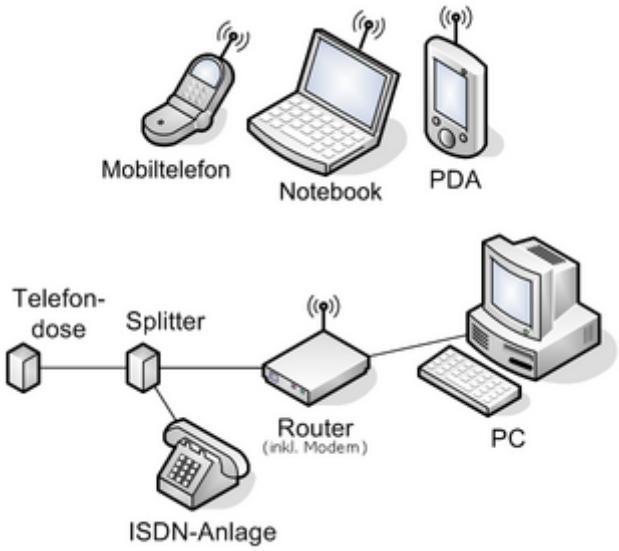
Wireless LAN

aus Wikipedia, der freien Enzyklopädie



Typisches Wireless LAN im Privathaushalt

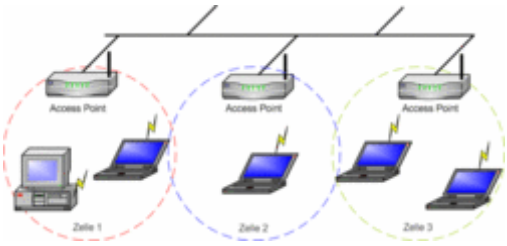
Wireless LAN /ˈwaɪələs ˈlɑːn/ (***Wireless Local Area Network***, **WLAN**) bezeichnet ein "drahtloses" lokales Funknetz, wobei meistens ein Standard der IEEE 802.11-Familie gemeint ist. Das Kürzel *Wi-Fi* wird oft fälschlich mit WLAN gleichgesetzt.

Im Gegensatz zum Wireless Personal Area Network (WPAN) haben WLANs größere Sendeleistungen und Reichweiten und bieten im allgemeinen höhere Datenübertragungsraten. WLANs stellen Anpassungen der Schicht 1 und 2 des OSI-Referenzmodells dar, wohingegen in WPANs z.B. über eine im Protokoll vorgesehene Emulation der seriellen Schnittstelle und PPP bzw. SLIP eine Netzverbindung aufgebaut wird.

Inhaltsverzeichnis

- 10 Weblinks

Betriebsarten



WLAN Infrastruktur-Netz (Zelltopologie)

Ein WLAN kann man in zwei Modi betreiben: dem Infrastruktur-Modus und dem Ad-hoc-Modus.

Im Infrastruktur-Modus wird eine Basisstation, häufig ein Wireless Access Point, speziell ausgezeichnet. Er koordiniert die einzelnen Netzknoten. Häufig ist diese Basis-Station dann auch Mittler in ein weiteres Netz, das sowohl Funknetz als auch ein klassisches Kabelnetz sein kann.

Im Ad-hoc-Modus ist keine Station besonders ausgezeichnet, sondern alle sind gleichwertig. In solchen Netzen ist zwar ein Datenaustausch einfach möglich, jedoch ist kein gezieltes Routing in externe Netze möglich. Dafür lassen sich Ad-Hoc-Netze schnell und ohne großen Aufwand aufbauen. Infrastrukturnetze erfordern, implementiert man sie sinnvoll, mehr Planung. OLSR ist ein spezielles Ad-hoc Protokoll.

WLANs nach IEEE 802.11 und HIPERLAN unterstützen beide Betriebsmodi. Gerade in WPANs werden gerne Ad-Hoc-Verfahren eingesetzt.

Datensicherheit

Verschlüsselung

Teil des WLAN-Standards IEEE 802.11 ist *Wired Equivalent Privacy* (*WEP*), ein Sicherheitsstandard, der den RC4-Algorithmus enthält. Die enthaltene Verschlüsselung mit nur 40 Bit bzw. 104 Bit, bei einigen Herstellern auch 128 Bit oder 232 Bit, reicht jedoch selbst bei 232 Bit (256 Bit genannt) längst nicht aus. Durch das Sammeln von Schlüsselpaaren sind *Known-Plaintext-Attacken* möglich. Es gibt frei erhältliche Programme, die sogar ohne vollständigen Paketdurchlauf in der Lage sind, einen schnellen Rechner vorausgesetzt, das Passwort zu entschlüsseln, wobei das bei einem 232 Bit Schlüssel etwas dauern kann, aber eben nicht unmöglich ist. Jeder Nutzer des Netzes kann den gesamten Verkehr zudem mitlesen. Die Kombination von RC4 und CRC wird als mathematisch unsicher betrachtet.

Aus diesen Gründen haben sich technische Ergänzungen entwickelt, etwa WEPplus, WPA (Wi-Fi Protected Access) als Vorgriff und Teilmenge zu 802.11i, Fast Packet Keying,

Extensible Authentication Protocol (EAP), Kerberos oder High Security Solution, die alle mehr oder weniger gut das Sicherheitsproblem von WLAN verkleinern.

Der Nachfolger des WEP ist der neue Sicherheitsstandard 802.11i. Er bietet eine erhöhte Sicherheit durch die Verwendung von TKIP bei WPA bzw. AES bei WPA2 und gilt zur Zeit als nicht zu entschlüsseln, solange man bei der Einrichtung keine trivialen Passwörter verwendet (Brute Force Attacke). Als Empfehlung kann gelten, mit einem Passwortgenerator Passwörter zu erzeugen, die Buchstaben in Groß- und Kleinschreibung, Zahlen und Sonderzeichen enthalten und nicht kürzer als 32 Zeichen sind.

WPA2 ist das Äquivalent der WiFi zu 802.11i das mit dem Verschlüsselungsalgorithmus AES (Advanced Encryption Standard mit Schlüssellängen von 256 Bit) arbeitet und in neueren Geräten meist unterstützt wird. Ein genaues Betrachten der technischen Daten um herauszufinden, ob WPA2 auch tatsächlich unterstützt wird, empfiehlt sich allerdings vor dem Kauf.

Eine alternative Herangehensweise besteht darin die Verschlüsselung komplett auf IP-Ebene zu verlagern. Hierbei wird der Datenverkehr beispielsweise durch die Verwendung von IPsec oder auch durch einen VPN-Tunnel geschützt. Besonders in freien Funknetzen werden so die Inkompatibilitäten verschiedener Hardware umgangen, eine zentrale Benutzerverwaltung vermieden und der offene Charakter des Netzes gewahrt.

Beim so genannten WarWalking werden mit einem WLAN-fähigen Notebook oder PDA offene WLAN-Netze gesucht. Diese werden dann mit Kreide markiert (WarChalking). Das Ziel ist hierbei entweder, Sicherheitslücken aufzudecken und dem Betreiber zu melden, oder aber einen kostenlosen Internetzugang zu erhalten oder gar Daten auszuspähen oder zu manipulieren. Fährt man bei der Suche eines WLAN-Netzes mit einem Auto, so spricht man von WarDriving.

Authentifizierung

Extensible Authentication Protocol ist ein Protokoll zur Authentifizierung von Clients. Es kann zur Nutzerverwaltung auf RADIUS-Server zurückgreifen. EAP wird hauptsächlich innerhalb von WPA für größere WLAN-Installationen eingesetzt.

Gesundheit

Die von WLAN-Geräten genutzten Funkfrequenzen liegen um 2,4 GHz, im Mikrowellenbereich. Die gleiche Wellenlänge wird von Mikrowellenherden, Mobilfunk und Radar genutzt. Es herrscht allgemein Unsicherheit darüber, ob die Strahlungsleistungen, die von Mobilfunk- oder WLAN-Geräten ausgehen, schädliche Auswirkungen auf Organismen haben – sprich gefährlich sind. Bei den Leistungen innerhalb eines Mikrowellenherdes oder in der Nähe militärischer Radaranlagen sind schädliche Auswirkungen unbestritten.

Im Unterschied zu GSM senden WLAN-Geräte jedoch mit einer deutlich niedrigeren Sendeleistung (0,1 Watt statt 1-10 Watt) und mittels Frequenzspreizung mit einer höheren Bandbreite. Die Energie pro Frequenzband ist also deutlich niedriger und teilweise kaum vom Hintergrundrauschen zu unterscheiden.

Reichweite und Antennen

Die Antennen handelsüblicher 802.11 Endgeräte lassen 30 bis 100 Meter Reichweite erwarten. Mit neuester Technik lassen sich sogar 80 Meter in geschlossenen Räumen erreichen.

Bessere WLAN-Hardware sollte den Anschluss einer externen Antenne erlauben. Mit externen Rundstrahlantennen lassen sich bei Sichtkontakt 100 bis 300 Meter im Freien überbrücken.

Leichtbauwände mindern die Reichweite, sind aber einzeln kein Hindernis; dagegen werden Stahl und Beton nicht durchdrungen, können im Außenbereich aber experimentell als Reflektorwand dienen, um Funklöcher "auszuspiegeln". Bäume, insbesondere dicht belaubte, sind ebenfalls Hindernisse für WLAN-Verbindungen.

WLAN nach 802.11b (maximal 11 Mbit/s brutto) oder 802.11g (maximal 54 Mbit/s brutto) funkt im 2,4-GHz-Band (Wellenlänge von ca. 13 cm). Damit werden alle Gegenstände, ab einer Dicke von 13 cm, zu echten Wellenbrechern. Je stärker die elektrische Leitfähigkeit des Materials, desto stärker der Effekt. Außerdem können leitende Gegenstände in der Nähe von Antennen deren Richtcharakteristik stark beeinflussen.

WLAN nach 802.11a (maximal 54 Mbit/s brutto) funkt im 5-GHz-Band, in dem ein größerer Frequenzbereich (455 MHz) zur Verfügung steht und damit 19 nicht überlappende Frequenzen (in Deutschland) nutzbar sind. Auch dieser Frequenzbereich ist in Deutschland lizenzfrei nutzbar. Im Normalbetrieb nach 802.11a sind 30 mW Sendeleistung erlaubt. Unter strengeren Auflagen (TPC, Transmit Power Control und DFS, Dynamic Frequency Selection) sind höhere Sendeleistungen bis 1000 mW gestattet. TPC und DFS sollen sicherstellen, dass Satellitenverbindungen und Radargeräte nicht gestört werden (World Radio Conference 2003). Dies und die höheren Kosten der Hardware auf Grund der höheren Frequenz bewirken, dass sich 802.11a noch nicht gegen 802.11b oder g durchgesetzt hat.

Mit speziellen Richtfunkantennen lassen sich bei Sichtkontakt mehrere Kilometer überbrücken. (Hier werden teilweise irrsinnige Rekorde mit Verbindungen über mehrere hundert Kilometer ohne aktiven Verstärker – abgesehen von den Antennen – erzielt. Allerdings funktioniert das nur zwischen hohen Bergen; auf dem Meer endet nach etwa 30 km durch die Erdkrümmung der Sichtkontakt.)

Antennen bringen einen Sende- wie Empfangs-Gewinn (Antennengewinn, in dBi), indem sie elektromagnetische Wellen bündeln. Rechtlich darf die Sendeleistung aller Komponenten zusammengenommen in Deutschland 100mW (=20dBm) EIRP (bei 2,4 GHz) bzw. 1000 mW EIRP (bei 5,7 GHz mit TPC und DFS) nicht übersteigen. Es besteht keine Meldepflicht. Der Betreiber trägt die Verantwortung, dass seine Anlage die vorgeschriebenen Grenzwerte nicht überschreitet. Es dürfen in Deutschland uneingeschränkt auch selbstgebaute Antennen verwendet werden; hierfür ist keine Amateurfunklizenz notwendig, da die Regulierungsbehörde für Telekommunikation und Post (RegTP, früher Bundespost, BAPT) und heute Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen, die entsprechenden Frequenzbereiche in einer Allgemeinzuteilung lizenzfrei gestellt hat.

Berechnet wird die Sendeleistung (in dBm) eines WLAN-Gerätes aus:

+ Sendeleistung (dBm)
+ Gewinn Verstärker (dB) (falls vorhanden)

- Dämpfung Kabel (dB)
- Dämpfung Stecker (dB)
- Dämpfung Blitzschutz (dB)
+ Gewinn Antenne (dBi)

= Gesamtsendeleistung

Berechnet wird lediglich der Sendeweg. Für den Empfangsweg wurden von Seiten des Gesetzgebers keine Beschränkungen erlassen.

Einige WLAN-Geräte beherrschen auch Antenna Diversity-Modes, bei denen die durch Interferenzen verursachten Fehler verringert werden, indem zwei Antennen *gleichzeitig* zum Empfang bzw. *abwechselnd* zum Senden verwendet werden.

WDS Bridging und Repeating

Manche Access-Points (APs) bieten die Möglichkeit, in einen "Bridging-/Repeating-Modus" zu wechseln. Hierbei können zwei oder mehrere APs zu einem Verbund zusammengeschaltet werden. Diese Verschaltung findet auf der Ebene der MAC-Adresse (Schicht 2 im OSI-Modell) statt. Im Betrieb als Bridge (Brücke), bei dem zwei APs zusammengeschlossen werden, ohne dass weitere Clients Zugang erhalten, dienen die APs sozusagen als Ersatz eines Kabels (Point-to-Point-Verbindung). Im Repeating-Modus (Point-to-Multi-Point) werden mehrere Access Points miteinander verbunden, und zusätzlich können sich Clients wie Laptops verbinden. Damit kann man die Reichweite eines einzelnen WLAN-Netzes erhöhen. Diese Funktionalität wird Wireless Distribution System (WDS) genannt. Es handelt sich jedoch nicht um eine Hersteller-übergreifende Norm, sodass es nicht gewährleistet ist, dass zwei Geräte unterschiedlicher Hersteller sich verständigen können.

Nachteile:

1. Für jeden zusätzlichen AP im Bridging-Mode halbiert sich die Übertragungsleistung, da die Daten über den gleichen Kanal geschickt werden und für jeden AP erneut geschickt werden müssen. Bei Geräten, die mehrerer Standards unterstützen (zum Beispiel IEEE 802.11b und g), kann die WDS-Bridge auf 802.11g laufen und die Clients auf IEEE 802.11b. Somit reduziert sich die Datenrate für die Clients an einem AP nicht und zwischen Clients von verschiedenen APs nur minimal.

2. Als Verschlüsselung ist nur WEP möglich, da keine dynamisch verteilten Schlüssel möglich sind.

Gesellschaftliches

In bestehenden Netzen sind die Endverbraucher um große Provider versammelt, über die der Datenverkehr relativ zentral abgewickelt wird, was die großen Provider in eine mächtige Position bei der Kontrolle des Datenverkehrs erhebt. Der Benutzer tritt hier relativ konsumorientiert am Rande der Netzwerke auf.

NETGEAR Funknetzkarte für Notebook

Durch Wegfall der Kosten einer teuren kabelgebundenen Infrastruktur können Bürgerschaften mit dieser Technik öffentliche Netze errichten. Bildlich wird gerne das Entstehen einer Datenwolke im Äther als frei verfügbares Allgemeingut über einer Gemeinde, geschildert. Ihr volles Potential entwickelt diese Idee durch Protokolle für Mesh-Netze (MANET, Mobiles Ad-hoc-Netzwerk).

Es gibt seit wenigen Jahren weltweit lokale Initiativen in dieser Richtung. Eine deutsche Anlaufstelle ist zum Beispiel http://www.freifunk.net.

Frequenzen

Überblick über die Frequenzbänder

Es gibt mittlerweile mehrere WLAN-Frequenzbänder, die teilweise auf völlig unterschiedlichen Frequenzen arbeiten:

Standard	Frequenzen	Kanäle
IEEE 802.11a	5.15 GHz bis 5.725 GHz	Kanäle: 19, alle überlappungsfrei, in Europa mit TPC und DFS nach 802.11h
IEEE 802.11b	2.4 GHz bis 2.4835 GHz	Kanäle: 11 in den USA / 13 in Europa / 14 in Japan. Maximal 3 Kanäle überlappungsfrei nutzbar.
IEEE 802.11g	2.4 GHz bis 2.4835 GHz	Kanäle: 11 in den USA / 13 in Europa / 14 in Japan. Maximal 3 Kanäle überlappungsfrei nutzbar.

Die Kanalbandbreite beträgt bei allen Standards zwischen 10 und 30 MHz.

Datenraten

IEEE 802.11	2 Mbps maximal
IEEE 802.11a	54 Mbps maximal
IEEE 802.11b	11 Mbps maximal
IEEE 802.11g	54 Mbps maximal
IEEE 802.11n	540 Mbps max. (Verabschiedung des Standards voraussichtlich 2006)
802.11b+	44 Mbps max. (nicht standardisiert, Hersteller-gebunden)

802.11a+/g+	108/125 Mbps max. (nicht standardisiert, Hersteller-gebunden)

Bei der Betrachtung der Datenraten ist allerdings zu berücksichtigen, dass sich alle Geräte im Netz die Bandbreite teilen. Weiterhin sind die angegebenen Datenraten Bruttowerte und selbst unter optimalen Bedingungen liegt die erreichbare Netto-Datenrate nur wenig über der Hälfte dieser Angaben.

Kanal	Frequenz	Bemerkung
1	2.412 MHz	Europa, USA, Japan; keine Überschneidung
2	2.417 MHz	Europa, USA, Japan;
3	2.422 MHz	Europa, USA, Japan;
4	2.427 MHz	Europa, USA, Japan;
5	2.432 MHz	Europa, USA, Japan;
6	2.437 MHz	Europa, USA, Japan; keine Überschneidung
7	2.442 MHz	Europa, USA, Japan;
8	2.447 MHz	Europa, USA, Japan;
9	2.452 MHz	Europa, USA, Japan;
10	2.457 MHz	Europa, USA, Japan;
11	2.462 MHz	Europa, USA, Japan; keine Überschneidung
12	2.467 MHz	Europa, Japan;
13	2.472 MHz	Europa, Japan;
14	2.484 MHz	Japan;

Literatur

- Martin Sauter, Grundkurs Mobile Kommunikationssysteme, September 2004, ISBN 3-528-05886-2, http://www.cm-networks.de
- Jörg Roth: *Mobile Computing*. dpunkt, Berlin 2002, ISBN 3898641651
- Armin Medosch: *Freie Netze – Geschichte, Politik und Kultur offener WLAN-Netze*. Heise, Hannover 2004, ISBN 3936931100 (Das Buch steht unter einer Creative Commons-Lizenz und kann als PDF-Datei heruntergeladen werden)
- Ulf Buermeyer: *Der strafrechtliche Schutz drahtloser Computernetzwerke (WLANs)*. In: HRRS. Heft 8/2004. S. 285
- Mike Radmacher: *Sicherheits- und Schwachstellenanalyse entlang des Wireless-LAN-Protokollstacks* (als PDF)
- Thomas Otto: *Netzwerkauthentifizierung im WLAN, TU Braunschweig, April 2004* (als PDF)

Siehe auch

- IEEE 802.11 für technische Details zu Frequenzbändern, Übertragungsraten etc.
- HIPERLAN und HomeRF – Alternative Standards

- Wireless Access Point, Hotspot, Bluetooth, Wireless Adapter, Freie Funknetze, SSID, WLAN-Sniffer, Wardriving, WiMAX, WMAN, Wireless mesh network

Weblinks

- Umfangreiche Infos zu WLAN, Standards, FAQ und Chipsätzen
- WLAN-Richtfunk
- kleine WLAN FAQ (PDF)
- Freie WLAN Bürgernetze
- Techpaper: gut zu lesende Hintergrundinformationen zu den Verschlüsselungs- und Authentifizierungsmechanismen (Zu empfehlen: TP-WLAN-80211i-DE.pdf)
- Frequenzbänder
- EICAR Task Force on Wireless LAN Security Zusammenschluss unterschiedlichster Interessenvertretungen (englisch)
- Kostenlose WLAN-Hotspots in Deutschland

Von "http://de.wikipedia.org/wiki/Wireless_LAN"

Einordnung: WLAN | Funktechnik

Hauptautoren:
- Magnus Manske
- MR
- Dick Tracy
- Neuroposer
- Captain Crunch