**WLAN (Wireless Local Area Network)**

**Was ist ein WLAN?**

* Wireless Local Area Network
* lokales Funknetz
* gehört zur Familie der IEEE-Standards; offizielle Bezeichnung: **IEEE 802.11**

**Übertragungstechnik**

* Übertragung via elektromagnetische Wellen auf unterschiedlichen Frequenzen
* WLANs sind angepasste Form der OSI Schicht I und II und verwenden heute meist das Modulationsverfahren OFDM (Orthogonal Frequency-Division Multiplexing).
* ODFM: spezielle Implementierung der Multicarrier-Modulation kurz MCM
* Aufteilen des Frequenzbereiches in mehrere schmalbandige Träger orthogonal zueinander
* Dadurch viel höhere Datenrate auf gleicher Bandbreite möglich, da Träger unabhängig voneinander gleichzeitig im selben Frequenzspektrum übertragen können

**Betriebsmodi**

**Infrastruktur-Modus**

* Ähnlich einem Mobilfunknetz
* Senden von kleinen Datenpaketen „Beacons“ an alle Stationen im Empfangsbereich
* Beacons enthalten SSID, unterstützte Übertragungsraten und Verschlüsselungen
* erleichtert den Verbindungsaufbau, Clients müssen nur Netzwerknamen und evtl. Verschlüsselungsparameter kennen
* Überwachung der Empfangsqualität, jedoch keine Garantie für stabile Verbindung
* Ethernet-Netzwerkkarte kann nicht unterscheiden, ob sie mit einer anderen Netzwerkkarte oder einer WLAN-Karte kommuniziert, da Adressierung dieselbe ist
* Es muss jedoch zwischen IEEE 802.11 (WLAN) und IEEE 802.3 (Ethernet) konvertiert werden
* Trotz 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“ (dynamischer Wechsel) zwischen Basisstationen gibt, 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 initiiert
* 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
* momentan nur proprietäre Lösungen möglich

**Ad-hoc-Modus**

* alle Stationen gleichwertig
* schneller Aufbau ohne großen Aufwand
* im kleineren Rahmen allerdings Techniken wie Bluetooth gebräuchlicher
* keine zentrale Instanz gibt, daher koordinierende Funktion durch Endgeräte
* Paketweiterleitung zwischen Stationen nicht möglich, da keine Informationen über Netzwerktopografie ausgetauscht werden können
* Deshalb Ad-hoc-Modus nur für eine geringe Anzahl an Geräten, die physisch nahe beieinanderliegen müssen, da Gerät sonst möglicherweise mit einzelnen anderen Geräten nicht mehr kommunizieren kann
* Lösung durch Ausstattung einzelner Geräte mit Routing 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
* 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 Hybrid Wireless Mesh Protocol, oder aber auch ein neuer IEEE-Standard 802.11s

**Wireless Distribution System (WDS)**

* Verfahren zur Adressierung für WLANs mit anspruchsvollen Topologien
* 1999 in aller Kürze definiert, bis heute lässt die Definition eine genaue Nutzung offen
* 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**

* Nimmt WLAN-Signale auf, verstärkt diese und sendet sie weiter
* Erweitert Drahtlosnetzwerk räumlich
* Repeater sind „transparent“, da verbundene Clients nicht wissen, ob sie mit einem Repeater kommunizieren.

**Bridge**

* Für die Trennung eines großen Netzwerks mit viel Datenverkehr
* Soll Problem der steigenden Anzahl von Kollisionen in einem Netzwerk mit hohem Datenaufkommen innerhalb des Netzwerks lösen und Netzwerkeffizienz steigern
* Sammelt Adressen aller Geräte in Datenbank und koordiniert anschließend den Datenverkehr so, dass sich Datenverkehr vermindert und so Fehleranfälligkeit sinkt
* Nur sinnvoll bei viel Datenverkehr im Intranet.

**Unterschiede zwischen Repeater und Bridge**

* Bridge hat netzwerkerweiternde bzw. koordinierende Aufgabe
* Repeater hat netzwerkverstärkende Aufgabe

**Versionsgeschichte und Datenübertragungsraten**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **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 802.11n | 2009 | 2,4 GHz / 5,0 GHz | 20, 40 MHz | 600 Mbit/s |
| 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 |

* 802.11a ermöglichte erstmals den Einsatz im 5 Ghz-Bereich und bietet heute die Basis für diverse Erweiterungen, u.a. c, d und h.
* 802.11n wird heute überwiegend genutzt und ist selbst in den billigsten Geräten zu finden, oft jedoch nur auf 2,4 GHz Basis
* Ermöglichte erstmals den Einsatz von 40 MHz Kanalbreiten, was jedoch die Anzahl der überlappungsfreien Kanäle halbiert
* 802.11h 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 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 Geräte über Unterstützung für den neuesten 802.11ad Standard, dieser muss sich bei den Geräteherstellern jedoch erst durchsetzen.
* nur für Distanzen bis zu 10m um den Sender ausgelegt, und für hohe Datenraten konzipiert, die in einem Frequenzbereich operieren, wo keine Störung auftritt
* 802.11ah wurde für extremen Langstreckeneinsatz konzipiert und bietet eine Empfangsreichweite von bis zu 1km (!) bei einer theoretischen Bandbreite von 347 Mbit/s.

Hinweis: Geschwindigkeitsangaben 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**

* 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.
* maximale Sendeleistung 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
* Im 60GHz-Bereich gibt es 4 Kanäle zwischen 58,32 und 65,88 GHz, dies sind jedoch vorläufige Angaben, da sie 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**

* Wired Equivalent Privacy (WEP) als Teil des Originalstandards 802.11
* 2001 auf Grund des schwachen RC4-Algorithmus mit einer maximalen statischen Schlüssellänge von 232 Bit als gebrochen erklärt
* 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 Finden eines schwachen Initialisierungsvektors
* Kerberos unterband über die Authentifizierung mit einem externen Kerberos-Server man-in-the-middle-Attacken
* WPA hatte Schlüssellänge von 48 Bit
* Mit TKIP wurden der kryptographische Algorithmus samt MAC-Adresse als Erweiterung für den Verschlüsselungsalgorithmus implementiert
* 2009 auch diese Technologie gehackt
* offizieller Nachfolger war dann IEEE 802.11i.
* 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)**

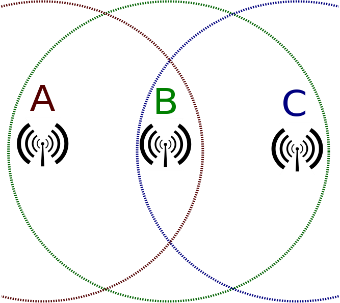
* Prinzip zur Vermeidung von Kollisionen bei Zugriff mehrerer Netzwerkstationen auf denselben Übertragungskanal.
* Es stellt eine Erweiterung zu CSMA/CD (Ethernet)
* listen-before-talk-Mechanismus
* anstatt Kollisionserkennung bestmögliche Kollisionsvermeidung
* Möchte Gerät Daten nach diesem Verfahren 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**

* tritt zum Beispiel auf, wenn Sender A mit Empfänger B drahtlos kommuniziert und in Reichweite von Empfänger B eine weitere Station C (hidden terminal) befindet, jedoch vom Sender A nicht gesehen wird, da sie außer Reichweite von A liegt.
* Somit kann 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 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
* 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 Nachteil eines relativ hohen Aufwands für den Austausch der Reservierungsnachrichten.
* Jedoch lohnt sich Aufwand, weil er immer noch geringer ist, als jener eines Datenverlustes bei Kollisionen und die dadurch zwingende Neusendung des Pakets,
* 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.)



**Zukunft von WLAN**

* Forschung an Optimum zwischen Reichweite und Bandbreite in optimalen Frequenzbereich, da die Datengröße in den letzten Jahren enorm gestiegen ist.
* WiGig (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?**

* Industriestandard zur Datenübertragung zwischen Geräten über kurze Distanz per Funktechnik (WPAN = Wireless Private Area Network).
* 1994 von Ericsson entwickelt und stellte ursprünglich die kabellose Alternative zu RS-232 dar.
* Seit 1998 von der Bluetooth Special Interest Group verwaltet und weiterentwickelt.
* gemäß IEEE 802.15.1 zertifiziert, wird aber heute von der IEEE nicht mehr unterstützt.

**Übertragungstechnik**

* 2,4GHz-Frequenzbereich über UHF (Ultra High Frequency) Mikrowellen
* 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
* 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
* Daten können auch verschlüsselt übertragen werden
* gilt dann als abhörsicher, wenn eine mehrstufige dynamische Schlüsselvergabe stattfindet, bei welcher der PIN-Code nicht zu kurz gewählt wird (mehr als 4 Dezimalziffern)
* 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
* Ein Client kann in mehreren Pico-Netzen gleichzeitig angemeldet sein, jedoch nur in einem als Master fungieren.

**Leistungsklassen**

* Reichweite abhängig von der Sendeleistung und Empfindlichkeit der Bauteile
* 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 |
| 2.0+EDR | 2004 | 2,1 Mbit/s | Bis 100m |
| 3.0+HS | 2009 | 24 Mbit/s | Bis 100m |
| 4.0 | 2010 | 24 Mbit/s | Bis 100m |
| 5.0 | 2016 | 48 Mbit/s | Bis 400m |

* Angaben sind theoretische Werte bei maximaler Empfindlichkeit und maximalem Strombedarf
* Seit der Version 4.0 gibt es parallel Bluetooth Low Energy, welches 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.

**Zukunft von Bluetooth**

* In den letzten Jahren hat sich Konkurrenzkampf um die IoT-Geräte und deren Konnektivität entwickelt
* Bluetooth 5 und WLAN 802.11ah konkurrieren gegeneinander, wobei hier Bluetooth das Nachsehen haben dürfte, da WLAN im IoT-Bereich schon weit verbreitet ist.