SYP(SEP) - Referat: WLAN & Bluetooth

WLAN (Wireless Local Area Network)

Was ist ein WLAN?

Das Wireless Local Area Network, kurz WLAN ist ein lokales Funknetz und gehört zur Familie der IEEE-Standards. Die offizielle Bezeichnung des Wireless Local Area Network ist somit **IEEE 802.11** Zur Erklärung: IEEE 802.11 ist eine IEEE-Norm für die Kommunikation in Funknetzwerken, welche vom Institute of Electrical and Electronics Engineers kurz IEEE in erster Version 1997 verabschiedet wurde.

Was bedeutet IEEE?

Das Institute of Electrical and Electronics Engineers ist ein weltweiter Berufsverband von Ingenieuren aus den Bereichen Elektrotechnik und Informationstechnik mit Sitz in New York City. Es wurde offiziell „zur Förderung technologischer Innovationen zum Nutzen der Menschheit“ am 1. Jänner 1963 gegründet und zählt mittlerweile weit über 430.000 Mitglieder. Es operiert in über 160 Ländern und ist damit der größte technische Berufsverband der Welt. Zu den vielen verabschiedeten Standards gehören u.a. die

- Gleitkomma-Arithmetik-Spezifikation (IEEE 754)
- LAN (IEEE 802), Ethernet (IEEE 802.3)
- Bluetooth (IEEE 802.15)
- Standard for Software Configuration Management Plans (IEEE 828)
- Standard for Software and System Test Documentation (IEEE 829) und
- Software Requirements Specification (IEEE 830)

Übertragungstechnik

Die Übertragung von Daten findet über elektromagnetische Wellen auf unterschiedlichen Frequenzen zwischen einem Sender und Empfänger statt.
WLANs sind eine angepasste Form der OSI Schicht I und II und verwenden heute meist das Modulationsverfahren OFDM (Orthogonal Frequency-Division Multiplexing).
Das ODFM ist eine spezielle Implementierung der Multicarrier-Modulation kurz MCM. Dabei werden Daten in mehrere Teile aufgeteilt und auf mehrere Träger-Signale aufgeteilt. Diese Träger-Signale haben eine hohe Frequenz, das zusammengesetzte Signal jedoch eine niedrige. Durch dieses Prinzip der Modulation kann eine hohe Datenübertragungsrate auf niedrigen und somit weitreichenden Frequenzen erreicht werden.

Betriebsmodi

WLANs können abhängig von der Hardwareausstattung und Anforderungen der Betreiber in verschiedenen Modi betrieben werden. Dazu zählen

Der Infrastruktur-Modus

Dieser ähnelt einem Mobilfunknetz, wobei in einstellbaren Abständen kleine Datenpakete, „Beacons“ genannt, an alle im Empfangsbereich vorhandenen Stationen Informationen wie SSID, unterstützte Übertragungsraten und Art der Verschlüsselung liefern. Dies erleichtert den Verbindungsaufbau, da Clients nur den Netzwerknamen und evtl. Verschlüsselungsparameter kennen müssen. Außerdem wird so die Empfangsqualität überwacht, jedoch garantiert der Empfang eines Beacons keinesfalls eine stabile Verbindung.
Da WLAN auf OSI-Schicht II dieselbe Adressierung wie Ethernet verwendet, kann eine Ethernet-Netzwerkkarte nicht unterscheiden, ob sie mit einer anderen Netzwerkkarte oder einer WLAN-Karte kommuniziert. Es muss jedoch zwischen IEEE 802.11 (WLAN) und IEEE 802.3 (Ethernet) konvertiert werden.

Trotz des im Standard vorgesehenen Aufbaus von großen WLANs mit mehreren Basisstationen und unterbrechungsfreiem Wechsel zwischen Basisstationen kommt es in der Praxis zu Problemen:

- Durch die Frequenzüberlappung mehrerer Basisstationen kommt es zu Störungen
- Da es kein „Handover" zwischen Basisstationen gibt (die Intelligenz liegt beim Client), sucht ein Client erst nach einer neuen Station, wenn die Verbindung zur vorherigen abgebrochen ist.

Eine Lösung dieser Probleme kann es nur durch Implementierung einer Kontrollinstanz im WLAN geben, welche mit den Basisstationen kommuniziert und so z.B. einen Handover initiieren können. Dafür wird seit einigen Jahren an einem Standard inklusive neuer Geräteklasse namens „Lightweight Access Point" und dem dazugehörigen Protokoll „Lightweight Access Point Protocol" gearbeitet, wobei man sich noch immer nicht einig ist, welches Gerät letztlich welche Funktionen übernehmen soll. Bis dieser offene Standard fertiggestellt ist, kann man momentan nur auf proprietäre Lösungen zurückgreifen.

Ad-hoc-Modus

Im Ad-hoc-Modus sind alle Stationen gleichwertig. Sie lassen sich schnell ohne großen Aufwand aufbauen, im kleineren Rahmen sind allerdings Techniken wie Bluetooth eher gebräuchlich. Da es keine zentrale Instanz gibt, muss die koordinierende Funktion von Endgeräten übernommen werden. Eine Paketweiterleitung zwischen Stationen ist nicht möglich, da keine Informationen über Überblick das Netzwerk ausgetauscht werden können. Deshalb eignet sich der Ad-hoc-Modus nur für eine geringe Anzahl an Geräten, die auf Grund der Signalschwäche auch physisch nahe beieinander liegen müssen, da ein Gerät sonst möglicherweise mit einzelnen anderen Geräten nicht mehr kommunizieren kann, da schlicht weg kein Signal mehr empfangen wird.
Dieses Problem kann durch Ausstattung einzelner Geräte mit Routing-Fähigkeiten gelöst werden, sodass eine indirekte Weiterleitung an ein Gerät außer Empfangsreichweite über dritte Routing-Station möglich ist. Die Aufwertung zum mobilen Ad-hoc-Netzwerk, indem Softwarekomponenten auf jeder Station Daten zur Sichtbarkeit anderer Stationen und somit Weiterleitungsentscheidungen treffen, ist momentan in der Forschung, jedoch noch lange nicht abgeschlossen. Es gibt bereits eine lange Liste von Protokollen wie AODV (Ad-hoc On-demand Distance Vector), OLSR (Optimized Link State Routing), RoofNet (vom MIT), jedoch noch keinen Standard. Standardvorschläge wären einerseits das Hybrig Wireless Mesh Protocol, oder aber auch ein neuer IEEE-Standard 802.11s. Auf dieser Idee des standardisierten freien Funknetzes basiert auch das „Mesh networking", einer experimentellen neuen Form des Internets, bei dem alle Geräte direkt über ein „vermaschtes Netz" verbunden sind und die Kommunikation somit uneinsehbar von Ende zu Ende verschlüsselt ist. Momentan wird diese Technik in amerikanischen Städten erprobt, soll jedoch ein erster Schritt in Richtung Internet 2.0 sein.

Wireless Distribution System (WDS)

Ist ein Verfahren zur Adressierung von WLANs, das anspruchsvolle Topologien ermöglicht. Es wurde 1999 in aller Kürze definiert und bis heute lässt die Definition eine genaue Nutzung offen. Die Adressierung schafft Grundlagen für erweiterte WLANs und dient zum Beispiel dazu, ein Funknetzwerk mit mehreren Basisstationen aufzubauen, um eine größere Netzabdeckung zu erreichen. (Zum Beispiel das dynamische Wechseln eines Clients zwischen mehreren Routern mit derselben SSID)

Repeater

Ein Repeater hat die Funktion, WLAN-Signale aufzunehmen, zu verstärken und weiterzusenden.
Er erweitert das Drahtlosnetzwerk räumlich beispielsweise durch mehrere Wände bzw. Decken. Repeater sind „transparent", da verbundene Clients nicht wissen, ob sie mit einem Repeater kommunizieren.

Bridge

Eine Bridge wird zur Trennung eines großen Netzwerks mit viel Datenverkehr eingesetzt. Die soll das Problem der steigenden Anzahl von Kollisionen in einem Netzwerk mit hohem Datenaufkommen innerhalb des Netzwerks lösen und somit die Netzwerkeffizienz steigern. Eine Bridge sammelt dann die Adressen aller Geräte in einer Datenbank und koordiniert anschließend den Datenverkehr so, dass sich der Datenverkehr vermindert und so die Fehleranfälligkeit sinkt. Sinn macht dies allerdings nur bei viel Datenverkehr im Intranet.

Unterschiede zwischen Repeater und Bridge
Im Unterschied zum Repeater verbindet eine Bridge zwei gleichwertige Bereiche eines Netzwerks und hat dabei eine koordinierende Aufgabe. Währenddessen verstärkt ein Repeater die Sendeleistung eines Netzwerks und hat somit eine räumlich erweiternde bzw. verstärkende Funktion.

Versionsgeschichte und Datenübertragungsraten
Seit der Verabschiedung der 1. Version des Standards 1997 hat sich vor allem in Sachen Geschwindigkeit enorm viel getan. Es folgt ein Überblick über die wichtigsten IEEE 802.11 Standards.

Standard	Jahr	Frequenz	Bandbreite	Max. Datenrate
IEEE 802.11-1997*	1997	2,4 GHz	20 MHz	2 Mbit/s
IEEE 802.11a	1999	5,0 GHz	20, 40 MHz	54 Mbit/s
IEEE 802.11b	1999	2,4 GHz	22, 40, 80 MHz	11 Mbit/s
IEEE 802.11g	2003	2,4 GHz	20, 40 MHz	54 Mbit/s
IEEE 802.11-2007**	2007	---	---	---
IEEE 802.11n	2009	2,4 GHz / 5,0 GHz	20, 40 MHz	600 Mbit/s
IEEE 802.11p	2010	5,0 GHz	20, 40 MHz	54 Mbit/s
IEEE 802.11-2012***	2012	---	---	---
IEEE 802.11ac	2013	5,0 GHz	20, 40, 80, 160 MHz	6936 Mbit/s
IEEE 802.11ad	2016	60 GHz	1760 MHz	6930 Mbit/s
IEEE 802.11ah	2016	0,9 GHz	2000 MHz	347 Mbit/s

* Erste Version des Standards
** Zusammenfassung des Standards 1997 mit den 8 Erweiterungen a,b,d,e,g,h,i,j
*** Zusammenfassung des Standards 2007 mit den 10 Erweiterungen k,n,p,r,s,u,v,w,x,y,z

Der 802.11a Standard ermöglichte erstmals den Einsatz im 5 Ghz-Bereich und bietet heute die Basis für diverse Erweiterungen, u.a. c, d und h. Der 802.11n Standard wird heute überwiegend genutzt und ist selbst in den billigsten Geräten zu finden, oft jedoch nur auf 2,4 GHz Basis. Er ermöglichte erstmals den Einsatz von 40 MHz Kanalbreiten, was jedoch die Anzahl der überlappungsfreien Kanäle halbiert. Der 802.11h Standard ist eine Erweiterung für 802.11a und fügt Transmission Power Control (TCP) und Dynamic Frequency Selection (DFS) hinzu, damit Radaranlagen und Satelliten nicht gestört werden. Mittlerweile muss bei großen Sendeleistungen und außerhalb von Gebäuden der Standard in Europa zwingend eingesetzt werden. In den neuen Geräten ab 2013 ist außerdem der Empfang von 802.11ac Standard, bei welchem die Kanalbreiten 80 und 160 MHz eingeführt wurden. Seit 2017 verfügen die neuesten Smartphones (u.a Samsung Galaxy S8) über Unterstützung für den neuesten 802.11ad Standard, dieser muss sich bei den Geräteherstellern jedoch erst durchsetzen. Der 802.11ad ist außerdem nur für Distanzen bis zu 10m um den Sender ausgelegt, und für hohe Datenraten konzipiert, die in einem Frequenzbereicht operieren, wo keine Störung auftritt. Die Version 802.11ah wurde für extremen Langstreckeneinsatz konzipiert und bietet eine Empfangsreichweite von bis zu 1km (!) bei einer theoretischen Bandbreite von 347 Mbit/s. Noch eine Bemerkung zu den oben angeführten Datenraten: Diese stellen jeweils das rechnerische Maximum mit der jeweils höchsten Bandbreite und maximalen Antennenkonfiguration dar und dürften in der Praxis deshalb kaum erreicht werden.

Frequenzbereiche, Kanäle und Reichweiten
Der Frequenzbereich im 2,4 GHz Band wurde in 14 Kanäle aufgeteilt, wobei der 14. ausschließlich in Japan lizenzfrei benutzbar ist. In Österreich sind die Kanäle 1-13 nutzbar, wobei nur die Kanalkonfiguration 1,5,9,13 bei einer Bandbreite von 20 MHz störungsfrei nutzbar ist. Die maximale Sendeleistung ist in Europa und Japan auf 100mW begrenzt, in den USA sind bis zu 1.000mW legal nutzbar. Im 5Ghz-Bereich stehen insgesamt 24 (in Europa 21) Kanäle zur Verfügung, welche sich auf den Kanalnummern 36-165 unregelmäßig verteilen. Die maximale Sendeleistung beträgt auf den 1. 8 Kanälen 200mW, auf den letzten 5 25mW und dazwischen 1.000mW. Im neuen 60GHz-Bereich gibt es

4 Kanäle zwischen 58,32 und 65,88 GHz, dies sind jedoch vorläufige Angaben, da diese noch nicht normiert sind.
Bei einer Sendeleistung von 100mW im 2,4GHz-Bereich und 500mW im 5Ghz-Bereich sind Reichweiten von 30 bis 100 Metern auf freier Fläche möglich, mit zusätzlichen externen Antennen sind auf Sichtkontakt mehrere Kilometer Überbrückung möglich. Der 802.11ad-Standard im 60GHz-Bereich kann wie oben erwähnt mit aktueller Technik nur eine Entfernung von bis zu 10 Metern überwinden.

Sicherheit und Verschlüsselungsmethoden
Als Teil des 802.11 Originalstandards war Wired Equivalent Privacy (WEP) implementiert, welches jedoch auf Grund des schwachen RC4-Algorithmus mit einer maximalen statischen Schlüssellänge von 232 Bit bereits 2001 als „gebrochen" erklärt wurde. Danach folgten technische Ergänzungen wie u.a. WEPplus, Wi-Fi Protected Access (WPA), Extensible Authentication Protocol (EAP) oder Kerberos, die alle das Sicherheitsproblem mehr oder weniger verkleinerten. WEPplus erschwerte das Finden eines schwachen Initialisierungsvektors und Kerberos unterband über die Authentifizierung mit einem externen Kerberos-Server man-in-the-middle-Attacken. WPA hatte dann eine Schlüssellänge von 48 Bit und mit TKIP wurden der kryptographische Algorithmus samt MAC-Adresse als Erweiterung für den Verschlüsselungsalgorithmus implementiert. Jedoch war 2009 auch diese Technologie gehackt worden. Der offizielle Nachfolger war dann IEEE 802.11i. Dieser bietet erhöhte Sicherheit durch Advanced Encryption Standard (AES) bei WPA2 und gilt derzeit als „sicher", wobei damit der Verschlüsselungsalgorithmus an sich gemeint ist, denn Angriffe mit Wörterbuch oder Brute-Force sind weiterhin möglich. Es hängt also bei WPA2 und AES 256 nicht mehr am Verschlüsselungsalgorithmus, jedoch umso mehr beim verwendeten Passwort.

CSMACA (Carrier Sense Multiple Access with Collision Avoidance)
Ist ein Prinzip zur Vermeidung von Kollisionen bei Zugriff mehrerer Netzwerkstationen auf denselben Übertragungskanal. Es stellt eine Erweiterung zu CSMA/CD (Ethernet) dar und wurde zu einem listen-before-talk-Mechanismus weiterentwickelt, um anstatt Kollisionserkennung bestmögliche Kollisionsvermeidung zu gewährleisten. Möchte ein Gerät Daten nach diesem Verfahren senden, ist folgender Ablauf möglich:

1. Medium horcht (Carrier Sense)
2. Wenn Medium für reguläre Sendezeit frei → Backoffzeit aus Contention Window auswürfeln und nach Ablauf senden
3. Wenn Medium belegt → Backoff bis zum Ablauf des Network Allocation Vectors gestoppt, bevor es nach weiterem Distributed Coordination Function Interframe Spacing weiterläuft
4. Nach Empfang wartet Empfänger Sendezeit eines CTS-Pakets (Short Interframe Spacing) ab, bevor gesendet wird
5. Kollision durch gleichzeitigen Ablauf von Backoffs führt zu Timeout, es wird festgelegte Zeit (Extended Interframe Spacing) gewartet, bevor Vorgang sich wiederholt

Grundsätzlich gilt: SIFS < PIFS < DIFS < EIFS

WLAN und das Hidden Terminal Problem
Das Hidden Terminal Problem (engl.: Hidden Node Problem) tritt zum Beispiel auf, wenn der Sender A mit dem Empfänger B drahtlos kommuniziert und sich in Reichweite des Empfängers B eine weitere Station C (hidden terminal) befindet, jedoch vom Sender A nicht gesehen wird, da sie außer Reichweite liegt. Somit kann die Station C ebenfalls an Empfänger B senden und so die Kommunikation zwischen A und B stören, was Kollisionen zur Folge haben kann. Dies muss aber von C nicht Absicht sein, denn C kann A ebenfalls nicht sehen, wodurch C davon ausgeht, dass Empfänger B frei ist und ihn ansprechen kann. Durch spezielle Verfahren wie RTS/CTS (eine Erweiterung von CSMA, auch unter dem Synonym MACA Multiple Access with Collision Avoidance bekannt) wird versucht, das Hidden-Station-Problem zumindest teilweise zu vermeiden. Wenn B auf einen Request-to-send von A mit einem Clear-to-send antwortet, hört Station C dies mit und wartet für die Zeit der Übertragung von A zu B. Jedoch kann das Problem nicht vollständig verhindert werden. Das bedeutet, wenn Sender A ein CTS-Paket sendet, ist

der Kanal für eine bestimmte im Paket angegebene Dauer belegt. Auch das CTS Antwortpaket des Empfängers hält den Kanal für eine bestimmte Zeit frei. Alle Stationen, die diese Pakete empfangen, schweigen solange, bis die CTS-Antwort konfliktfrei empfangen wurde und die Sendestation die Daten versandt hat. Dadurch sind Kollisionen nur mehr während des Sendens von RTS und CTS-Paketen möglich, jedoch entsteht der Nachteil eines relativ hohen Aufwands für den Austausch der Reservierungsnachrichten. Jedoch lohnt sich der Aufwand, weil er immer noch geringer ist, als jener eines Datenverlustes bei Kollisionen und die dadurch zwingende Neusendung des Pakets, welche möglicherweise wieder unterbrochen werden könnte. Es ergeben sich daraus also weitere Bedingungen zusätzlich zu den bei CSMACA genannten Vorgängen:

- Sendevorgang wird nicht aufgenommen, solange Sendung läuft (jeder hat nur begrenzte Sendezeit)
- Sendevorgang wird abgebrochen, sobald Sender durch Empfang eines anderen Senders Kollision feststellt. Nächste Aussendung wird um zufällig bestimmte Pause verzögert
- Empfänger, der Kollision feststellt, sendet selbst Signal in Erwartung, dass kollidierende Sender dies erkennen und beide Pauseroutine einleiten. (Durch zufällige Pausenzeiten verzögert sich einer länger als der andere und es kommt nur in ganz seltenen Fällen zu einer weiteren Kollision.)

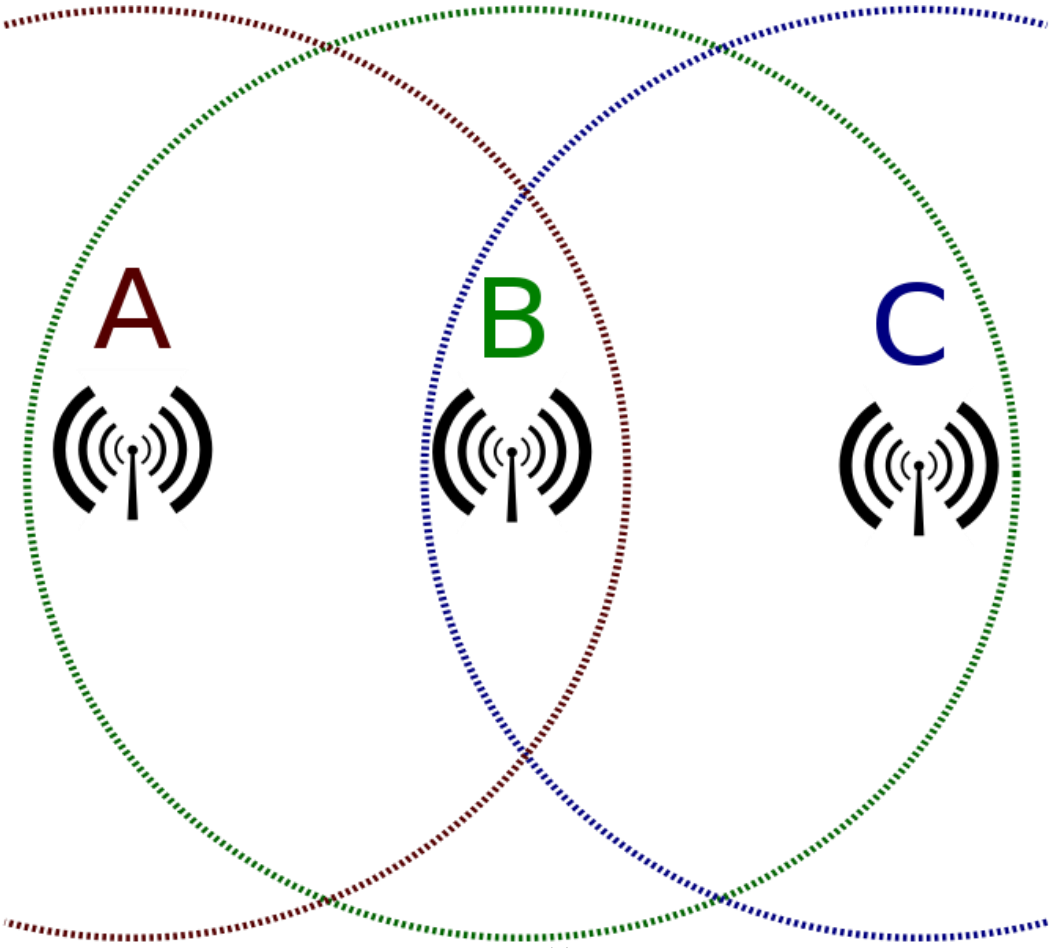

Abbildung 1: Hidden Terminal Problem

Zukunft von WLAN

In näherer Zukunft wird man in immer neuen Frequenzbereichen versuchen, das Optimum zwischen Reichweite und Bandbreite zu finden, da die Datengröße in den letzten Jahren enorm gestiegen ist. Technologien wie WiGig, also WLANs mit Multi-Gigabit-Geschwindigkeit zusammen mit dem 802.11ad Standard werden weiterentwickelt, um Initiativen wie Public Wifi zu pushen und den immer wachsenden Datenraten gerecht zu werden.

Bluetooth (Wireless Personal Area Network)

Was ist Bluetooth?

Bluetooth ist Industriestandard zur Datenübertragung zwischen Geräten über kurze Distanz per Funktechnik (WPAN = Wireless Private Area Network). Er wurde 1994 von Ericsson entwickelt und stellte ursprünglich die kabellose Alternative zu RS-232 Kabeln dar. Die Technologie wird seit 1998 von der Bluetooth Special Interest Group verwaltet und weiterentwickelt. Bluetooth ist gemäß dem IEEE 802.15.1 Standard zertifiziert, wird aber heute von der IEEE nicht mehr unterstützt. Die Bluetooth Special Interest Group ist eine Interessensgemeinschaft von mehr als 30.000 Unternehmen, die die Technologie weiterentwickeln und verbreiten. Sie wurde 1998 von Ericsson, IBM, Intel, Nokia und Toshiba gegründet. Sie ist Eigentümer des Bluetooth-Warenzeichens und Herausgeber der Spezifikationen.

Ursprung

Die Entwicklung der „Short-link radio technology", später „Bluetooth", wurde 1989 von Ericsson CTO Nils Rydebeck und Johan Ullman gestartet, um kabellose Kopfhörer zu entwickeln.

Übertragungstechnik

Die Datenübertragung findet im 2,4GHz-Frequenzbereich über UHF (Ultra High Frequency) Mikrowellen statt. Dabei wird ein Datenpaket auf 79 Einzelkanäle mit einer Frequenz von 1 MHz aufgeteilt und übertragen. Die neuere Technik Bluetooth Low Energy setzt auf 40 Kanäle mit je 2 MHz. Die Übertragung basiert dabei auf dem Frequenzsprungverfahren (frequency hopping), bei dem die Kanäle im 1MHz-Abstand bis zu 1600-mal pro Sekunde gewechselt werden. Am unteren und oberen Ende gibt es ein Sicherheitsband zu anderen Frequenzbereichen. Die Daten können auch verschlüsselt übertragen werden. Bluetooth gilt dann als abhörsicher, wenn eine mehrstufige dynamische Schlüsselvergabe stattfindet, bei welcher der PIN-Code nicht zu kurz gewählt wird (mehr als 4 Dezimalziffern). Die Übertragung findet nach dem Master-Slave-Prinzip in einem Piconet statt, dass aus bis zu acht aktiven Teilnehmern besteht. Jeder Teilnehmer wird über eine 3-Bit-Adresse angesprochen. Der Master steuert die Kommunikation und vergibt Sende-Zeiteinheiten an die Slaves (Zeitmultiplexverfahren). Ein Client kann in mehreren Pico-Netzen gleichzeitig angemeldet sein, jedoch nur in einem als Master fungieren.

Leistungsklassen

Die Reichweite ist abhängig von der Sendeleistung und der Empfindlichkeit der Bauteile bei Sender und Empfänger. Bluetooth kann in 4 „Klassen" je nach Sendeleistung grob eingeteilt werden:

- Klasse I: Bis zu 100m Reichweite bei 100mW
- Klasse II: Bis zu 10m Reichweite bei 2,5mW
- Klasse III: Bis zu 1m Reichweite bei 1mW
- Klasse IV: Bis zu 0,5m Reichweite bei 0,5mW

Versionsgeschichte und Übertragungsraten

Version	Jahr	Datenrate	Reichweite
1.0	1999	0,7322 Mbit/s	Bis 10m
1.1	2001	0,7322 Mbit/s	Bis 10m
1.2	2003	1 Mbit/s	Bis 10m
2.0+EDR	2004	2,1 Mbit/s	Bis 100m
2.1+EDR	2007	2,1 Mbit/s	Bis 100m
3.0+HS	2009	24 Mbit/s	Bis 100m
4.0	2010	24 Mbit/s	Bis 100m
4.1	2013	24 Mbit/s	Bis 100m
4.2	2014	24 Mbit/s	Bis 100m

5.0	2016	48 Mbit/s	Bis 400m

Wie bereits im Vorfeld erwähnt hängt die Reichweite stark von der Empfindlichkeit der Bauteile und dem Strombedarf ab. Die oben genannten Angaben sind theoretische Angaben bei maximaler Empfindlichkeit und maximalem Strombedarf. Seit der Version 4.0 gibt es außerdem Bluetooth Low Energy, welches den Stromverbrauch in einem ähnlichen Kommunikationsbereich erheblich reduziert. Dieser Standard wird parallel zu den normalen Versionen weiterentwickelt und findet seinen Einsatz vor allem in Smartphones, Smartwatches und anderen Kleinstgeräten in der Konsumelektronik, welche grundsätzlich einen niedrigen Energiebedarf hat.

In den letzten Jahren hat sich ein Konkurrenzkampf um die IoT-Geräte und deren Konnektivität entwickelt, bei deren Bluetooth 5 und WLAN 802.11ah gegeneinander konkurrieren, wobei hier Bluetooth das Nachsehen haben dürfte.

Quellen

https://de.wikipedia.org/wiki/Wireless_Local_Area_Network
https://de.wikipedia.org/wiki/IEEE_802.11
https://de.wikipedia.org/wiki/Orthogonales_Frequenzmultiplexverfahren
http://whatis.techtarget.com/definition/multi-carrier-modulation-MCM
https://de.wikipedia.org/wiki/Institute_of_Electrical_and_Electronics_Engineers
https://de.wikipedia.org/wiki/Optimized_Link_State_Routing
https://de.wikipedia.org/wiki/Optimized_Link_State_Routing
https://de.wikipedia.org/wiki/Freies_Funknetz
https://de.wikipedia.org/wiki/Vermaschtes_Netz
https://de.wikipedia.org/wiki/Wireless_Distribution_System
http://www.itbusinessedge.com/blogs/data-and-telecom/the-age-of-wigig-is-almost-here.html
https://de.wikipedia.org/wiki/IEEE_802.11p
https://de.wikipedia.org/wiki/IEEE_802.11ad
https://de.wikipedia.org/wiki/IEEE_802.11ah
https://de.wikipedia.org/wiki/IEEE_802.11i
https://de.wikipedia.org/wiki/Wireless_Personal_Area_Network
https://de.wikipedia.org/wiki/Bluetooth
https://en.wikipedia.org/wiki/Bluetooth
https://en.wikipedia.org/wiki/Frequency-shift_keying#Gaussian_frequency-shift_keying
https://en.wikipedia.org/wiki/Phase-shift_keying
https://en.wikipedia.org/wiki/Ultra_high_frequency
https://de.wikipedia.org/wiki/Bluetooth_Low_Energy
http://blueapp.io/blog/history-of-bluetooth/
https://de.wikipedia.org/wiki/Extensible_Authentication_Protocol
https://de.wikipedia.org/wiki/Pre-shared_key
https://de.wikipedia.org/wiki/Temporal_Key_Integrity_Protocol
https://de.wikipedia.org/wiki/Wi-Fi_Protected_Access
https://de.wikipedia.org/wiki/Kerberos_(Informatik)
https://de.wikipedia.org/wiki/WEPplus
https://de.wikipedia.org/wiki/Wired_Equivalent_Privacy
https://www.golem.de/news/broadcom-sicherheitsluecke-angriff-ueber-den-wlan-chip-1704-127151.html
https://www.pcwelt.de/ratgeber/Hacker-Angriff-aufs-WLAN-WLAN-Sicherheit-5632681.html
https://www.computerwoche.de/a/modernes-wlan-hacking,2521564
http://www.wlanrepeater.org/ratgeber/unterschied-router-repeater-bridge/
https://de.wikipedia.org/wiki/Carrier_Sense_Multiple_Access/Collision_Avoidance
https://de.wikipedia.org/wiki/Interpacket_Gap
https://de.wikipedia.org/wiki/Wireless_Access_Point
https://www.ieee.org/standards/index.html