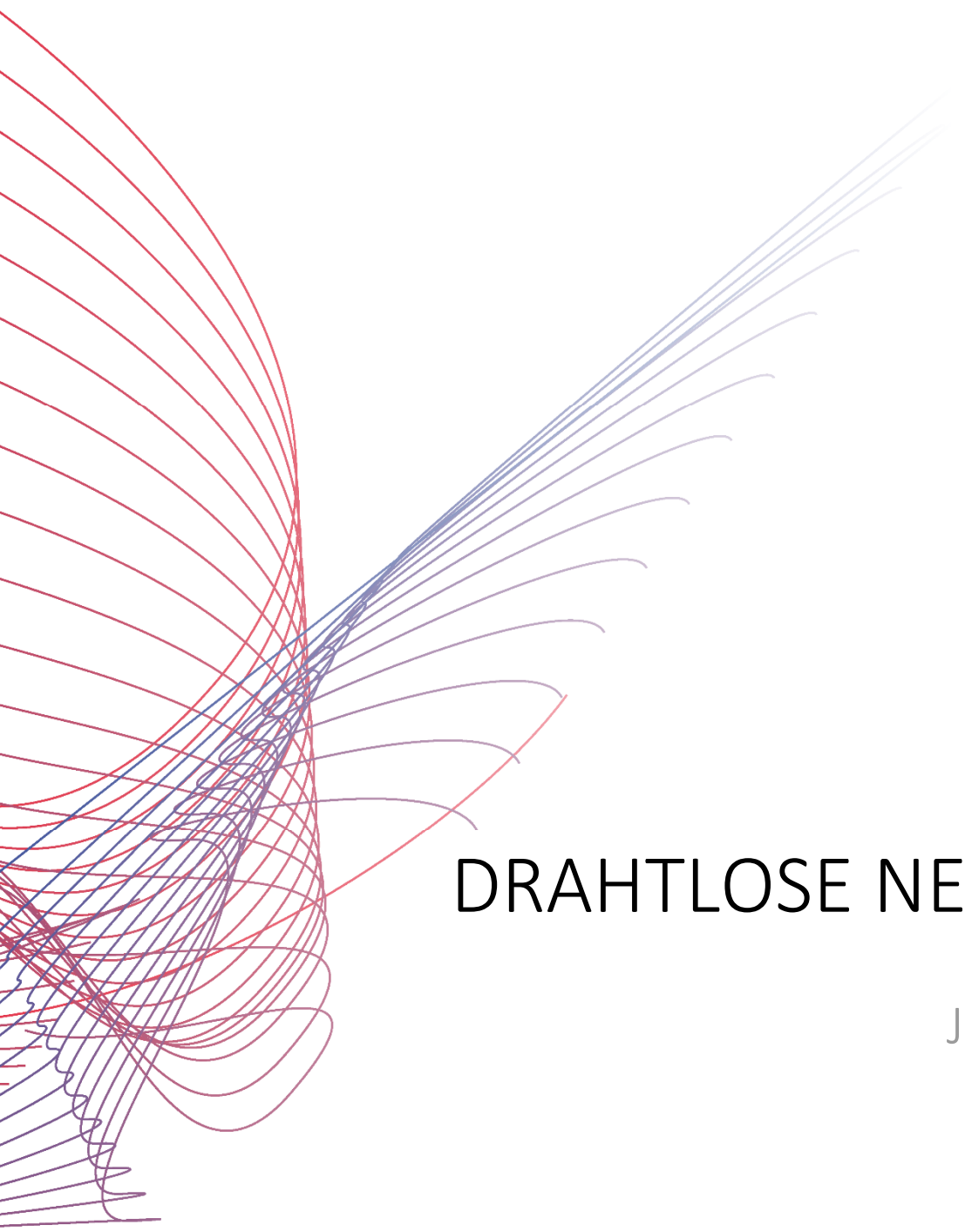
en cs de sk es

TECH pedia



DRAHTLOSE NETZWERKE

JORDI SALAZAR

Titel der Arbeit: Drahtlose Netzwerke
Author: Jordi Salazar
Übersetzt (von): Alena Dvořáková
Veröffentlicht (von): Czech Technical University of Prague
Faculty of electrical engineering
Kontaktadresse: Technicka 2, Prague 6, Czech Republic
Tel.: +420224352084
Drucken: (nur elektronisch)
Anzahl der Seiten: 38
Ausgabe: Testversion

TechPedia
European Virtual Learning Platform for
Electrical and Information Engineering

http://www.techpedia.eu

Erasmus+

Dieses Projekt wurde mit Unterstützung der Europäischen Kommission finanziert. Die Verantwortung für den Inhalt dieser Veröffentlichung (Mitteilung) trägt allein der Verfasser; die Kommission haftet nicht für die weitere Verwendung der darin enthaltenen Angaben.

ERLÄUTERUNG

	Definition(en)
	Interessantheit (Interessantes)
	Bemerkung
	Beispiel
	Zusammenfassung
	Vorteile
	Nachteile

ZUSAMMENFASSUNG

Dieses Modul bietet eine aktuelle Übersicht der drahtlosen Netzwerke im Allgemeinen und der drahtlosen LAN-Netzwerke im Besonderen. Es beschreibt die Grundlagen der verschiedenen drahtlosen Technologien, ihre Hauptcharakteristiken, die Sicherheitsproblematik sowie Vor- und Nachteile und Anwendungen.

ZIELE

Das Modul konzentriert sich auf Spezifika und Unterschiede der Netzwerkarchitekturen verschiedener Typen der drahtlosen Technologien. Desweiteren behandelt es die Sicherheitsaspekte der drahtlosen Netzwerke und stellt Vor- und Nachteile der drahtlosen Netzwerke vor.

LITERATUR

[1] STALLINGS, W.: *Wireless Communications and Networks*, Second Edition, Pearson Prentice Hall, Upper Saddle River, NJ, 2005. ISBN 0-13-191835-4.

[2] CIUBOTARU, B.; MUNTEAN, G. M.: *Advanced Network Programming. Principles and Techniques*, Springer-Verlag London, 2013. ISBN 978-1-4471-5292-7.

[3] SHARMA, K.; DHIR, N.: *A study of wireless networks: WLANs, WPANs, WMANs, and WWANs with comparison*, International Journal of Computer Science and Information Technologies, Vol. 5 (6), S. 7810-7813, 2014.

[4] POTHUGANTI, K.; CHITNENI, A.: *A comparative study of wireless protocols: Bluetooth, UWB, ZigBee, and Wi-Fi*, Advance in Electronic and Electric Engineering, Vol. 4 (6), S. 655-662, 2014.

[5] *An introduction to Wi-Fi*, Rabbit product manual, Digi International Inc., 2007-2008. (www.rabbit.com)

[6] Webseite von IEEE Standards Association (http://standards.ieee.org/index.html) [online].

Inhaltsverzeichnis

1 Einführung in drahtlose Netzwerke

Dieses Modul bietet eine Einführung in drahtlose Netzwerke im Allgemeinen und drahtlose **LAN**-Netzwerke (*lokale Netzwerke*, engl. *Local Area Network*) im Besonderen. Es beschreibt und erklärt die Grundlagen der verschiedenen drahtlosen Technologien, ihre Hauptcharakteristiken, die Sicherheitsproblematik sowie Vor- und Nachteile und Anwendungen.

Drahtlose Netzwerke verwenden Radiowellen für die Verbindung der Endgeräte und benötigen keinerlei Verkabelung.

Geräte, die üblicherweise in drahtlosen Netzwerken verwendet werden, können tragbare Computer, Desktop-Rechner, **PDA** (engl. *Personal Digital Assistant*), Handys, Tablets und Pager sein. Drahtlose Netzwerke arbeiten ähnlich wie Festnetze, jedoch müssen drahtlose Netzwerke die übertragenen Signale in eine Form umwandeln, die für eine Übertragung durch den freien Raum geeignet ist.

Drahtlose Netzwerke dienen vielen Zwecken. In einigen Fällen werden sie als Kabelersatz verwendet, können aber auch den externen Zugriff auf Unternehmensdaten ermöglichen.

Die drahtlose Infrastruktur kann im Vergleich zu klassischen Festanschlüssen mit einem sehr niedrigen Aufwand aufgebaut werden. Dies führt nicht nur zu Kosteneinsparungen. Durch einen billigeren und einfacheren Zugriff auf Informationen können die angeschlossenen Teilnehmer alle Vorteile des Internetzugangs nutzen. Dies spart Zeit und Aufwand.

Drahtlose Netzwerke ermöglichen einen problemlosen Anschluss entfernter Geräte unabhängig davon, ob sie vom Zugriffspunkt einige Meter oder sogar einige Kilometer entfernt sind. Es ist auch nicht erforderlich, für die Verkabelung Wände zu durchbrechen oder Steckverbinder zu installieren. Diese Merkmale haben den Einsatz von drahtlosen Technologien sehr beliebt gemacht und beschleunigen ihre Massenverbreitung.

In drahtlosen Netzwerken werden viele unterschiedliche Technologien genutzt, die sich in den verwendeten Übertragungsfrequenzen, -raten und -reichweiten unterscheiden.

Dabei muss man jedoch spezifische rechtliche Fragen in Betracht ziehen, die die gesetzlichen Vorschriften des elektromagnetischen Spektrums betreffen. Elektromagnetische Wellen werden von verschiedensten Gerätetypen gesendet, dabei ist ihr Betrieb sehr störungsempfindlich. Deshalb brauchen alle Länder gesetzliche Regulierungen und verbindliche Empfehlungen, zur Definition der erlaubten Frequenzbereiche und Übertragungsleistungen für die einzelnen Technologien.

Außerdem sind elektromagnetische Wellen nicht einfach geographisch begrenzbar. So können Hacker den Datenverkehr abhören, wenn die übertragenen Daten nicht ordnungsgemäß verschlüsselt werden. Deshalb sollten die drahtlos übertragenen Informationen geschützt werden.

2 Drahtlose Technologien

Drahtlose Netzwerke können in vier spezifische Gruppen gemäß Anwendungsbereich und Signalreichweite eingeteilt werden [1-3]: **WPAN**-Netzwerke (*drahtloses persönliches Netzwerk*, engl. *Wireless Personal Area Network*), **WLAN**-Netzwerke (*drahtloses lokales Netzwerk*, engl. *Wireless Local Area Network*), **WMAN**-Netzwerke (*drahtloses städtisches Netzwerk*, engl. *Wireless Metropolitan Area Network*) und **WWAN**-Netzwerke (*Weitverkehrsfunknetz*, engl. *Wireless Wide Area Network*). Das Bild 1.1 zeigt diese vier Kategorien und Beispiele einiger Technologien in dem gegebenen Netzwerktyp.

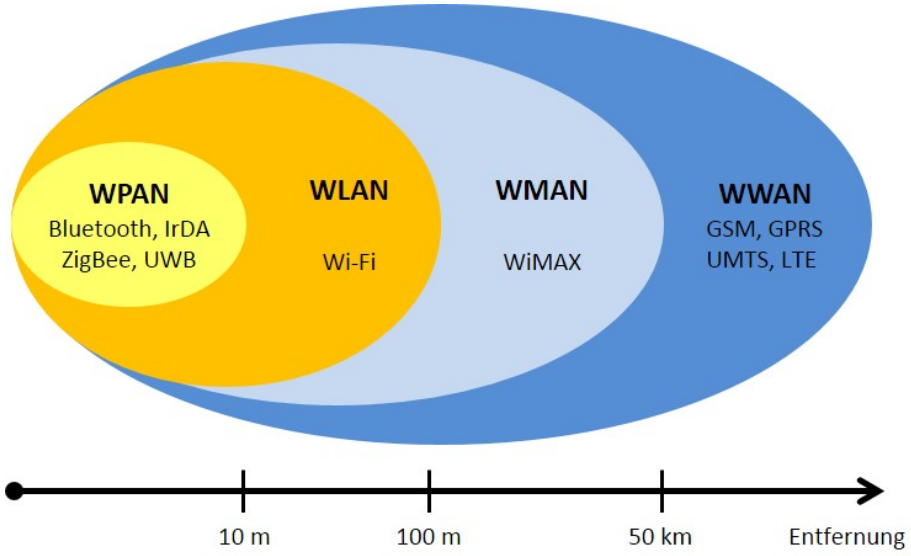


Bild 1.1 Klassifikation drahtloser Netzwerke mit Beispielen der verwendeten Technologien

Außerdem können drahtlose Netzwerke auch gemäß ihrer Reichweite in zwei breite Segmente unterteilt werden: Kurzstrecken- (engl. **SR**, *short-range*) und Langstreckennetze (engl. **LR**, *long-range*). Drahtlose Kurzstreckennetze sind für eine begrenzte Reichweite konzipiert. Das betrifft vor allem drahtlose **LAN**-Netzwerke (engl. *Local Area Network*), die man beispielsweise in Firmengebäuden, auf Schulgeländen, in Fertigungsanlagen oder in Privathaushalten finden kann, aber auch **PAN**-Netzwerke (engl. *Personal Area Network*), dank derer tragbare Geräte in der näheren Umgebung miteinander kommunizieren können. **WPAN**-Netzwerke verwenden üblicherweise unlizenzierte Frequenzbänder **ISM** (engl. *Industrial, Scientific and Medical*), die für industrielle, wissenschaftliche und medizinische Zwecke reserviert sind. Die verfügbaren Frequenzen unterscheiden sich in verschiedenen Ländern. Oft genutzte Frequenzbänder sind Bänder um 2,4 GHz und 5 GHz, die in den meisten Staaten zur Verfügung stehen. Die Verfügbarkeit dieser Frequenzen ermöglicht es den Benutzern, drahtlose Netzwerke ohne eine Lizenz und kostenlos zu betreiben. Dadurch wurde die Verbreitung dieser Netzwerke gefördert.

In Langstreckennetzen wird Konnektivität typischerweise von Firmen realisiert, die drahtlosen Internetzugang als eine Dienstleistung anbieten. Diese Netze decken

große Gebiete ab, wie zum Beispiel Metropolen (WMAN), Stadtbezirke, Bundesländer oder ein ganzes Land. Die Hauptaufgabe der Langstreckennetze ist daher eine globale Sicherstellung von drahtlosen Verbindung. Das verbreitetste Langstreckennetz ist **WWAN**. Wird jedoch globale Abdeckung erforderlich, stehen Satellitennetze zur Verfügung.

2.1 Drahtlose persönliche Netzwerke (WPAN)

Drahtlose persönliche Netzwerke basieren auf dem IEEE 802.15 [http://en.wikipedia.org/wiki/IEEE_802.15] -Standard [3-4]. Ihre Konzeption erlaubt die Kommunikation über sehr kurze Entfernungen von etwa 10 Metern. Im Unterschied zu anderen drahtlosen Netzwerken brauchen **WPAN** nur geringe oder gar keine Infrastruktur. Damit können leistungsfähige und billige Lösungen für eine breite Skala von Geräten, wie zum Beispiel Smartphones und **PDA** realisiert werden.

WPAN-Netzwerke werden durch einen niedrigen Energiebedarf und eine niedrige Übertragungsrate charakterisiert. Dieser Netztyp nutzt Technologien wie Bluetooth, **IrDA** (*Infrared Data Association*), ZigBee oder **UWB** (*Ultrabreitband*, engl. *Ultra Wide Band*). Bluetooth ist für Geräte wie schnurlose Mäuse, Tastaturen und Freisprechanlagen bestimmt. **IrDA** eignet sich für Punkt-zu-Punkt-Verbindungen zwischen zwei Geräten zur einfachen Datenübertragung und Dateisynchronisierung. ZigBee wurde für die zuverlässige drahtlose Überwachung des Zustandes des Netzwerkes und seiner Steuerung entworfen und **UWB** wird für breitbandige Multimedia-Verbindungen genutzt.

Die Bitrate ist die Anzahl von übertragenen oder empfangenen Bits pro Zeiteinheit (*bps* oder *bit/s)*.

Ein Modem ist ein Gerät, das einem Rechner das Senden und den Empfang von Daten ermöglicht.

Bluetooth

Die Bluetooth-Technologie basiert auf dem Standard IEEE 802.15.1. Ursprünglich wurde Bluetooth für die Kommunikation mit einem niedrigen Energieverbrauch, einer kurzen Reichweite und Senden in alle Richtungen (*Punkt-zu-Mehrpunkt*) für billige Geräte als Kabelersatz entwickelt. Es verbindet die Geräte mittels Ad-Hoc-Netzen. Zurzeit werden Bluetooth-Komponenten und -Systeme für eine Reihe von neuen Anwendungen entworfen. Bluetooth spezifiziert drei unterschiedliche Geräteklassen: *Klasse 1* (Reichweite bis zu 100 Metern), *Klasse 2* (Reichweite bis zu 10 Metern) und *Klasse 3* (Reichweite bis zu 1 Meter). Bei einem Band von 2,4 GHz können zwei Geräte innerhalb ihres Signalabdeckungsbereichs bis zu 720 kbit/s ihrer Kapazität oder Übertragungsrate teilen. Die meistbenutzte Klasse ist die *Klasse 2*.

Ein Bluetooth-Netz wird auch als Piconetz bezeichnet und besteht aus bis zu 8 aktiven *Master-Slave*-Geräten. Das erste Bluetooth-Gerät im Piconetz ist der *Master*, alle weiteren Geräte sind *Slaves*, die im Netz mittels des *Masters* kommunizieren. Ein Piconetz hat typischerweise eine Reichweite von 10 Metern, unter idealen Bedingungen können jedoch auch Reichweiten von bis zu 100 Metern erzielt werden. Aus Sicherheitsgründen werden alle Verbindungen verschlüsselt und gegen Abhören und Störung geschützt. Zwei Piconetze können in einem

Scatternet verbunden werden. Ein Bluetooth-Gerät kann zugleich an mehreren Piconetzen angeschlossen sein und hat damit die Möglichkeit, dass Informationen über die Reichweite eines einzigen Piconetzes hinaus fließen können. Ein Gerät im Scatternet kann als *Slave* in mehreren Piconetzen, jedoch als *Master* nur in einem Piconetz arbeiten.

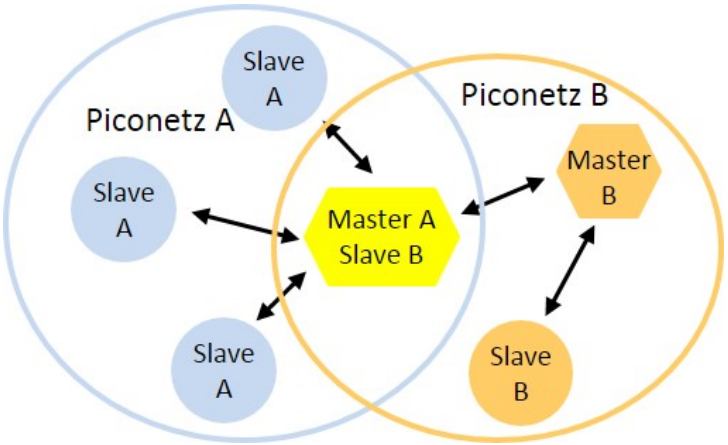


Bild 1.2 Bluetooth-Scatternet mit zwei Piconetzen. Der Master im Piconetz A ist ein Slave im Piconetz B.

IrDA

Die Assoziation **IrDA** spezifiziert einen kompletten Satz von infraroten Kommunikationsstandards. **IrDA** standardisiert drahtlose Verbindungen von Geräten, die normalerweise durch Kabel verbunden werden. **IrDA** hat einen niedrigen Energieverbrauch, geringe Kosten und einen schmalen Ausgangswinkel (< 30º). Sie stellt unidirektionale Verbindungen (*Punkt-zu-Punkt*) für Ad-Hoc-Netze mit einer Reichweite von bis zu 1 Meter und Übertragungsraten von 9600 bit/s bis zu 4 Mbit/s (zurzeit) bzw. 16 Mbit/s (in Entwicklung) bereit. Geräte, die **IrDA** verwenden, sind beispielsweise Notebooks, **PDA**, Drucker und Kameras.

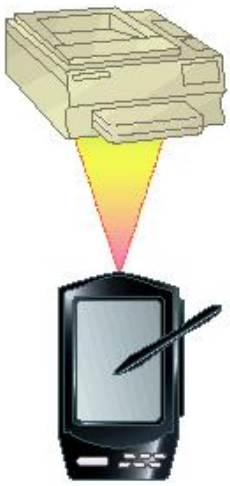


Bild 1.3 IrDA-Kommunikation zwischen PDA und Drucker (Punkt-zu-Punkt)

ZigBee

Die Technologie ZigBee beruht auf dem Standard IEEE 802.15.4 und wurde als ein offener globaler Standard entwickelt, um besondere Bedürfnisse von drahtlosen Netzwerken mit einer einfachen Implementierung und einer hoher Zuverlässigkeit zu erfüllen. Dabei sind Kosten, Energieverbrauch und Übertragungsrate gering. ZigBee arbeitet in unlizenzierten Bändern bis einschließlich 2,4 GHz, 900 MHz und 868 MHz mit einer maximalen Übertragungsrate von bis zu 250 kbit/s, die für drahtlose Übertragungen in Sensoren- und Automatisierungssystemen ausreichend ist.

ZigBee dient auch zum Aufbau großer drahtloser Netzwerke, die keinen hohen Datendurchsatz erfordern. In einem ZigBee-Netz können zwei unterschiedliche Gerätetypen arbeiten – völlig funktionsfähige Geräte **FFD** (engl. *Full-Function Device*) und Geräte mit begrenzten Funktionen **RFD** (engl. *Reduced-Function Device*). **FFD**-Geräte können in drei unabhängigen Modi arbeiten: als **WPAN**-Koordinator, als allgemeiner Koordinator (*ZigBee-Router*) oder als Endgerät. **RFD**-Geräte sind für sehr einfache Anwendungen bestimmt, beispielsweise Lichtschalter. ZigBee unterstützt drei unterschiedliche Netztopologien: Stern, Mesh und *Cluster-Baum* (siehe Bild 1.4). In der Sterntopologie wird die Kommunikation zwischen Geräten und dem zentralen Controller (**WPAN**-Koordinator) aufgenommen. In der Mesh-Topologie kann jedes Gerät mit einem anderen Gerät kommunizieren, solange sich jedes innerhalb der Reichweite des anderen befindet. Ein Cluster-Baum-Netzwerk stellt einen Sonderfall des Mesh-Netzwerkes dar, in dem die meisten Geräte **FFD** sind, **RFD**-Geräte können an das Cluster-Baum-Netzwerk als Endgeräte ohne Möglichkeit weiterer Gabelung angeschlossen werden. Jedes **FFD**-Gerät kann als Router arbeiten und die Synchronisierung für weitere Geräte und Router sicherstellen. Nur einer dieser Router ist jedoch **WPAN**-Koordinator.

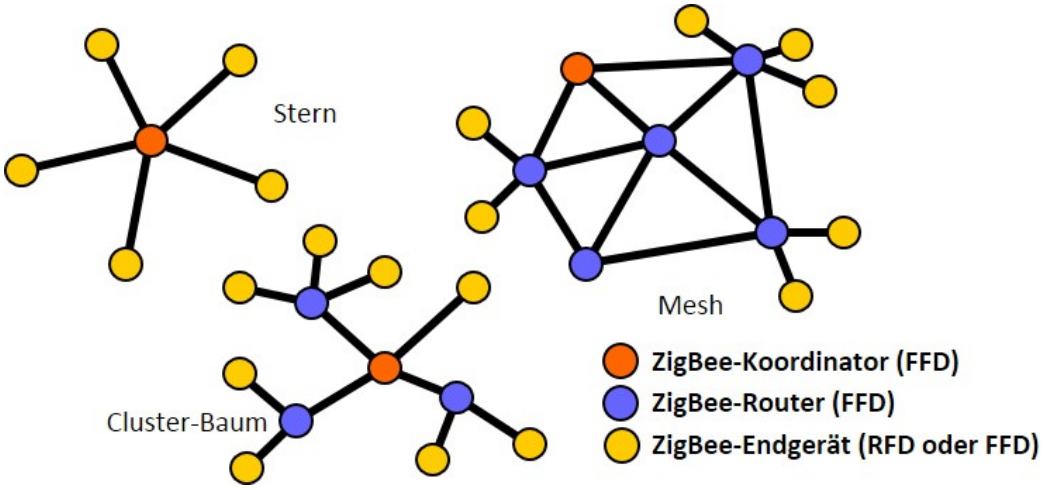


Bild 1.4 Struktur eines ZigBee-Netzwerkes

UWB

Die Technologie **UWB**, die auf dem Standard IEEE 802.15.3 basiert, wird für drahtlose Hochgeschwindigkeits-Kommunikation mit einer kurzer Reichweite in

Innenräumen (z. B. Gebäuden, Haushalte) genutzt. Im Unterschied zu den anderen hier genannten Technologien verfolgt **UWB** einen anderen Zweck. **UWB** ermöglicht die Übertragung von großen Dateien mit hohen Übertragungsraten über kurze Entfernungen. Die Technologie **UWB** erreicht Datenübertragungsraten von 110 Mbit/s bis 480 Mbit/s über Entfernungen von bis zu einigen Metern, was den Bedarf der meisten Multimediaanwendungen, wie Audio- und Videoanwendungen für Haushalte, abdecken kann. Sie kann auch als drahtloser Kabelersatz eines seriellen Hochgeschwindigkeits-Busses, wie USB 2.0 oder IEEE 1394 dienen. In Amerika wurde für **UWB** das Frequenzband ab 3,1 GHz bis 10,6 GHz reserviert. In Europa hat das Frequenzband zwei Teile: von 3,4 GHz bis 4,8 GHz und von 6 GHz bis 8,5 GHz.

Übertragungen mittels **UWB** geschehen durch Generieren eines Funksignals in gewissen Zeitintervallen, womit jedoch eine große Breite des Frequenzbandes besetzt wird (siehe Bild 1.5). So ermöglichen sie Pulsposition- oder Pulsweitenmodulation. Die Informationen können an UWB-Signale (Pulse) durch Verschlüsselung der Pulspolarität, -amplitude und/oder mittels orthogonaler Pulse moduliert werden. UWB-Pulse senden sporadisch mit einer relativ niedrigen Pulsrate, um die Puls- oder Positionsmodulation zu unterstützen, aber sie können auch mit Raten gesendet werden, die proportional zu der für die **UWB**-Pulse reservierten Bandbreite sind.

Bild 1.5 Gebrauch von UWB-Leistung und -Frequenzbandbreite

2.2 Drahtlose lokale Netzwerke (WLAN)

Drahtlose lokale Netzwerke (**WLAN**) wurden so entworfen, dass sie den Zugriff in einer Reichweite von bis zu 100 Metern erlauben, und werden am häufigsten in Haushalten, Schulen, Computerlabors oder Büros angewandt (siehe Bild 1.6). Damit hat der Benutzer die Möglichkeit, sich in einem bestimmten Gebiet zu bewegen und gleichzeitig wird noch eine Verbindung zum Netzwerk sichergestellt [2,5]. **WLAN** beruht auf den Standard IEEE 802.11, der mit dem Markennamen **Wi-Fi** (engl. *Wireless Fidelity*) bezeichnet wird. Dank seiner großen Verbreitung wurden keine anderen Standards, wie z. B. HiperLAN, kommerziell realisiert. Die Standards IEEE 802.11 waren einfacher implementierbar und gelangten schneller auf den Markt. Die ganze Familie dieser Standards wird in Sektion 4 dieses Moduls detailliert behandelt.

IEEE 802.11 ist eine Gruppe von Standards für drahtlose lokale Netzwerke. Der Standard IEEE 802.11b war der erste anerkannte Standard dieser Gruppe und unterstützt Datenübertragungen mit Raten bis zu 11 Mbit/s im unlizenzierten Band von 2,4 GHz. Als Nachfolger des IEEE 802.11b wurde der Standard IEEE 802.11g erstellt, der für Übertragungen ein erweitertes Frequenzband verwendet. Ein auf IEEE 802.11g basierender Knoten unterstützt Klienten sowohl von 802.11b als auch von 802.11g. Ähnlich kann auch ein Laptop mit einer Karte für IEEE 802.11g Verbindungen über 802.11b aufbauen. Der Grund ist, dass drahtlose **LAN** mit dem Standard 802.11g das gleiche unlizenzierte Band von 2,4 GHz wie 802.11b verwenden. Die maximale Übertragungsrate für IEEE 802.11g beträgt 54 Mbit/s, aber sie wird automatisch reduziert, wenn das Funksignal schwach ist oder eine Störung erkannt wird.

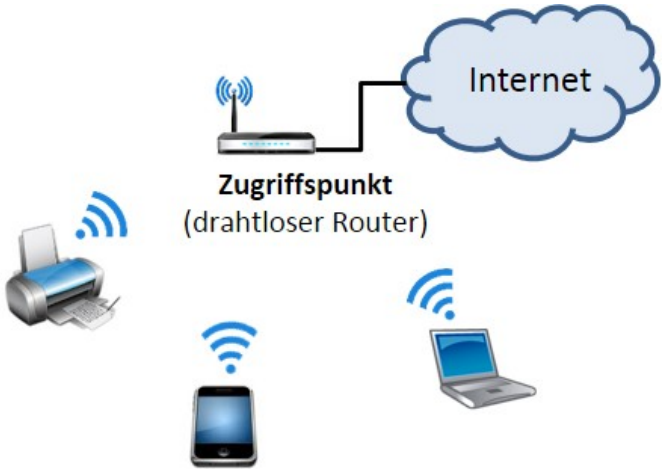


Bild 1.6 WLAN im Haushalt

2.3 Drahtlose städtische Netzwerke (WMAN)

Drahtlose städtische Netzwerke **WMAN** sind die dritte Gruppe von drahtlosen Netzwerken. **WMAN** basieren auf dem Standard IEEE 802.16, der häufig als **WiMAX** (engl. *Worldwide Interoperability for Microwave Access*) bezeichnet wird. **WiMAX** ist eine Kommunikationstechnologie, die eine Punkt-zu-Mehrpunkt-Architektur (*Point-to-Multipoint*) mit Orientierung auf drahtlose Hochgeschwindigkeitsdatenübertragung in städtischen Netzwerken unterstützt [1-3]. Dies ermöglicht es kleineren drahtlosen **LAN**, mittels **WiMAX** verbunden zu werden und damit ein weites **WMAN** zu schaffen. So können Netzwerke zwischen Städten ohne eine aufwendige Verkabelung geschaffen werden.

WiMAX ähnelt **Wi-Fi**, bietet aber die Abdeckung eines viel größeren Gebietes. **Wi-Fi** ist zur Abdeckung von relativ kleinen Gebieten, beispielsweise Büros oder Hot Spots, bestimmt - dagegen arbeitet **WiMAX** in zwei Frequenzbändern, die eine Kombination eines lizenzierten und unlizenzierten Bandes sind. Das erste Band erstreckt sich von 2 GHz bis 11 GHz und das zweite liegt zwischen 10 GHz und 66 GHz. So kann eine Übertragungsrate von 70 Mbit/s über eine Entfernung von 50 km für Tausende Benutzer aus einer einzigen Basisstation erzielt werden (siehe Bild 1.7). Weil **WiMAX** zwei unterschiedliche Frequenzbänder verwendet, kann sie sowohl für Line-of-Sight-Systeme als auch für Systeme eingesetzt werden, die keine direkte Sichtverbindung erfordern. Das Band von 2 GHz bis 11 GHz kann für Systeme ohne direkte Sichtverbindung ausgenutzt werden, beispielsweise für die Kommunikation eines Computers in einem Gebäude mit einem Turm oder einer Antenne außerhalb des Gebäudes. Die Übertragungen auf diesen Frequenzen werden von physischen Hindernissen kaum unterbrochen. Dagegen werden die Frequenzen im Band von 10 GHz bis 66 GHz für Line-of-Sight-Systeme verwendet. Damit ist auch über größere Entfernungen eine Kommunikation zwischen Türmen und Antennen möglich.

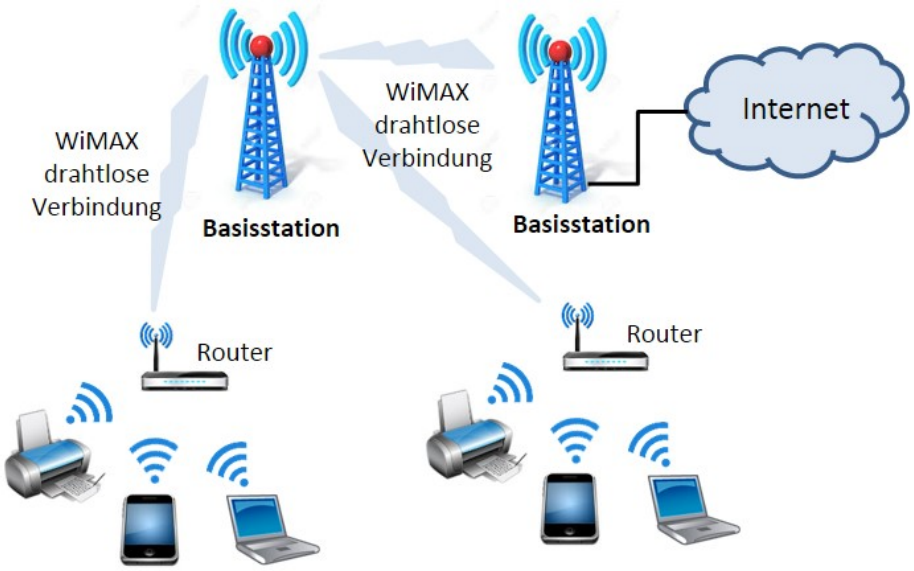


Bild 1.7 WiMAX-Netzwerk

2.4 Weitverkehrsfunknetze (WWAN)

Weitverkehrsfunknetze **WWAN** erstrecken sich über 50 Kilometer und verwenden typischerweise lizenzierte Frequenzen. Dieser Netzwerktyp deckt umfangreiche Gebiete ab, wie z. B. Städte oder Länder, und zwar mittels mehrfacher Satelliten- oder Antennensysteme, die von einem **ISP** (*Internetdienstleister*, engl. *Internet Service Provider*) verwaltet werden. Es gibt im Wesentlichen zwei verfügbare Technologien: digitale Mobilfunksysteme und Satellitensysteme [1-3].

Mobilfunknetze

In einem Mobilfunknetz ist das abgedeckte Gebiet in Zellen aufgeteilt. Ein Sender in der Mitte der Zelle realisiert die Kommunikation der gegebenen Zelle. Alle Sender sind an eine Basisstation und die Basisstationen weiter an eine Mobilfunk-Vermittlungsstelle angeschlossen, die das Mobilfunk- und Festnetz verbindet. Das System bemüht sich um eine Wiederverwendung von Frequenzen mit einem niedrigen Energiebedarf durch die Wahl kurzer Entfernungen.

Seit 1980 wurden verschiedene Mobilfunkgenerationen entwickelt. Die erste Generation (1G) war analog und nur für Sprachanruf ohne Berücksichtigung von Datendiensten konzipiert und entworfen. Die Übertragungsrate betrug lediglich 2,4 kbit/s. Die zweite Generation (2G) basierte auf digitaler Technologie und Netzinfrastruktur **GSM** (*globales System für mobile Kommunikation*, *Global System for Mobile Communications*, früher *Groupe Spécial Mobile*). Sie hat auch Kurznachrichten **SMS** (*Kurznachrichtendienst*, engl. *Short Message Service*) ermöglicht und unterstützt eine Datenrate von bis zu 64 kbit/s. Die Generation 2,5G entstand zwischen der zweiten und der dritten Generation. Manchmal wird sie als 2G + **GPRS** (*allgemeiner paketorientierter Funkdienst*, engl. *General Packet Radio Service*) bezeichnet. Es handelt sich um eine verbesserte Version von 2G mit einer Übertragungsgeschwindigkeit von bis zu 144 kbit/s. Die dritte Generation (3G) wurde im Jahre 2000 mit einer Datenrate von bis zu 2 Mbit/s eingeführt. Die 3,5G ist eine erweiterte Version der 3G, die **HSDPA** (engl. *UMTS-Broadband* oder *High-Speed Downlink Packet Access*) verwendet und Datenübertragungsraten bis zu 14 Mbit/s realisiert. Schließlich kommt die vierte Generation (4G), die Übertragungsleistungen von 1 Gbit/s ermöglicht und alle erforderlichen Dienste unterstützt. Die fünfte Generation (5G) wird für das Jahr 2020 erwartet.

Satellitennetze

Drahtlose Kommunikation kann auch mittels Satelliten sichergestellt werden. Wegen ihrer Position über dem Erdboden können Satellitenübertragungen ein großes Gebiet abdecken. Das kann sehr nützlich für Benutzer von Satellitentelefonen sein, die sich in einer entlegenen Gegend aufhalten oder auf einer Insel befinden, wo es keinen Anschluss über ein Unterseekabel gibt.

Jeder Satellit ist mit verschiedenen Transpondern ausgestattet, die aus einem Sende-/Empfangsgerät und einer Antenne bestehen. Das Eingangssignal wird verstärkt und dann auf einer anderen Frequenz noch einmal gesendet.

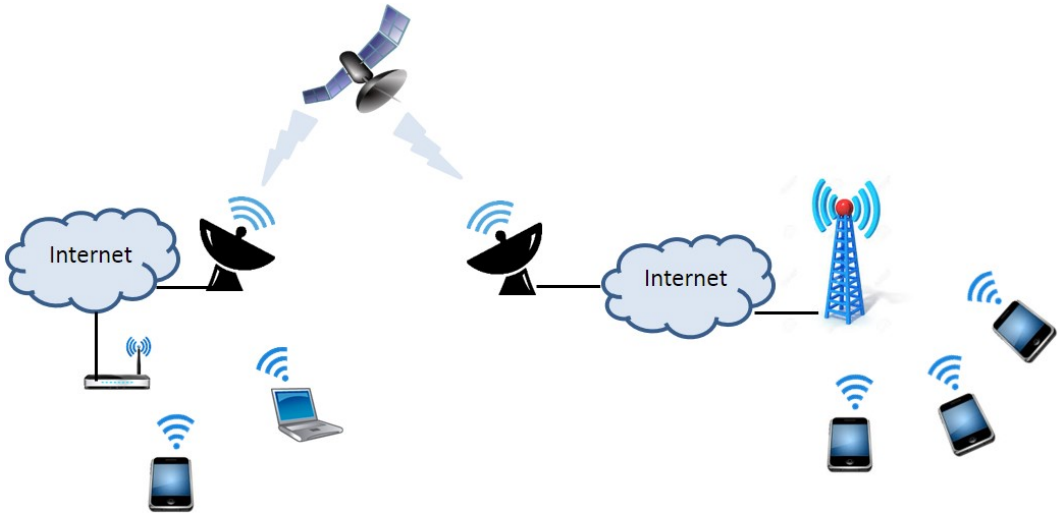


Bild 1.8 Satelliten- und Mobilfunknetze

3 Netzwerkarchitektur

3.1 Begriffe und Terminologie

Dieses Kapitel definiert verschiedene Begriffe, die in der drahtlosen Netzwerkarchitektur verwendet werden. Nicht alle Begriffe einer generischen Architektur existieren für alle Technologien und die Funktionalität kann abweichen.

Die logische Architektur gemäß IEEE 802.11 besteht aus einigen wichtigen Komponenten: Station **STA**, drahtloser Zugriffspunkt **AP** (engl. *Access Point*), unabhängiger Basisdienstleistungssatz **IBSS** (engl. *Independent Basic Service Set*), Basisdienstleistungssatz **BSS** (engl. *Basic Service Set*), Verteilungssystem **DS** (engl. *Distribution System*) und erweiterter Dienstleistungssatz **ESS** (engl. *Extended Service Set)*. Einige Komponenten der logischen Architektur gemäß IEEE 802.11 hängen direkt mit konkreten Geräten, wie Stationen **STA** und drahtlosen Zugriffspunkten **AP**, zusammen. Eine drahtlose Station **STA** hat eine Adapterkarte, eine PC-Karte oder ein anderes integriertes Gerät zur Sicherstellung der drahtlosen Verbindung. Ein drahtloser Zugriffpunkt **AP** arbeitet wie eine Brücke zwischen der drahtlosen Station **STA** und dem Backbone-Netz, um den Netzzugriff zu ermöglichen.

Eine Station **STA** kann ein klassischer **PC**, Laptop, **PDA**, Handy oder ein beliebiges Gerät mit der Fähigkeit des Zugriffs auf ein drahtloses Medium sein.

Ein Zugriffspunkt **AP**, manchmal auch Basisstation **BS** bezeichnet, ist ein Gerät, das es drahtlosen Geräten ermöglicht, sich an Festnetze mittels **Wi-Fi** oder weiterer Standards zu verbinden.

Ein Basisdienstleistungssatz **BSS** besteht aus einem Zugriffspunkt **AP** mit allen assoziierten Stationen **STA**. Ein Zugriffspunkt **AP** arbeitet als *Master*, der die Stationen innerhalb des Basisdienstleistungssatzes **BSS** steuert. Der einfachste Basisdienstleistungssatz **BSS** hat einen Zugriffspunkt **AP** und eine Station **STA**.

Ein erweiterter Dienstleistungssatz **ESS** ist ein Satz mit einem oder mehreren verbundenen Basisdienstleistungssätzen **BSS**, die aus der Sicht des logischen Aufbaus und ihrer Steuerung wie ein **BSS** auf jeder Station **STA** mit einem dieser **BSS** aussehen.

Wenn alle Stationen **STA** im **BSS** Mobilfunkstationen sind und es keinen Anschluss an das Festnetz gibt, wird der Basisdienstleistungssatz **BSS** als unabhängiger Basisdienstleistungssatz **IBSS** bezeichnet. Ein **IBSS** ist ein *Ad-Hoc-*

Netzwerk, das keine Zugriffspunkte **AP** umfasst - das heißt, dass kein Anschluss an einen anderen **BSS** möglich ist.

Ein Verteilungssystem **DS** ist ein Mechanismus, durch den die Zugriffspunkte **AP** einzelne Frames untereinander und eventuell mit dem Festnetz austauschen. **DS** muss nicht ein Netzwerk sein und der Standard IEEE 802.11 schreibt für **DS** keine konkrete Technologie vor. Fast in allen kommerziellen Produkten wird als Technologie für Backbone-Netze Kabel-Ethernet verwendet.

Bild 1.9 Unabhängiger und Infrastruktur-Basisdienstleistungssatz BSS

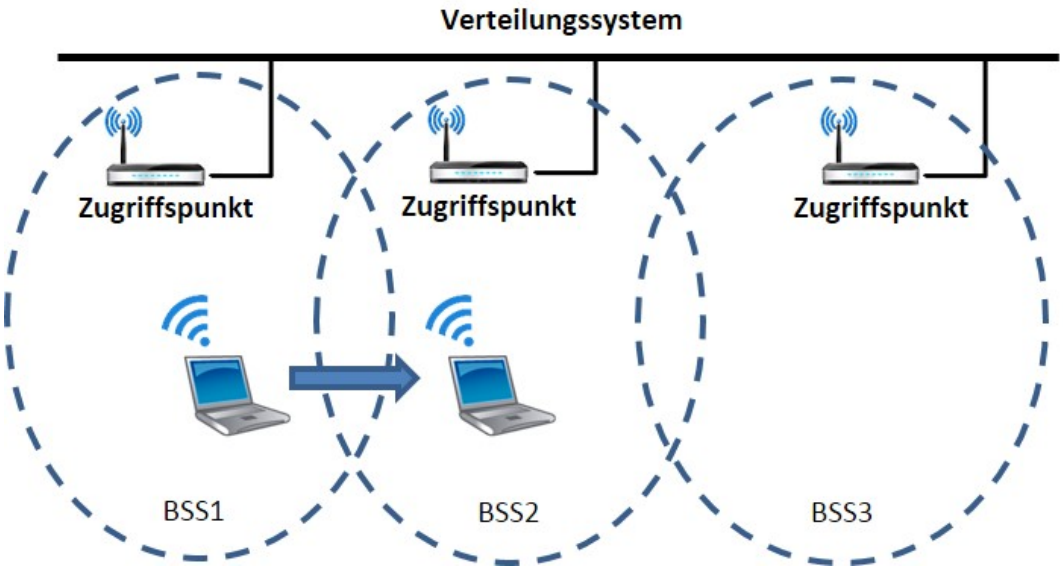


Bild 1.10 Erweiterter Dienstleistungssatz ESS und Mobilitätsunterstützung

3.2 Architekturen

In drahtlosen Netzwerken stehen zwei Modi der Konfiguration drahtloser Architekturen zur Verfügung: *Ad-hoc-Modus* und *Infrastrukturmodus* [1-2]. Beim *Ad-Hoc-Modus* tauschen Geräte die Daten direkt in Peer-to-Peer-Kommunikation aus, wobei sie beim Infrastrukturmodus über einen Zugriffspunkt **AP** kommunizieren, der als Brücke zu weiteren Netzwerken dient.

Ad-Hoc-Modus

Durch den *Ad-Hoc-Modus* kommunizieren alle Geräte im drahtlosen Netzwerk miteinander und direkt im Peer-to-Peer-Betrieb (*Punkt-zu-Punkt,* engl. *Point-to-Point*). Das Netzwerk hat keine feste Struktur oder feste Punkte. Kein Zugriffspunkt **AP** ist für die Kommunikation zwischen den Geräten erforderlich.

Der *Ad-Hoc-Modus* ist für kleine Gruppen von Geräten geeignet. Jedoch müssen sich alle Geräte physisch in unmittelbarer Nähe zueinander befinden. Die Leistung des Netzwerkes sinkt mit der steigenden Anzahl von Geräten. Häufig können zufällige Unterbrechungen einzelner Geräte auftreten. Der Ad-Hoc-Modus stellt auch hohe Anforderungen an die Netzwerkadministration. Eine weitere Einschränkung des *Ad-Hoc-Modus* ist, dass sich die Netzwerke in diesem Modus nicht direkt an lokale Festnetze anschließen lassen und dass ein Internetzugang ohne Installation von speziellen *Gateways* nicht möglich ist.

Dennoch arbeitet der Ad-Hoc-Modus in kleinen Umgebungen gut und stellt die einfachste und billigste Art des Aufbaus eines drahtlosen Netzwerkes dar.

Infrastrukturmodus

Die zweite verfügbare Architektur für drahtlose Netzwerke ist der Infrastrukturmodus. Alle Geräte werden an das drahtlose Netzwerk mittels eines Zugriffspunktes **AP** angeschlossen. Drahtlose Zugriffspunkte **AP** sind üblicherweise Router oder Switches, welche die drahtlos übertragenen Daten in Ethernetdaten von Festnetzen umwandeln und als eine Brücke zwischen **LAN**-Festnetzwerken und drahtlosen Benutzern dienen. Durch die Verbindung von mehren Zugriffspunkten mittels Fest-Backbone-Netzen auf der Basis von Ethernet kann die Reichweite der drahtlosen Netzwerke erweitert werden. Wenn sich ein mobiles Gerät aus der Reichweite eines Zugriffspunktes **AP** bewegt, gelangt es in die Reichweite eines anderen. Infolgedessen können sich drahtlos arbeitende Geräte von dem Bereich eines Zugriffspunktes zu einem anderen frei bewegen und immer noch einen übergangslosen Netzwerkanschluss haben.

Der Infrastrukturmodus bietet bessere Sicherheit, einfache Verwaltung sowie mehr Skalierbarkeit und Stabilität. Jedoch muss man beim Infrastrukturmodus mit Mehrkosten für die Implementierung von Zugriffspunkten **AP** rechnen, wie z. B. Router und Switches.

ESSID

Die **ESSID** (engl. *Extended Service Set Identification*) und die **SSID** (engl. *Service Set Identification*) bezeichnen zwei Servicetypen. In drahtlosen Ad-Hoc-Netzwerken ohne Zugriffspunkte **AP** wird die **BSSID** (engl. *Basic Service Set Identification*) verwendet. In drahtlosen Infrastrukturnetzwerken mit Zugangsknoten wird die **ESSID** verwendet, die aber vereinfacht immer noch als **SSID** bezeichnet werden kann.

Die **SSID** ist ein alphanummerischer Schlüssel mit (höchstens) 32 Zeichen zur Identifikation des drahtlosen lokalen Netzwerkes.

Einige Verkäufer verwechseln die **SSID** mit dem Namen des Netzwerkes. Um die gegenseitige Kommunikation von drahtlosen Geräten in einem Netzwerk zu ermöglichen, müssen alle Geräte mit der gleichen **SSID** konfiguriert werden.

4 Standard IEEE 802.11

Der Standard IEEE 802.11 umfasst Spezifikationen für die Medienzugriffssteuerung **MAC** (engl. *Medium Access Control*) und die Bitübertragungsschicht **PHY** (engl. *Physical Layer*) zur Implementation von drahtlosen lokalen Netzwerken in Frequenzbändern von 2,4, 5 und 60 GHz [1-2].

Diese Spezifikationen werden von der Arbeitsgruppe IEEE 802.11 erstellt und verwaltet. Die erste Version des Standards wurde 1997 veröffentlicht und später verbessert. Der Standard und seine Verbesserungen bilden die Grundlage für drahtlose Netzwerkprodukte unter dem Markennamen **Wi-Fi**.

4.1 Protokoll 802.11

Der Standard IEEE 802 definiert zwei gesonderte Schichten, die Steuerung logischer Verbindungen **LLC** (engl. *Logical Link Control*) und die Medienzugriffssteuerung **MAC** (engl. *Medium Access Control*) für die Sicherungsschicht (engl. *Data Link Layer*) des Referenzmodells **OSI** (engl. *Open System Interconnection*). Der drahtlose Standard IEEE 802.11 definiert Spezifikationen für die Bitübertragungsschicht **PHY** und Medienzugriffssteuerung **MAC**, die mit der **LLC**-Schicht kommuniziert (siehe Bild 1.11).

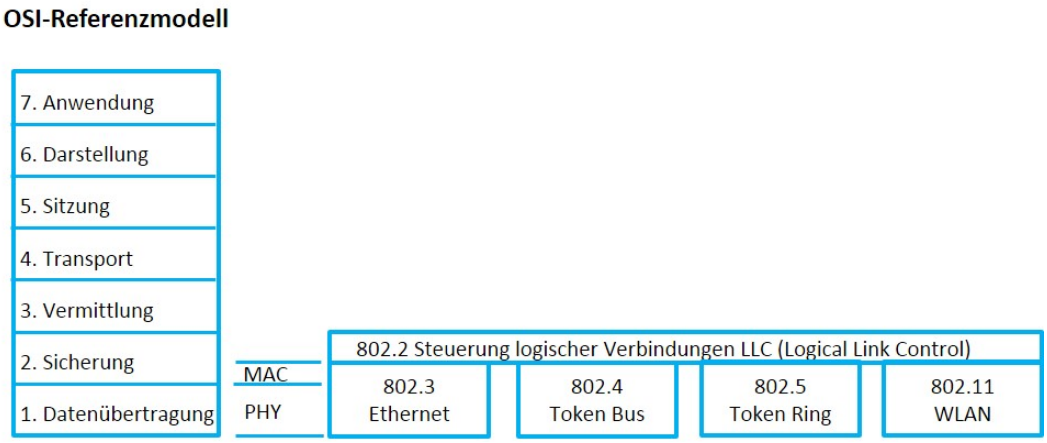


Bild 1.11 Standard IEEE 802.11 und OSI-Referenzmodell

Alle Komponenten der Architektur gemäß IEEE 802.11 gehören entweder zur Medienzugriffssteuerung **MAC** (Unter-Schicht der Sicherungsschicht) oder zur Bitübertragungsschicht **PHY**.

4.2 MAC-Frame gemäß IEEE 802.11

Ein **MAC**-Frame gemäß IEEE 802.11 (siehe Bild 1.12) besteht aus einem **MAC**-Header, einem Körper des Frames (Frame Body) und einer Blockprüfzeichenfolge **FCS** (engl. *Frame Check Sequence*). Das Format des **MAC**-Frames umfasst einen Satz von neun Feldern, die in einer festen Reihenfolge in allen **MAC**-Frames auftreten.

Frame Control

Das Feld Frame Control (siehe Bild 1.12) enthält Steuerungsinformationen, die zur Unterscheidung des Typs des **MAC**-Frames gemäß IEEE 802.11 verwendet werden, und liefert die erforderlichen Informationen für die folgenden Felder, so dass sichergestellt ist, wie der **MAC**-Frame zu verarbeiten ist.

Nachfolgend werden weitere Felder von Frame Control beschrieben:

- **Protocol Version** gibt die aktuelle Version des verwendeten Protokolls IEEE 802.11 an. Die Empfangsstation **STA** verwendet diesen Wert um festzustellen, ob die Version des Protokolls für den Frame unterstützt wird.

- **Type and Subtype** bestimmen die Funktion des Frames. Es gibt drei Typen der Frames: Steuerungs-, Daten- und Überwachungsframes. Für jeden Typ des Frames gibt es mehrere Subtypen. Jeder Subtyp bestimmt die spezifische Funktion, die für den damit assoziierten Typ des Frames verknüpft wird.

- **To DS und From DS** indizieren, ob der Frame in die Richtung zum oder vom Verteilungssystem **DS** (engl. *Distributed System*) gesendet wird. Es werden nur diejenigen Datenframes von den Stationen **STA** verwendet, die mit einem Zugriffspunkt **AP** assoziiert sind.

- Das Feld **More Fragments** bestimmt, ob mit weiteren Teilen des Frames, entweder des Daten- oder Überwachungstyps, zu rechnen ist.

- **Retry** indiziert, ob der Frame, entweder als Daten- oder Steuerungstyp, erneut gesendet wurde.

- **Power Management** gibt an, ob sich die Sendestation **STA** im aktiven Betrieb oder Stromsparmodus befindet.

- Das Feld **More Data** informiert die Station **STA** im Stromsparmodus, dass der Zugriffspunkt **AP** weitere Frames zu senden hat. Es ermöglicht dem Zugriffspunkt **AP** zu signalisieren, dass weitere Frames des Typs *Broadcast* oder *Multicast* gesendet werden.

- **WEP** indiziert, ob Verschlüsselung und Authentifizierung im Frame verwendet wurden. Es kann für alle Daten- und Steuerungsframes eingestellt werden, bei dem der **Subtype** auf Authentifizierung eingestellt ist.

- **Order** bestimmt, dass alle empfangenen Datenframes in der gegebenen Reihenfolge verarbeitet werden müssen.

Duration/ID

Dieses Feld wird für alle Steuerungsframes, mit Ausnahme des Subtyps Stromsparframe **PSP** (engl. *Power Save Poll*) zur Indikation der restlichen Dauer verwendet, die für den Empfang der Übertragung des weiteren Frames erforderlich ist. Beim Stromsparframe **PSP** hat dieses Feld die Identifikation der Assoziierung **AID** (engl. *Association Identity*) der Sendestation **STA**.

Adressfelder

In Abhängigkeit vom Typ des Frames werden die vier Adressfelder eine Kombination der folgenden Adresstypen beinhalten:

- Die *BSS Identifier* (**BSSID**) identifiziert eindeutig jeden **BSS**. Wenn der Frame von einer Station **STA** in Infrastruktur-**BSS** stammt, ist **BSSID** die **MAC**-Adresse des gegebenen Zugriffspunktes **AP**. Wenn der Frame von einer Station **STA** in **IBSS** stammt, ist **BSSID** eine zufällig generierte, lokal verwaltete **MAC**-Adresse der Station **STA**, die durch die **IBSS** initialisiert wurde.

- Die *Destination Address* (**DA**) indiziert die **MAC**-Adresse des endgültigen Bestimmungsortes des Frames.

- Die *Source Address* (**SA**) bestimmt die **MAC**-Adresse der ursprünglichen Quelle, die den Frame erstellt und gesendet hat.

- Die *Receiver Address* (**RA**) bestimmt die **MAC**-Adresse der nächsten benachbarten Station **STA** im drahtlosen Medium, die den Frame empfangen kann.

- Die *Transmitter Address* (**TA**) indiziert die **MAC**-Adresse der Station **STA**, die den Frame ins drahtlose Medium gesendet hat.

Weitere Informationen über alle Adresstypen und Adressfelder der **MAC**-Header sind in der Dokumentation des Standards IEEE 802.11 auf der Webseite von IEEE zu finden [6].

Sequence Control

Das Feld Sequence Control beinhaltet zwei Subfelder, Feld mit Nummer des Fragments und Feld mit Nummer des Ablaufs, wie auf dem Bild 1.12 zu sehen ist.

Nachfolgend sind die Felder Sequence Control beschrieben:

- Die Sequence Number gibt die Ablaufnummer jedes Frames an. Sie ist für alle Fragmente eines Frames gleich. Die Nummer wird um eins bis 4095 erhöht und fängt dann wieder bei 0 an.

- Die Fragment Number gibt die Nummer des Fragments der aufgeteilten Frames an. Der Ausgangswert ist 0 und wird um eins für jedes folgende Fragment des aufgeteilten Frames erhöht.

Frame Body

Frame Body enthält Daten oder Informationen von Steuerungs- bzw. Datenframes.

Blockprüfzeichenfolge FCS

Die Sendestation **STA** setzt zyklische Redundanzprüfung **CRC** (engl. *Cyclic Redundancy Check*) für alle Felder des **MAC**-Headers und Körpers des Frames ein, um einen Wert der Blockprüfzeichenfolge **FCS** zu generieren. Die Empfangsstation **STA** verwendet dann die gleiche **CRC**-Berechnung, um ihren eigenen Wert des **FCS**-Feldes zu bestimmen. So wird überprüft, dass kein Übertragungsfehler im Frame aufgetreten ist.

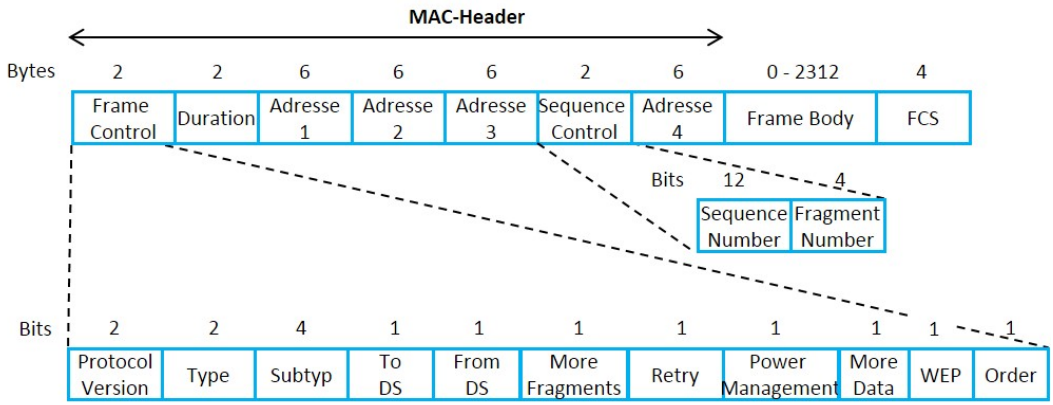


Bild 1.12 Format des MAC-Frames gemäß Standard IEEE 802.11. Die Felder Frame Control und Sequence Control sind detailliert angezeigt.

4.3 Bitübertragungsschicht PHY gemäß 802.11

Der Standard IEEE 802.11 definiert in der Bitübertragungsschicht **PHY** für drahtlose Kommunikation einige Verschlüsselungs- und Übertragungsverfahren. Oft verwendet werden das Frequenzsprung-Spektrumspreizverfahren **FHSS** (engl. *Frequency Hopping Spread Spectrum*), das Direktsequenz-Spektrumspreizverfahren **DSSS** (engl. *Direct Sequence Spread Spectrum*) und das orthogonale Frequenzmultiplexverfahren **OFDM** (engl. *Orthogonal Frequency Division Multiplexing*). Das Bild 1.13 zeigt die Standards IEEE 802.11, IEEE 802.11b, IEEE 802.11a, IEEE 802.11g, IEEE 802.11n und IEEE 802.11ac, die zurzeit auf der Bitübertragungsschicht **PHY** verwendet werden. Diese Standards werden in der folgenden Absätzen beschrieben.

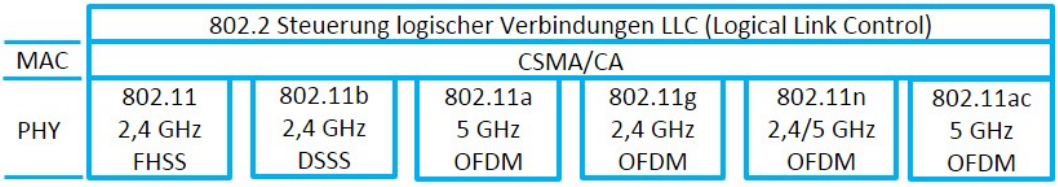


Bild 1.13 Standards IEEE 802.11 auf Bitübertragungsschicht

IEEE 802.11

Die Übertragungsrate des ursprünglichen Standards IEEE 802.11 beträgt 2 Mbit/s, wobei das Übertragungsverfahren **FHSS** mit dem Frequenzband **ISM** eingesetzt wird, welche den Frequenzbereich von 2,4 bis 2,5 GHz verwenden. Unter ungünstigen Bedingungen wird eine niedrigere Übertragungsrate von 1 Mbit/s verwendet.

IEEE 802.11b

Die wichtigste Verbesserung des Standards IEEE 802.11 in der Version IEEE 802.11b ist die Standardisierung der Bitübertragungsschicht **PHY** zur Unterstützung von höheren Übertragungsraten. IEEE 802.11b unterstützt zwei weitere Raten, 5,5 Mbit/s und 11 Mbit/s, die das Frequenzband von 2,4 GHz ausnutzen. Um höhere Übertragungsraten zu erzielen, wird das Verfahren **DSSS** eingesetzt. Unter idealen Bedingungen wird die Übertragungsrate von 11 Mbit/s erreicht. In anderen Fällen stehen niedrigere Übertragungsraten von 5,5 Mbit/s, 2 Mbit/s und 1 Mbit/s zur Verfügung.

Es ist darauf hinzuweisen, dass IEEE 802.11b das gleiche Frequenzband wie Mikrowellenherde, schnurlose Telefone, Babyfons, drahtlose Videokameras und Bluetooth-Geräte verwendet.

IEEE 802.11a

IEEE 802.11a kann mit Übertragungsraten von bis zu 54 Mbit/s arbeiten und verwendet das Frequenzband 5 GHz. Anstatt **DSSS** verwendet IEEE 802.11a das **OFDM**-Verfahren, das eine parallele Datenübertragung im Rahmen von Subfrequenzen ermöglicht und eine höhere Störfestigkeit und einen größeren Datendurchsatz erlaubt. Die höhere Übertragungsrate ermöglicht drahtlosen **LAN** bessere Leistungen für Video- und Konferenzanwendungen.

Wegen der Arbeitsfrequenz, die sich von Frequenzen anderer Geräte unterscheidet (z. B. schnurlose Telefone mit 2,4 GHz), kann IEEE 802.11a mit **OFDM** sowohl höhere Übertragungsrate als auch ein reineres Signal garantieren. Die Übertragungsrate von 54 Mbit/s kann nur unter idealen Bedingungen erzielt werden. In anderen Fällen stehen niedrigere Übertragungsraten von 48 Mbit/s, 36 Mbit/s, 24 Mbit/s, 18 Mbit/s, 12 Mbit/s und 6 Mbit/s zur Verfügung.

IEEE 802.11g

IEEE 802.11g kann mit Übertragungsraten von bis zu 54 Mbit/s arbeiten, aber verwendet das Frequenzband von 2,4 GHz und das **OFDM**-Verfahren. Er ist auch rückwärtskompatibel zum Standard IEEE 802.11b und kann mit den Übertragungsraten des IEEE 802.11b arbeiten und das **DSSS**-Verfahren verwenden. Drahtlose Netzwerkadapter von IEEE 802.11g können problemlos an drahtlose Zugriffspunkte **AP**, die den IEEE 802.11b Standard verwenden, angeschlossen werden. Umgekehrt können drahtlose Netzwerkadapter für den Standard IEEE 802.11b auch an drahtlose Zugriffspunkte **AP** für den Standard IEEE 802.11g angeschlossen werden.

IEEE 802.11g erlaubt daher die Netzwerkmigration für Netzwerke von IEEE 802.11b mit frequenzkompatibler Technologie und höherer Übertragungsrate.

Bestehende drahtlose Netzwerkadapter für den Standard IEEE 802.11b können auf IEEE 802.11g nicht nur durch bloße Aktualisierung ihrer Firmware upgegradet werden, sondern müssen ersetzt werden. Im Unterschied zur Migration von IEEE 802.11b auf IEEE 802.11a, bei der alle Netzwerkadapter sowohl bei drahtlosen Kunden als auch drahtlosen Zugriffspunkten **AP** zugleich ersetzt werden müssen, kann die Migration von IEEE 802.11b auf IEEE 802.11g schrittweise durchgeführt werden.

Wie IEEE 802.11a erzielt auch IEEE 802.11g unter idealen Bedingungen die Übertragungsrate von 54 Mbit/s und anderenfalls werden niedrigere Raten von 48 Mbit/s, 36 Mbit/s, 24 Mbit/s, 18 Mbit/s, 12 Mbit/s und 6 Mbit/s erreicht.

IEEE 802.11n

IEEE 802.11n verbessert vor allem die Reichweite (bis zu 250 m) und den Netzwerkdurchsatz im Vergleich mit den zwei Standards IEEE 802.11a und IEEE 802.11g (von 54 Mbit/s bis zu 600 Mbit/s unter idealen Bedingungen). Diese

Verbesserungen wurden durch Integration des Verfahrens **MIMO** (engl. *Multiple Input Multiple Output*) und Erweiterung des Übertragungskanals auf 40 MHz erreicht. Das **MIMO**-Verfahren verwendet mehrere drahtlose Signale und Antennen sowohl für Sender als auch für Empfänger. Es kann auch in den Frequenzbändern von 2,4 GHz oder 5 GHz eingesetzt werden.

IEEE 802.11ac

Der Standard IEEE 802.11ac stellt ein Upgrade von IEEE 802.11n dar und leistet eine ähnliche Reichweite, aber einen erhöhten Durchsatz. Er arbeitet auf dem Frequenzband von 5 GHz und nutzt beam-forming, breite Bänder und mehrere Antennen, um theoretisch Übertragungsraten von bis zu 1,3 Gbit/s zu erzielen, was mehr als das Zweifache der maximalen Übertragungsrate von 600 Mbit/s bei IEEE 802.11n ist.

5 Sicherheit

Drahtlose Netzwerke sind im Allgemeinen nicht so sicher wie Festnetze. Festnetze übertragen im einfachsten Fall Daten zwischen zwei Punkten A und B, die mit einem Netzkabel verbunden sind. Im Unterschied dazu senden drahtlose Netzwerke Daten in alle Richtungen und an alle Geräte in einem begrenzten Radius, die diese Sendung zufällig empfangen können. Festnetze können zum Beispiel durch die Beschränkung des physischen Zugriffs und die Installation von Firewalls gesichert werden. Die drahtlosen Netzwerke sind beim Einsatz der gleichen Maßnahmen immer noch durch Abhören gefährdet. Daher erfordern drahtlose Netzwerke einen höheren Aufwand, um die Sicherheit gewährleisten zu können.

5.1 Sichere Kommunikation

Der Begriff Kommunikationssicherheit wird häufig mit den folgenden drei Prozessen verbunden: Authentifizierung (engl. *authentication*), Vertraulichkeit (engl. *confidentiality*) und Integrität (engl. *integrity*) [1].

Die Authentifizierung stellt sicher, dass Knoten wirklich diejenigen sind, als die sie sich ausgeben.

Die Authentifizierung basiert typischerweise auf eine Überprüfung von Zugriffsdaten, wie zum Beispiel Benutzername und Passwort, durch eine beauftragte Autorität. In komplexeren Systemen kann die Authentifizierung für den Nachweis auf den Besitz eines gewissen Schlüssels oder Tokens beruhen, das schwieriger gestohlen oder gefälscht werden kann, als ein Zertifikat oder eine Chipkarte.

Vertraulichkeit stellt sicher, dass ein Lauscher den Netzverkehr nicht abhören kann.

Die Vertraulichkeit wird typischerweise durch Verschlüsselung des Nachrichteninhalts geschützt. Die Verschlüsselung verwendet eine bekannte reversible Transformationsmethode (auch Chiffre oder Verschlüsselungsalgorithmus bezeichnet) für den Inhalt der ursprünglichen Nachricht (auch Klartext oder Plaintext bezeichnet), um den Schlüsseltext (auch Chiffretext bezeichnet) durch Scrambling oder Maskieren zu generieren. Nur diejenigen, die wissen, wie der Prozess umgekehrt werden kann (d. h. wie die Nachricht entschlüsselt werden kann), können den ursprünglichen Text rekonstruieren. Zu den bekanntesten Verschlüsselungsmethoden gehören mathematische Transformationen, die als Variable einen Schlüssel verwenden, der einen unteilbaren Bestandteil des Transformationsprozesses schafft. Der Empfänger muss dann das richtige Verfahren und den verwendeten Schlüsselwert kennen, so dass er die Nachricht entschlüsseln kann. Für kommerzielle Verschlüsselungsverfahren sind die Methoden allgemein bekannt. Die Geheimhaltung des Schlüssels ist entscheidend.

Integrität stellt sicher, dass die Nachrichten ohne Änderungen zugestellt werden.

In Hinblick auf Kommunikationssicherheit bedeutet Integrität die Garantie, dass die empfangene Nachricht keineswegs geändert wurde und identisch mit der gesendeten Nachricht ist. Bytes in Blockprüfzeichenfolge **FCS** sind ein Beispiel für ein Datenintegritätsverfahren, aber sie sind als nicht sicher zu betrachten. Die üblichen **FCS**-Bytes werden für den Inhalt der Nachricht nicht berechnet und auch nicht durch Verschlüsselung geschützt. Stattdessen werden sie von dem Schlüsseltext mit einer bekannten Methode berechnet und in einer direkten, d. h. nicht verschlüsselten Form gesendet. Die **FCS**-Bytes helfen bei der Identifikation der Pakete, die zufällig bei der Übertragung beschädigt werden. Der Angreifer könnte jedoch die richtigen Werte der **FCS**-Bytes berechnen, um zum Beispiel eine absichtliche Änderung eines empfangenen und weitergeleiteten Pakets zu maskieren. Je schwieriger für den Angreifer die richtige Berechnung der

Integritätsprüfzeichenfolge oder der Sicherheits-Hash-Funktion ist, desto zuverlässiger ist der Test der Nachrichtenintegrität.

Die Konzeption der Integrität wird manchmal durch eine Überprüfung ergänzt, dass die Quelle der Nachricht identisch mit der angegebenen Quelle der Nachricht ist. Zeitstempel (engl. *timestamp*) und Sequenznummern können einen erfolgreichen Schutz vor wiederholten Angriffen darstellen, aber noch einmal wiederholt, können Übertragungen ohne Verschlüsselung als unsicher betrachtet werden.

Der Begriff Sicherheit ist immer relativ, nie absolut. Für jede Verteidigung gibt es einen erfolgreichen Angriff (oder wird es bald geben). Und für jeden Angriff gibt es eine erfolgreiche Verteidigung (oder wird es bald geben). Es ist nur eine Frage von Zeit und Aufwand. Je besser die Verteidigung ist, desto mehr Zeit und Aufwand wird für einen Angriff benötigt.

Die richtige Verteidigung muss ausgewogen sein und dem erwarteten Ausmaß der Angriffe entsprechen. Die Ausgewogenheit muss aus zwei Aspekten beachtet werden. Erstens muss das schwächste Kettenglied ausreichend sicher sein. Zweitens müssen passive Elemente der Authentifizierung, Verschlüsselung und Integritätsprüfung mit aktiven Elementen ergänzt werden, wie z. B. Überwachung des Netzverkehrs, Verfolgung der Verletzungsversuche und Einhaltung von Sicherheitsregeln. Die richtige Verteidigung ist die Verteidigung, die nur ein wenig mehr Zeit und Mühe aufwendet, die ein Angreifer aufzuwenden gewillt ist. Sicherheitsmaßnahmen bedeuten Kosten und Beschränkungen für den Verteidiger. Wie bei anderen Geschäftsentscheidungen müssen auch hier Kompromisse unter Berücksichtigung von allen möglichen Gesichtspunkten getroffen werden.

5.2 Vertraulichkeit und Verschlüsselung

Die Vertraulichkeit, d. h. das Verhindern von unerlaubten Zugriffen auf die Inhalte einer Nachricht, wird durch Verschlüsselung erreicht. Die Verschlüsselung ist für das **WLAN** optional, denn ohne sie kann jedes kompatible Gerät in seiner Reichweite den Netzverkehr abhören.

Für das **WLAN** gibt es drei grundlegende Sicherheitsverfahren. Seit der zweiten Hälfte der neunziger Jahre haben **Wi-Fi**-Sicherheitsalgorithmen mehrere Upgrades erlebt, einschließlich der Entfernung älterer Algorithmen und Updates neuerer Algorithmen. In der chronologischen Reihenfolge handelt es sich um die folgenden Algorithmen:

- **WEP**-Verfahren (engl. *Wired Equivalent Privacy*)
- **WPA**-Verfahren (engl. *Wi-Fi Protected Access*)
- **WPA2**-Verfahren (engl. *Wi-Fi Protected Access version 2*)

WEP

WEP wurde als Sicherheitsstandard für **Wi-Fi**-Netze im September 1999 genehmigt. Die ersten **WEP**-Versionen waren nicht besonders stark, nicht einmal zu Zeiten ihrer Veröffentlichung, weil Ausfuhrbeschränkungen der USA seitens verschiedener Verschlüsselungstechnologien zu Herstellerbeschränkungen der Geräte auf max. 64-Bit-Verschlüsselung führten. Nachdem diese Beschränkungen aufgehoben wurden, stiegen die späteren Versionen auf 128 Bits. Trotz der Einführung der **WEP**-Verschlüsselung mit 256 Bits, sind 128 Bits eine der gängigsten Implementierungen.

Trotz der Überarbeitung des Algorithmus und Verlängerung der Schlüssel wurden im Laufe der Zeit viele Sicherheitsschwachstellen im **WEP**-Standard gefunden und mit der Steigung der Rechenleistung war es auch einfacher, diese Schwachstellen auszunutzen. Schon 2001 wurde das grundlegende Konzept in Frage gestellt und 2005 organisierte das **FBI** eine öffentliche Vorführung mit dem Ziel, ein Bewusstsein für die **WEP**-Schwächen zu schaffen. In dieser Vorführung wurden **WEP**-Passwörter in wenigen Minuten mittels frei verfügbarer Software geknackt.

Obwohl mehrere Verbesserungen, provisorische Lösungen und weitere Versuche zur Modernisierung des **WEP**-Verfahrens führten, war es immer noch sehr unsicher. Die Systeme, die auf dem **WEP**-Verfahren beruhen, sollten upgegradet werden oder, wenn Sicherheitsupgrades nicht möglich sind, ersetzt werden. Die **Wi-Fi**-Allianz zog **WEP** im Jahre 2004 zurück.

WPA

Um die Verwundbarkeit von **WEP** zu überwinden, wurde am Anfang 2003 die **WPA**-Gruppe im Rahmen der **Wi-Fi**-Allianz gegründet. Die übliche **WPA**-Konfiguration ist **WPA-PSK** (engl. *Wi-Fi Protected Access Pre-Shared Key*). Die

Länge des von **WPA** verwendeten Schlüssels beträgt 256 Bits, was eine erhebliche Erhöhung gegenüber 64 Bits und 128 Bits bei **WEP** darstellt.

Eine der bedeutendsten, in **WPA** eingeführten Änderungen sind die Integritätsprüfung der Nachrichten (zur Feststellung, ob ein Angreifer die Pakete zwischen dem Zugriffspunkt **AP** und Klienten abgefangen und geändert hat) und das **TKIP**-Protokoll (engl. *Temporal Key Integrity Protocol*). **TKIP** verwendet ein Schlüsselsystem für jedes übertragene Paket, das viel sicherer als ein Festschlüssel im **WEP**-System ist. **TKIP** wurde später vom **AES**-Standard (engl. *Advanced Encryption Standard*) ersetzt.

Trotz einer erheblichen Verbesserung des **WPA** im Vergleich mit dem **WEP** konkurriert **WEP** immer noch mit **WPA**. **TKIP**, die grundlegende Komponente des **WPA**, wurde so entworfen, dass es einfach mittels Firmwareupgrades in bestehende **WEP**-Geräte eingeführt werden kann. Als solches werden einige Elemente wiederverwendet, was dann auch zu einer Ausnutzung von Schwachstellen geführt hat.

Bei **WPA**, wie bei seinem Vorgänger **WEP**, wurde sowohl mit einem Machbarkeitsnachweis als auch mit einer öffentlichen Vorführung gezeigt, dass ihre Integrität von Angreifern erfolgreich verletzt werden kann. Es ist interessant, dass der Prozess, bei dem **WPA** üblicherweise angegriffen wird, kein direkter Angriff auf den **WPA**-Algorithmus ist (obwohl diese Angriffe auch erfolgreich getestet wurden), sondern es handelt sich um Angriffe auf ein zusätzliches System des **WPS** (engl. *Wi-Fi Protected Setup*), das mit **WPA** zusammenarbeitet und das so entworfen wurde, dass Geräte an modernen Zugriffspunkten **AP** einfach angeschlossen werden können.

WPA2

WPA wurde seit 2006 offiziell durch **WPA2** ersetzt. Eine der bedeutendsten Änderungen im Vergleich zu **WPA** war der obligatorische Einsatz von **AES** und dem **CCMP**-Protokoll (engl. *Counter Cipher Mode with Block Chaining Message Authentication Code Protocol*) als Ersatz für das **TKIP** (es wurde in **WPA2** als Reservesystem und zur Interoperabilität mit **WPA** erhalten).

Zurzeit wird die primäre Sicherheitsverletzbarkeit des aktuellen **WPA2** als unbedeutend betrachtet (der Angreifer muss dabei schon einen Zugriff zu einem gesicherten **Wi-Fi**-Netz haben, um den Zugriff auf Sicherheitsschlüssel zu erlangen und dann weitere Geräte im Netz anzugreifen). So werden die Sicherheitsimplikationen der bekannten Verletzbarkeit von **WPA2** fast ausschließlich auf Unternehmensnetzwerke begrenzt und haben keine praktische Bedeutung für kleine Haushaltsnetze.

Leider blieb das größte Sicherheitsloch bei **WPA** auch bei modernen **WPA2**-Zugriffspunkten bestehen: Vektorangriff über **WPS**. Obwohl Einbrechen in ein mit **WPA**/**WPA2** gesichertes Netz durch Überwindung des **WPS** 2-14 Stunden mit einem modernen Computer dauern kann, handelt es sich immer noch um ein seriöses Sicherheitsrisiko und **WPS** sollte deaktiviert werden. Gleichzeitig sollte die Firmware der Zugangsknoten auf die Version wechseln, die **WPS** nicht unterstützt, so dass dieses Risiko nicht mehr besteht.

Nachfolgend eine Auflistung der aktuellen Sicherheitsverfahren von **Wi-Fi**-Netzen von den besten bis zu den schlechtesten:

1. **WPA2** + **AES**
2. **WPA** + **AES**
3. **WPA** + **TKIP**/**AES** (**TKIP** ist hier das Reserveverfahren)
4. **WPA** + **TKIP**
5. **WEP**
6. Offenes Netzwerk (ohne jede Sicherung)

Im Idealfall wird **WPS** deaktiviert und das Sicherungsniveau auf **WPA2** + **AES** eingestellt. Alle weitere Kombinationen in der Auflistung stellen eine wesentliche Verschlechterung dar.

6 Vor- und Nachteile

Drahtlose Netzwerke haben gegenüber Festnetzen eine Reihe von erheblichen Vorteilen, wie Mobilität, Kosteneffizienz und Adaptabilität, aber es gibt auch Nachteile, wie die Sicherheit. Unten sind grundlegende Vor- und Nachteile von drahtlosen Netzwerken gegenüber Festnetzen angeführt.

Die folgende Liste fasst einige Vorteile von drahtlosen Netzwerken zusammen:

Höhere Effizienz

Verbesserte Datenkommunikation führt zu schnellerer Informationsübertragung zwischen Unternehmen, Partnern und Kunden. Beispielsweise können Geschäftsleute Lagerbestände und Preise über Remote-Verbindungen kontrollieren und zugleich Telefongespräche führen.

Bessere Abdeckung und Mobilität

Kabelanschlüsse binden an einen Ort. Mit dem Übergang zu drahtlosen Netzwerken erhält man Bewegungsfreiheit bei gleichzeitiger Aufrechterhaltung von Verbindungen, ohne zusätzliche, für Büronetzwerke erforderliche Kabel oder Adapter.

Flexibilität

Büroangestellte können miteinander verbunden sein, ohne an benachbarten Computern sitzen zu müssen, und können auch außerhalb eines Büros produktiv arbeiten. Das kann zu einem neuen Arbeitsstil führen, beispielsweise durch ein Homeoffice oder den direkten Zugriff auf Unternehmensdaten während der Verhandlung beim Kunden.

Kosteneinsparung

Die Installation von drahtlosen Netzwerken kann einfacher und billiger sein, insbesondere in denkmalgeschützten Gebäuden oder wenn Vermieter keine Verlegung von Kabeln erlauben. Die Abwesenheit von Drähten und Kabeln reduziert die Gesamtkosten. Dies wird durch eine Kombination von mehreren Faktoren erzielt: relativ niedrige Kosten der drahtlosen Router, kein Graben, Bohren und Verlegen von Kabeln in Wänden oder keine weitere physische Installationen. Zusätzlich fällt die Wartung der Kabel-Infrastruktur weg.

Adaptabilität

Schnelle und einfache Integration der Geräte an das Netz und hohe Flexibilität bei einer Modifikation der Installation.

Neue Gelegenheiten/Anwendungen

Dank der drahtlosen Netzwerke können neue Produkte und Dienstleistungen angeboten werden. Zum Beispiel haben viele Abflughallen, Bahnhöfe, Hotels, Cafés und Restaurants Hot Spots für Dienstleistungen der drahtlosen Netzwerke

installiert, um den mobilen Benutzern einen Anschluss ihrer Geräte an die Netzinfrastruktur zu ermöglichen.

Es gibt auch gewisse Nachteile, die mit der Ausnutzung der drahtlosen Netzwerke verbunden sind.

Sicherheit

Eine drahtlose Übertragung ist verletzbarer beim Angriff seitens unbefugter Benutzer und daher muss der Sicherheit eine besondere Aufmerksamkeit gewidmet werden.

Installationsprobleme

Man kann gestört werden, wenn andere Geräte in demselben Gebäude auch drahtlose Technologien verwenden oder wenn weitere Quellen von Funksignale in der Nähe sind. Das kann zur schlechten Qualität der Kommunikation oder in einem extremen Fall zum totalen Ausfall der drahtlosen Kommunikation führen.

Abdeckung

In einigen Gebäuden kann eine gleichmäßige Abdeckung schwierig sein. Es können auch Gebäudeteile ohne Signal entstehen. Beispielsweise in Gebäuden mit stahlarmierten Materialien kann es problematisch sein, ein verwendbares mobiles Signal zu finden.

Übertragungsrate

Drahtlose Übertragungen können im Vergleich zu Festnetzen langsamer und weniger effizient sein. Bei umfangreichen drahtlosen Netzwerken wird das Backbone-Netz üblicherweise ein Festnetz und kein drahtloses Netzwerk sein.

7 Anwendungen

Die Reichweite der drahtlosen Kommunikation in integrierten Systemen wächst weiter. Die Gesellschaft Forrester Research, die sich mit betriebswirtschaftlichen Auswirkungen von technologischen Änderungen beschäftigt, berichtete, dass in wenigen Jahren bis zu 95 % aller Geräte, die Internetzugang haben, nicht-PC-Geräte mit einem integrierten Betriebssystem sein werden.

Es gibt viele Anwendungen für integrierte Geräte mit einer **Wi-Fi**-Schnittstelle:

- Industrieprozess- und Steueranwendungen, bei denen Festnetze zu teuer oder ungeeignet sind, z. B. häufige Umzüge von Maschinen.
- Notfallanwendungen, die sofortige und vorübergehende Einstellungen erfordern, wie z. B. in Kriegsgebieten oder in Gebieten von Naturkatastrophen.
- Mobile Anwendungen, z. B. zur Teileverfolgung.
- Überwachungskameras (vielleicht möchten Sie, dass die Kameras nicht sofort entdeckt werden, und Kabel lassen sich nur ungenügend verbergen).
- Vertikale Marktsegmente, z. B. Medizin, Ausbildung und Produktionstechnik.
- Kommunikation mit weiteren Wi-Fi-Geräten, z. B. Laptops oder PDA.
- Kommunikation unter Maschinen (**M2M**, engl. *Machine to Machine*).

Der letzte Begriff der M2M-Anwendungen bezieht sich auf Technologien, die eine Kommunikation von Geräten desselben Typs über drahtlose Netzwerke als auch Festnetze ermöglichen. [http://en.wikipedia.org/wiki/Machine_to_machine] Eine weitere Charakteristik der M2M-Kommunikation besteht darin, dass diese Verbindung vor allem die automatisierte Kommunikation zwischen entfernten Maschinen und einer oder mehr Schichten der zentralen Managementanwendungen ermöglicht. Sie stellt eine Echtzeitüberwachung und -steuerung ohne notwendige menschliche Eingriffe dar.

Im drahtlosen **M2M**-Raum gibt es zwei Hauptklassen der Verbindungen – mit einer kurzen und einer langen Reichweite. Die überwiegende Technologie der langen Reichweite verwendet integrierte Mobilfunkmodule zum Anschluss von entfernten Geräten an das Internet oder einen Anwendungsserver. Mobilfunkmodule haben viele ähnliche Funktionen wie Handys, einschließlich Sprach- und Datenkommunikation, und sind daher für integrierte Anwendungen ideal.

M2M-Anwendungen kann man in einer Reihe von Industrien finden, z. B. Zählerfernauslesung **AMR** (engl. *Automatic Meter Reading*), Verkaufsautomaten, Terminals an Verkaufsorten **POS** (engl. *Point Of Sales*), Transport- und Logistiksysteme (Flottenmanagement), Gesundheitspflege und Sicherheitstechnologie.

Gemäß der Gesellschaft ABI Research, die sich mit technologischer Forschung und Beratung beschäftigt, werden bis 2020 mehr als 30 Milliarden Geräte an das Internet der Dinge (engl. *Internet of Things*) drahtlos angeschlossen sein.

8 Schlussfolgerung

Drahtlose Netzwerktechnologien verbinden ohne Kabel unsere Hochtechnologie-Geräte mit Hochgeschwindigkeitsnetzen oder anderen Geräten. In der Vergangenheit musste man Kabel von einem Raum zum anderen, von einem Stock zum nächsten verlegen. Der finanzielle und zeitliche Aufwand war erheblich.

Heutzutage ist die Installation eines drahtloses Netzwerkes eine einfache Aufgabe und es gibt eine Unmenge von drahtlosen Produkten und Hilfsmitteln zur Einstellung und Konfiguration von drahtlosen Netzwerken.

Man kann aus verschiedenen Technologien wählen, um Anwendungsanforderungen zu erfüllen. Die Reichweite der Datenübertragung kann von einigen Metern bis zu einigen Kilometern reichen.

Damit bieten drahtlose Netzwerke neue Möglichkeiten für industrielle Lösungen, müssen aber unter besonderer Berücksichtigung der Sicherheit implementiert werden.

Vergleich der Typen der drahtlosen Netzwerke

Typ des Netzes	Name	Standard	Frequenzband	Nenn-Reichweite	Maximale Übertragungsrate
WPAN	Bluetooth	IEEE 802.15.1	2,4 GHz	10 m	720 Kbit/s
	IrDA	IrDA	Infrarotfenster Wellenlänge 850-900 nm	1 m	16 Mbit/s
	ZigBee	IEEE 802.15.4	868 MHz, 900 MHz, 2,4 GHz	10 m	250 Kbit/s
	UWB	IEEE 802.15.3	3,1-10,6 GHz (USA) 3,4-4,8 GHz & 6-8,5 GHz (Europa)	10 m	480 Mbit/s
WLAN	Wi-Fi	IEEE 802.11	2,4 / 5 GHz	100 m	1 Mbit/s
		IEEE 802.11a	5 GHz	100 m	48 Mbit/s
		IEEE 802.11b	2,4 GHz	100 m	11 Mbit/s
		IEEE 802.11g	2,4 GHz	100 m	54 Mbit/s
		IEEE 802.11n	2,4 / 5 GHz	250 m	600 Mbit/s
		IEEE 802.11ac	5 GHz	250 m	1,3 Gbit/s
WMAN	WiMAX	IEEE 802.16	2-11 GHz+10-66 GHz	50 km	70 Mbit/s
WWAN	Mobilfunknetze	AMPS, GSM, GPRS, UMTS, HSDPA, LTE	700 MHz, 850 MHz, 900 MHz, 1800 MHz, 1900 MHz, 2100 MHz, 2600 MHz	> 50 km	1 Gbit/s
	Satellitennetze	DVB-S2	3-30 GHz	> 50 km	60 Mbit/s