anforderung der Anwendung.

1. **Große Region** soll bestrichen werden. Bsp: Sat-TV.
2. **Punkt-zu-Punkt** Verbindung soll aufgebaut werden. Bsp: Richtfunk.
3. **Zelle** zur optimierten Versorgung kleiner Bereich. Bsp: 4G, 5G.

Schematisches Antennendiagramm

Vorzugsrichtung: Richtung mit maximaler Strahlungsdichte.

Hauptkeule: Vorzugsrichtung plus Winkelbereich, innerhalb dessen maximale Leistung auf die Hälfte abfällt.

Beachte: $\log_{10}(2) = 0.301$.
Daher: Halbe Leistung $= -3$ [dB]

Nebenkeule: Zweites lokales Maximum.

Vor- Rückverhältnis: Dämpfung in Gegenrichtung der Hauptkeule.

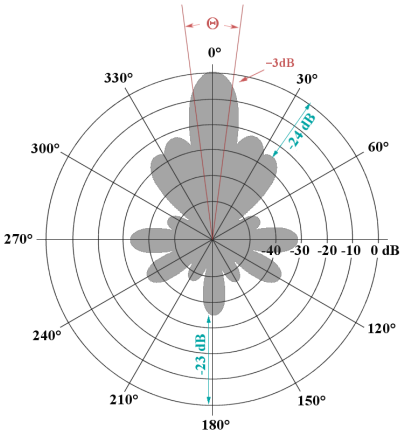

Abb. 1: Schematisches Antennendiagramm. Die -3 [dB] bestimmen den Öffnungswinkel der Hauptkeule.

Reales Antennendiagramm

Reale Antennendiagramme sehen aufgrund von Meßfehlern, Resonanzen und Rauschen meist deutlich zerklüfteter aus als die schematischen Antennendiagramme.

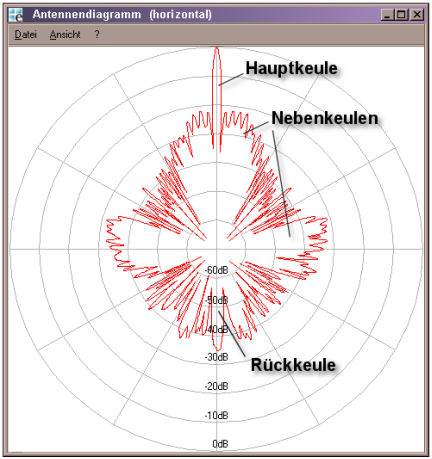

Abb. 2: Reales Antennendiagramm © Rechte siehe Anhang.

Parabol-Antenne

Brennpunkt-Eigenschaft der Parabel:

Alle Strahlen, die parallel zur Achse Scheitel S – Brennpunkt F verlaufen, werden in den Brennpunkt F reflektiert.

Der **Brennpunkt**

- sammelt einfallende parallele Strahlen.
- sendet erzeugte Strahlen parallel aus.

Parabolantennen eignen sich gut für **Punkt-zu-Punkt Verbindungen**. Alle Strahlen in eine Richtung werden an einem Punkt konzentriert; dort positioniert man Empfangs- oder Sende-Element.

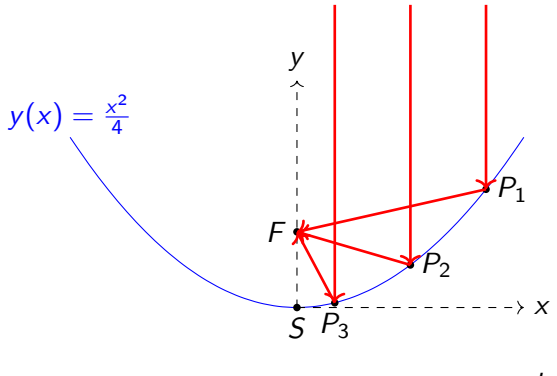

Abb. 3: Eine **Parabel** ist die Menge aller Punkte, die von einer Geraden l (**L**eitgerade) und einem Punkt F (Brennpunkt, **F**okuspunkt) gleich weit entfernt sind. Legt man in den Scheitel S ein Koordinatensystem, so hat die Parabel eine besonders einfache Darstellung.

Parabolantenne

Abb. 4: Parabolantenne im 2.4 [GHz] Band. Ausführung des Reflektors als Metallgitter.

Abb. 5: Parabolantenne auf dem Jungfraujoch im Einsatz für eine Bündelfunkstrecke.

Ausbreitungseffekte

Brechung (refraction): Trifft eine Welle von einem Medium auf ein *elektromagnetisch anderes* Medium, so kann die Welle um einen Brechnungswinkel abgelenkt werden.

Reflexion und Totalreflexion: Trifft eine Welle von einem Medium auf ein *elektromagnetisch anderes* Medium, so kann die Welle teilweise oder total reflektiert werden.

Beugung (diffraction): Trifft eine Welle auf eine *Kante* zwischen elektromagnetisch verschiedenen Medien, so kann die Welle in ihrer Ausbreitungsrichtung abgelenkt werden.

Absorption: Beim *Durchtritt* durch ein Medium wird die Welle abgeschwächt.

Streuung (scattering): Trifft eine Welle auf im Vergleich zur Wellenlänge *kleine Partikel*, so kann die Welle abgelenkt werden.

Freiraumdämpfung: Während der *Ausbreitung* verteilt sich die abgestrahlte Energie auf eine immer größere Kugelfläche um die Sendeantenne. Das erzeugt den Eindruck einer Dämpfung.

Zwei wichtige Modelle der Ausbreitung

Strahlenoptik: Beschreibung als punktuelle Störung (Teilchen).
Die Ausbreitung erfolgt eindimensional, gradlinig mit materialabhängiger Krümmung.
Mathematische Beschreibung: Fermatsches Prinzip des kürzesten Lichtwegs.
Näherungsmodell, das (erst) bei hohen Frequenzen gut zutrifft ("Optik").
Kann **Brechung**, **Reflexion** und **Totalreflexion** erklären.

Wellenoptik: Beschreibung als transversale, vektorielle Welle.
Die Ausbreitung erfolgt als räumliche Welle im elektro-magnetischen Feld.
Mathematische Beschreibung: Maxwell-Gleichungen.
Präzises Modell, das bei niedrigen Frequenzen notwendig wird.
Erforderlich zur Beschreibung von **Beugung**, **Absorption**, **Streuung** sowie der Wellen-Phänomene **Polarisation** und **Interferenz**.

Folgen der Ausbreitungseffekte

Mehrwege-Ausbreitung: Eine Welle kann sich von einem Raumpunkt zum anderen über mehrere Wege (gebrochen, gebeugt, reflektiert usw.) ausbreiten.

Überlagerung: Eine Welle kann mit anderen Wellen oder mit Mehrwege-Anteilen von sich selber überlagert werden. Ungünstige Phasenlage kann destruktive Interferenz und Selbstauslöschung bewirken.

Schwund (Fading): Veränderungen von Position (Bewegung) oder von äußeren Ausbreitungsbedingungen (Wetter) können dadurch die Empfangsfeldstärke verändern.

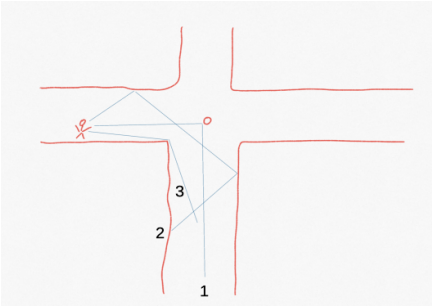

Abb. 6: Das Handy eines Fußgängers ist von Mehrwegeausbreitung betroffen. Der Strahlengang (1) wird an einer Verkehrsampel gestreut. Der Strahlengang (2) wird mehrfach reflektiert. Der Strahlengang (3) wird an einer Gebäudekante gebrochen. Während des Weitergehens verändern sich laufend die mit der spezifischen Geometrie verbundenen Bedingungen (Fading).

MIMO: Multiple Input – Multiple Output

Idee 1: Bei Nutzung mehrerer Antennen können ortsabhängige Aspekte teilweise kompensiert werden (sog. räumliche Diversität).

Bsp: *Eine Antenne* ist in Position destruktiver Interferenz, *die andere* Antenne nicht.

Idee 2: *Mehrere* Antennen können auch *mehr* Energie senden oder empfangen.

Name: MIMO: **M**ultiple **I**nput – **M**ultiple **O**utput, denn:
Funkkanal als Input-Output System betrachtet.
Input ist der Sender, Output ist der Empfänger.

MIMO Systeme

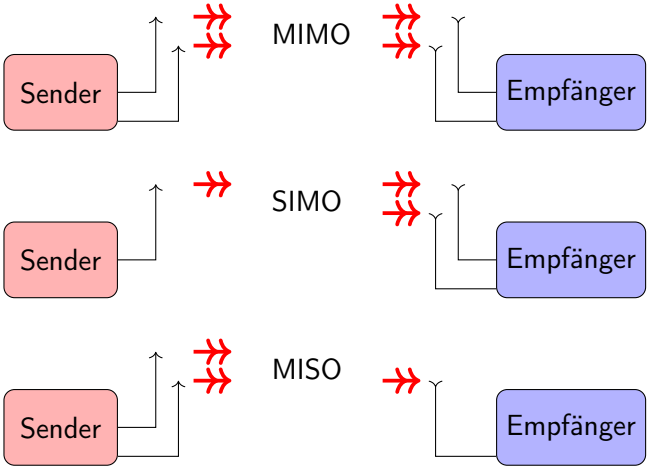

Abb. 7: Klassifikation von MIMO Systemen. Eine **3x2** Verbindung bedeutet, daß Sender-seitig 3 und Empfänger-seitig 2 Antennen zum Einsatz kommen.

Abb. 8: Wifi-Router von Asus für Gamer, mit 8 Antennen. Der Wifi-Standard **802.11n** hat MIMO für Wlan normiert.

2. Aufprägung von Information

Die entsprechenden Modulationsverfahren haben wir bereits in einem anderen Abschnitt behandelt.

3. Systeme und Standards

3.1. Bluetooth

3.2. WLAN: Wireless Local Area Network

3.3. Sonstige

Ziele: Es gibt sehr viele verschiedene Standards mit jeweils stark anwendungs-spezifischen Eigenschaften.

Wir lernen anhand der Beispiel-Systeme weitere Konzepte kennen.

Bluetooth

Ziel: Kabelersatz im Bereich der Personal Area Networks, vornehmlich bei mobilen Kleingeräten mit Akku-Betrieb.

Typische Eckwerte

Frequenz	2.4 [GHz]	FHSS mit 79 Kanälen zu je 1 [MHz]
		FHSS mit 40 Kanälen zu je 2 [MHz] (in BLE)
Entfernung	10 – 100[m]	3 Leistungsklassen
Sendeleistung	1 – 100 [mW]	3 Leistungsklassen
Datenrate	1, 2, 24 [Mbit/s]	

FHSS: Frequency Hopping Spread Spectrum

Problem: Wie Trägerfrequenz mit Partner abstimmen? Gewählte vielleicht gestört?

Konzept: Übertragung springt zwischen mehreren Trägerfrequenzen.
Pseudo-Zufallszahlengenerator legt Frequenzfolge fest.
Identischer Initialwert garantiert paralleles Springen von Sender und Empfänger.

Langsames FHSS: Frequenz wechselt langsamer als die Bits.
Auf jeder Frequenz werden mehrere Bits gesendet.

Schnelles FHSS: Frequenz wechselt schneller als die Bits.
Jedes Bit wird auf mehreren Frequenzen gesandt.

Bewertung:

1. **Störsicherheit:** Wenn eine Frequenz belegt oder gestört wird andere frei sein.
2. **Abhörsicherheit:** Partner wechseln laufend Frequenz, auf der sie kommunizieren.
3. **Komplexität:** Partner müssen sich "finden" & Frequenzwechsel abstimmen.

Beispiel Bluetooth: 79 Kanäle, pro Sekunde bis zu 1'600 Frequenzwechsel.

Stromverbrauch

Problem: Stromverbrauch reduziert Akku-Nutzzeit mobiler Geräte.

Idee: Absenken des Duty-Cycle: Immer mal wieder (kurz) abschalten.

Trade-Off: Tausche Stromeinsparung gegen (geringfügig) höhere Latenzzeit.

Beispiel Bluetooth:

- **Bsp:** Hold Modus: Gerät hört für 200 [ms] nicht mehr zu.
- **Bsp:** Sniff Modus: Gerät hört nur mehr alle 500[ms] für einige Pakete zu.
- **Bsp:** BLE: **B**luetooth **L**ow **E**nergy Protokoll-Variante.
  Viele Änderungen, ganz deutlich geringerer Stromverbrauch.

Profile

Problem: Welches Gerät nimmt wann, wie mit Partner Kontakt auf?
Wer darf Verbindung initiieren? Welche Datenrate? Unidirektional oder bidirektional?

Spezialität bei Bluetooth mit rund 50 Profilen.

Bsp: Bluetooth HSP: **H**ead**s**et **P**rofile.
- Kommunikation aktiviert durch Handy oder Headset-Button.
- Bidirektionaler Audiokanal, Datenkanal für Lautstärke und Hang-Up.

Bsp: Bluetooth HRP **H**eart **R**ate **P**rofile.
- Kommunikation aktiviert durch Heart Rate Sensor.
- Unidirektionaler Datenkanal sehr geringer Datenrate.

Pairing und Bonding

Problem: Geräte sollen sich nach Entfernung automatisch wieder-erkennen.
Bsp: Handy und Bluetooth-Freisprechanlage im Auto.
Bsp: Handy und Wifi Access-Point.

Erst Pairing: Initiales Vertrauen zwischen Geräten herstellen.
Dann Bonding: Schlüsselaustausch für Persistenz dieses Vertrauens.

Anwendungsspezifisch, je nach Ausstattung der Endgeräte:

- **Statische PIN** (0000, 1234) eingeben. Unsicher & gefährlich.
- **Identische PIN** auf beiden Geräten eingeben.
- **Anzeige der PIN** auf beiden Geräten, Benutzer bestätigen Gleichheit.
- **PSK Preshared Key** auf beiden Geräten eingeben.
- **Schütteln** beider Geräte, wird durch Sensor detektiert.
- **Nahkommunikation** Nähe herstellen für Schlüsselaustausch.

Netz-Architekturen

Problem: Mehr als 2 Geräte sollen kommunizieren.

Bei Bluetooth: Piconet, Scatternet.

Piconet: Bluetooth-Netzwerk aus bis zu 255 Teilnehmern.
Master-Slave Architektur: Master vergibt Zeitschlitze, in denen Slaves senden dürfen.
Maximal 8 Teilnehmer aktiv, der Rest ist standby.

Scatternet: Verbund von bis zu 10 Bluetooth Piconetzen.

Bei Wifi: SSID, BSSID

WLAN: Wireless Local Area Network

Ziel: Kabelersatz im lokalen Netzwerk (LAN)
auf voreingestellten oder automagisch zugewiesenen Kanälen.

Typische Eckwerte

Frequenz	2.4 [GHz], 5 [GHz]; 60 [GHz]	Viele nationale Varianten
Entfernung	50–100 [m]	In Spezialsituationen deutlich mehr
Sendeleistung	100 [mW] = 20 [dBm]	
Datenrate	1–9'609 [Mbit/s]	Verschiedene Standards

Anmerkungen

Sendeleistung:
100 [mW] $= 10 \cdot \log_{10}(100)$ [dezibel (zu) Milliwatt] $= 20$ [dBm].
In den USA: Bis 1 [W] zulässig.

Entfernung: Bis 20 [km] und mehr möglich bei:

- Höherer Sendeleistung (1 [W] und mehr).
- Spezielle Antennen, zB: Parabolantenne.
- Antennenbereich frei von Wasser, Metall und Störungen.
- Freie Sicht auf Antennenverbindung, LoS line-of-sight ist frei.

Kanal-Auslastung und Wechsel

Problem: Ein Funkkanal geht schlecht (gestört, überlastet).

Roaming: Wechsel eines Knotens im selben Netz (SSID) zu einem anderen Access Point (BSSID).

SSID: Service Set ID; menschlich vergeben, lesbarer Netz-Name. Identifiziert ein Wifi-Netzwerk als Ganzes.

BSSID: Basic Service Set ID; Id eines Access Points, oft MAC-Adresse.

Steering: Knoten bei Bedarf auf anderen Kanal verschieben.

TPC: Transmission Power Control.
Reduktion der Sendeleistung, wenn andere Teilnehmer auf dem Kanal.

DFS: Dynamic Frequency Selection.
Wechsel auf anderen Kanal, wenn priorisierte Teilnehmer senden.
Bsp: Wetterradar auf der Frequenz aktiv.

Sicherheits-Risiken für das eigene WLAN

Angriffsoberfläche: Angriffe drahtlos möglich.

Nutzung der Verbindung durch Dritte für illegale Zwecke.

Zugang des Angreifers zum eigenen internen Netz.

Implementierungsfehler in den Sicherheitsmechanismen WEP, WPA, WPA2 und WPS.

Sicherheitshinweise (1)

Verschlüsselung: Sichere Variante nutzen (WPA3; ggf. WPA2)

Netzwerkname: Default durch wenig-sagenden Netzwerknamen ersetzen.
Sonst: Angreifer erfährt: Nutzungszweck, Gerätestandort, Software-Schwachstellen uva.

Paßwörter: Defaults durch zufällige, lange (BSI: > 20) Paßwörter ersetzen.

Privilegien-Trennung: Verschiedenen Funktionen verschiedene Paßwörter geben.

Deaktivieren unsicherer Funktionen:
Fernzugriff & Fernkonfiguration (sog. TR-069) wenn nicht benötigt, WPS (**W**ifi **P**rotected **S**etup), UPnP Universal Plug and Play Firewall Konfiguration, DHCP (verteilt Meta-Information an jedes Gerät).

Abschalten, wenn nicht benötigt (Zeitautomatik nutzen).

Sendeleistung nur so hoch wie nötig, reduziert überflüssige Reichweite.

Aktualisieren von Firmware und Einstellungen (WPA2 -> WPA3).

Segmentierung des Netzwerks nach Funktionsbereichen (Bsp: Gast-Zugang)

Sicherheitshinweise (2)

MAC-Filter: Nur Geräte mit bekannter MAC-Adresse zulassen.

- Nicht in jeder Betriebsart sinnvoll (Bsp: Hotel-WLAN).
- Bringt nur wenig: Angreifer kann MAC-Adressen ermitteln und darauf umstellen.

Feste IP zuordnen: User und Geräten (MAC) feste IP zuordnen, danach filtern.

Hidden SSID: Einstellung so, daß AP den Netznamen nicht ausstrahlt.

- Bringt nichts, da leicht durch Angreifer zu ermitteln.
- Schlecht, da Client dann laufend Broadcast Pakete versendet mit dieser SSID

802.1x: Zusätzlichen Authentisierung-Server (Radius-Server).

Sicherheits-Risiken durch fremdes WLAN

Unverschlüsselte Verbindung: Erlaubt Abhören.

DNS Spoofing:

- Oft wird bei Wifi DHCP genutzt.
- DHCP sagt dem Client, welche Maschine als DNS Server zu nutzen ist.
- DNS Server sagt dem Client dann gefälschte IP-Adresse für einen Rechnernamen.
- Dieser andere Rechner sendet nun Schadcode.

Privatheit:

- Auch bei verschlüsseltem WLAN sieht DNS Server die Zugriffe.

Evil Twin: Gefälschter unverschlüsselter WLAN Access Point.

- Gesamter Datenverkehr fällt in die Hände des Angreifers.

Sicherheits-Hinweise bei Nutzung eines fremden WLAN

Generell:

- Davon ausgehen, daß der *gesamte Datenverkehr* abhörbar ist.
- Allen Systemdiensten des fremden WLAN mißtrauen. (Bsp: DHCP, DNS).

Konkret:

- **VPN: V**irtual **P**rivate **N**etwork über eigene oder vertrauenswürdige Server.
  Stellt grundsätzliche Verschlüsselung aller Verbindung her.
- **Konfiguration** des Endgeräts anpassen.
  Bsp: DNS Server manuell einstellen. (Cloudflare: 1.1.1.1, Google: 8.8.8.8)
  Bsp: Freigabe von Datenträgern, Diensten und Ports einschränken.
  Bsp: Firewall aktivieren (incoming und outgoing).
- **Verschlüsselung:** Anwendungsdienste nur verschlüsselt nutzen: Web, Email

Verschlüsselung

WEP Wired Equivalent Privacy

- 2001 gebrochen; Schlüssel zu geringer Länge; **völlig kaputt**.

WPA Wifi Protected Access

- Seit 2008 Schwachstellen bekannt.

WPA2 Wifi Protected Access.

- Nutzt AES; zwei Varianten der Schlüsselnutzung implementiert.
- Variante TKIP gilt als unsicher.
- Variante CCMP gilt als sicher.

WPA3 Wifi Protected Access

- 2018 standardisiert, seit 2020 für neue Wifi Geräte erforderlich.

Wifi Ortung

Problem: Mobilgerät will sich orten, hat aber kein GPS.

Lösung: Alle SSID im Umfeld eruieren. Namen in DB abfragen.

Bsp: wigle.net: Kennt 710 [M] Wifi Knoten und 379 [M] Bluetooth Knoten.

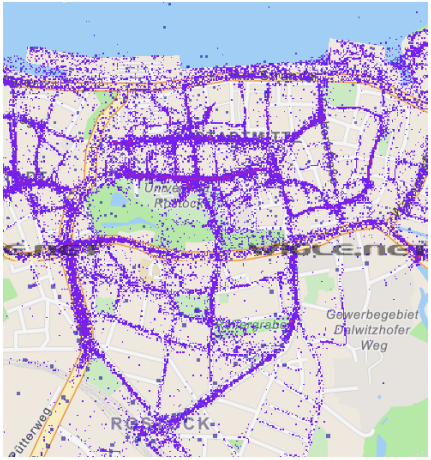

Abb. 9: Karte von Rostocker der Datenbank Wigle. Jeder Punkt ist ein Funkknoten mit bekannter Adresse.

Ortsbezogene Privatheit

Problem: Ort soll privat bleiben obwohl Mobilgerät ein Ortungsbeacon ist.

Bsp: Mobilgerät hat feste Adresse (MAC), die es bei jeder Umgebung aussendet.

Bsp: Wifi-Geräte senden regelmäßig Kontaktversuche zu den hidden SSIDs, die ihnen bekannt sind.

Lösungen:

- **Wifi:** Private MACs, zu jedem Knoten anders.
- **Bluetooth:** Zufallsadressen
- **3G, 4G, 5G:** Nur Abschirmfolie.

Abb. 10: Kupferfolie zur Abschirmung jeglicher Aussendung. ("Aluhut" für das Handy.)

Wichtige Wifi Standards

Standard	Name	[GHz]	[Mbit/s]	Technologie
802.11b		2.4	1–11	Der Start
802.11a		5	6–54	OFDM Modulation; Höhere Frequenz & Datenrate
802.11g		2.4	6–54	OFDM Modulation; Höhere Datenrate bei 2.4 [GHz]
802.11n	Wifi 4	2.4, 5	72–600	MIMO Antennen
802.11ac	**Wifi 5**	5	433-6'933	MIMO, Kanalbreite, Modulation
802.11ax	**Wifi 6**	2.4, 5	600–9'608	Viele Verbesserungen

Tab. 1: Die wichtigsten Standards und Leistungsklassen für Wifi im Vergleich.

NFC: Near-Field Communication

Ziel: Kontaktloser Datenaustausch im Nahbereich.

Passive Knoten können nur antworten, aktive auch anfragen.

Nahbereich: Entfernung bis 10 [cm].
Herstellung der Entfernung als Zustimmung der Besitzer zu Transaktion gewertet.

Problem 1: Mit besonderen Antennen und Verstärkern auch bis 1 [m].

Problem 2: Passive Tags können unerwünscht ausgelesen werden.
Bsp: Kreditkarte bei Drängelei im Bus durch Handy des Nachbarn.

Typische Eckwerte

Frequenz	13.56 [MHz]
Entfernung	10 [cm]
Datenrate	106 – 424 [kbit/s]
Anwendungen	Mobiles Bezahlen, Objekt-Tagging, Logistik, ÖPNV, Ausweise

IrDA: Infrared Data Association

Ziel: Ursprünglich Fernbedienung, dann Weiterentwicklung.

Optische Übertragung erfordert Sichtverbindung (LoS **L**ine **o**f **S**ight)

- Einfache Unterbrechung des Strahls durch Plastik-Klappe.
- Viel sicherer als typische Funkverbindung.
- Verbindungsaufnahme viel fragiler.

Typische Eckwerte:

Frequenz	850–900 [nm]	Licht im Infrarot-Bereich
Entfernung	0.2 - 2.0 [m]	
Sendeleistung		
Datenrate	115 [kbit/s], 4 [Mbit/s], 1 [Gbit/s]	Je nach Modulation
Anwendungen	Fernbedienung; Foto-Cameras, Settop-Boxen	

Der ganze Rest

Lorawan:	Long range low power Verbindung bis 10 [km].
Z-Wave:	Home Automation bis 100 [m].
Zigbee:	Home Automation bis 100 [m].
Enocean:	Home Automation bis 100 [m]. Geht ohne Batterie – Strom aus der Schalter-Betätigung.
Lifi:	Übertragung über das Licht im Raum, bis 200 [Gbit/s]. Kostengünstiger als Wifi und auf den Raum beschränkt.
DECT:	Schnurlos-Telefone und Home Automation im 2.4 [GHz] Band.
QR, Bar:	Streng genommen auch eine optische Nahkommunikation.

Mobilfunk: 3G 4G 5G 6G

Eigentlich "nur" als bestehender, mobiler Dienst nutzbar.

Wenig Konfiguration durch den Anwender.

3G: Abschaltung in 2020.

4G: Seit 2009, bis 500 [Mbit/s].

5G: Heute. 50 [Mbit/s] – 1.8 [Gbit/s].

6G: Ab 2030, bis 95 [Gbit/s].

Anhang

Übersicht

Literaturverzeichnis

Verzeichnis aller Abbildungen

Verzeichnis aller Tabellen

Rechtsnachweise

Abb. 1 Quelle: https://www.radartutorial.eu/06.antennas/pic/ks3.print.png, Christian Wolff, radartutorial.eu. Nutzung nach CC BY-SA 3.0 http://creativecommons.org/licenses/by-sa/3.0/.

Abb. 2 Quelle: https://commons.wikimedia.org/wiki/File:Uplink3.png, Averse, Nutzung nach CC BY-SA 3.0 http://creativecommons.org/licenses/by-sa/3.0/.

Abb. 4 Quelle: https://commons.wikimedia.org/wiki/File:Screen_dish_antenna.jpg, Jim Jaworski, derivative work: Chetvorno. Nutzung nach CC0.

Abb. 5 Quelle: https://commons.wikimedia.org/wiki/File:Com_C26-010-096-001-003.jpg, Patrick Lüthy, CC BY-SA 4.0 https://creativecommons.org/licenses/by-sa/4.0

Rechtliche Hinweise

Die hier angebotenen Inhalte unterliegen deutschem Urheberrecht. Inhalte Dritter werden unter Nennung der Rechtsgrundlage ihrer Nutzung und der geltenden Lizenzbestimmungen hier angeführt. Auf das Literaturverzeichnis wird verwiesen. Das Zitatrecht in dem für wissenschaftliche Werke üblichen Ausmaß wird beansprucht. Wenn Sie eine Urheberrechtsverletzung erkennen, so bitten wir um Hinweis an den auf der Titelseite genannten Autor und werden entsprechende Inhalte sofort entfernen oder fehlende Rechtsnennungen nachholen. Bei Produkt- und Firmennamen können Markenrechte Dritter bestehen. Verweise und Verlinkungen wurden zum Zeitpunkt des Setzens der Verweise überprüft; sie dienen der Information des Lesers. Der Autor macht sich die Inhalte, auch in der Form, wie sie zum Zeitpunkt des Setzens des Verweises vorlagen, nicht zu eigen und kann diese nicht laufend auf Veränderungen überprüfen.

Die Bereitstellung der Inhalte erfolgt hier zur persönlichen Information des Lesers. Eine Haftung für mittelbare oder unmittelbare Schäden wird im maximal rechtlich zulässigen Ausmaß ausgeschlossen, mit Ausnahme von Vorsatz und grober Fahrlässigkeit. Eine Garantie für den Fortbestand dieses Informationsangebots wird nicht gegeben.

Die Anfertigung einer persönlichen Sicherungskopie für die private, nicht gewerbliche und nicht öffentliche Nutzung ist zulässig, sofern sie nicht von einer offensichtlich rechtswidrig hergestellten oder zugänglich gemachten Vorlage stammt.

Zitierweise dieses Dokuments

Wenn Sie Inhalte aus diesem Werk nutzen oder darauf verweisen wollen,
zitieren Sie es bitte wie folgt:

Clemens H. Cap: Drahtlose Kommunikation. Electronic document. https://iuk.one/1010-1017
3. 1. 2021.

Bibtex Information: https://iuk.one/1010-1017.bib

```
@misc{doc:1010-1017,
    author        = {Clemens H. Cap},
    title         = {Drahtlose Kommunikation},
    year          = {2021},
    month         = {1},
    howpublished  = {Electronic document},
    url           = {https://iuk.one/1010-1017}
}
```

Typographic Information:
Typeset on January 3, 2021
This is pdfTeX, Version 3.14159265-2.6-1.40.21 (TeX Live 2020) kpathsea version 6.3.2
This is pgf in version 3.1.5b
This is preamble-slides.tex myFormat©C.H.Cap

Verzeichnis aller Folien

Legende:
Fortsetzungsseite
Seite ohne Überschrift
Bildseite