



Vorlesung

VPN: Drahtgebunden und drahtlos

Fachbereich Informatik (FB 20)

Lehrstuhl Prof. J.Buchmann

WS-05 / V2 - 20.205.1

In Zusammenarbeit mit dem CAST-Forum

Dr. Wolfgang Böhmer

Skript: <http://www.cdc.informatik.tu-darmstadt.de/~wboehmer/>

Email: wboehmer@cdc.informatik.tu-darmstadt.de





Vorlesungsinhalte

- Die Wireless Technologie als Remote Access Verfahren
 - Wireless Kategorien bzgl. einer 2-Wege Kommunikation
 - Zell-basierende Wireless Lösungen (2G, 2,5G und 3G)
 - Wireless-LAN-Lösungen (IEEE 802.15, HomeRF, IEEE 802.11, IEEE 802.16)
 - Wireless-Zugriffsreichweite
 - Die Spreizbandtechnik als Übertragungstechnologie (Bitübertragungsschicht)
 - Funkfrequenzen und die Vermittlungsschicht (Network-Layer)
 - Sicherheitsmängel in der WLAN Technologie (WEP, IV, MAC, etc.)
 - Sicherheitsergänzungen in der WLAN Technologie (EAP-TLS, VPN)



Die Wireless Technologie als Remote Access Verfahren



- Als das Konzept eines Netzwerkes ohne Kabel beziehungsweise Draht vor mehr als zwei Dekaden erstmals vorgeschlagen wurde, begeisterten sich dafür sofort Wissenschaftler, Hersteller und Benutzer in allen Teilen der Welt.
- Doch die erste Welle der Lösungen zeigte sich als wenig geeignet für Netzwerke und die Anforderungen an Portierbarkeit und Sicherheit in dem sich laufend ändernden IT-Umfeld.
- Während dieser Zustand bis in den 90 Jahren bei der Entwicklung von Zellen-basierter und LAN basierter Wireless Technologie größtenteils so blieb, gab es besonders in den letzten zwei Jahren große Fortschritte, im Bereich der Wireless Netzwerke in Unternehmen und im SOHO Bereich.
- Die Wireless Technologie ist in verschiedenen Formen verfügbar und bietet vielfältige Lösungen. Es lassen sich generell zwei Wireless Kategorien unterscheiden:
 1. Zellen-basierte Wireless-Datenlösungen
 2. Wireless-LAN-Lösungen (WLAN)





Zellenbasierte Wireless-Technologien

- Zellen-basierte Wireless-Netzwerke sind Netzwerke, die einen Wireless-Zugriff durch neue oder bereits existierende Zell-(Mobil)Telefon-Technologien bieten. Da Zellen-basierte Netzwerktechnologien große geographische Gebiete abdecken, werden diese zuweilen auch als Wide-Area-Netzwerktechnologien bezeichnet.
- Bei den Zellen-basierten Wireless Technologie koexistieren aktuell verschiedene Standards und Netzwerktechnologien für die Datenkommunikation, die sich generell in 2G, 2.5G und 3G-Wireless Netzwerke unterteilen.
 - **2G-Circuit-Switched-Cellular-Wireless Netzwerke**
 - **2.5G-Packet-Data-Overlay-Cellular-Wireless-Netzwerke**
 - **3G-Packet-Switched-Cellular-Wireless-Netzwerke**





2G-Circuit-Switched-Cellular-Wireless Netzwerke (1)

- 2G ist der Ausdruck, der allgemein für die zweite Generation der Zell-basierten Wireless-Kommunikationsnetzwerke verwendet wird. Es stellt eine Evolution der Advanced-Mobile-Phone-Service-(AMPS)-Netzwerken dar (1G).
- 2G Netzwerke unterstützen Sprach-, Text- und bidirektionale Datenkommunikation mit einem Datendurchsatz von 9,6 Kbit/s
- Eine Reihe wichtiger Wireless-Netzwerktechnologien wird als Teil der zweiten Zellen-basierter Netzwerke betrachtet:
- **CDMA**
 - Ein im zweiten Weltkrieg entwickeltes Verfahren (Code-Division-Multiple-Access), das als digitale Übertragungstechnik das DSSS-Verfahren nutzt. Spread-Spektrum (Spreizbandtechnik) setzt einem Rauschen ähnliche Trägerwellen ein und bietet gegenüber einer Standard Punkt-zu-Punkt-Kommunikation eine Erhöhung der Datenrate, bietet größeren Widerstand gegen Jamming-Signale. lässt sich schwerer abfangen und entdecken, und bietet Möglichkeiten, die Distanz, welche die Übertragung zurücklegen soll zu bestimmen.
- **TDMA**
 - Time-Division-Multiple-Access ist eine Digitale Übertragungstechnik, die Funkfrequenzen in spezifische Zeitabschnitte unterteilt. Es wird eine Art Timesharing der Funksignale in sechs eindeutige Zeitabschnitte erreicht. TDMA stellt die Zugriffstechnik für GSM dar und wird auf 800-Mhz und 1900 Mhz-Frequenzen implementiert.





2G-Circuit-Switched-Cellular-Wireless Netzwerke (2)

- **CDPD**
 - Ist eine paketvermittelnde Technik, die in den frühen 90er Jahren für Vollduplex-Datenübertragung über AMPS-800Mhz Mobiltelefonfrequenzen entwickelt wurde. Die CDPD-Technikspezifikation unterstützt IP und das Connectionless-Network-Protocol (CLNP). CDPD-Carrier stellen oftmals dedizierte Kanäle zur Verfügung. Die Sicherheit wird durch eine RSA-(RC-4) Verschlüsselung gewährleistet
- **GSM**
 - Das Global system for Mobile Communication (GSM) wurde 1980 als Standard für die Zellen-basierte Mobilkommunikation in Europa entwickelt es nutzt die TDM-Übertragungsmethode. Im Laufe der 90er Jahre hat sich GSM zu einer Wireless-Netzwerkarchitektur entwickelt, die Sprache und Datendienste (SMS) bereitstellt. Übertragungsraten erreichen 9,6 Kbit/s.





2.5G-Packet-Data-Overlay-Cellular-Wireless-Netzwerke

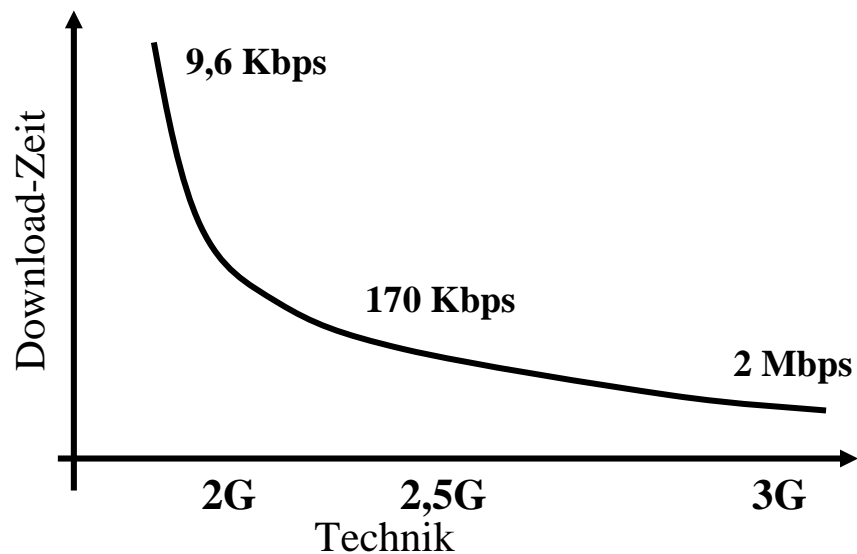
- Die 2,5G-Wireless-Netzwerke sind eine Übergangslösung von 2G Netzwerken zu 3G-Netzwerken. Die hauptsächliche Weiterentwicklung ist die Einführung der Übertragung von Paketdaten über existierende Sprachdienste. Es werden Datenraten von 100 bis 384 Kbit/s erreicht.
- **GPRS**
 - General-Packet-Radio-Service ist eine Erweiterung der GSM-Netze und rüstet existierende Wireless-Netzwerke-Zugriffsknoten auf, um eine Route zu Gateway-Knoten herzustellen. Gateway-Knoten bieten dann die Möglichkeit z.B. auf das Internet zuzugreifen. GPRS ermöglicht die Kommunikation über IP abzuwickeln und bietet 115 bis 170 Kbit/s und unterstützt eine immer vorhandene Verbindung. GPRS unterstützt definierte QoS-Spezifikationen und das GPRS-Tunneling-Protokoll (GTP). Sicherheitsprotokolle werden zur Abriegelung von Geräten und Sitzungen eingesetzt.
- **GPRS/EDGE**
 - Ist eine Zwischenlösung für den Übergang von existierenden GPRS-Netzwerken auf 3G-Edge-basierte Netzwerke.
- **1xRTT**
 - 1xRTT wird allgemein als CDMA2000-Phase-One bezeichnet und repräsentiert die erste Stufe des Übergangs existierende CDMA-Techniken zur vollständigen 3G-Fähigkeit.





3G-Packet-Switched-Cellular-Wireless-Netzwerke

- 3G-Wireless-Technik ist die für 2004 zu erwartende dritte Generation der Wireless Techniken. Die Zugriffsgeschwindigkeit wird bei IP bis zu 2MBit/s betragen.



Wireless-LAN-Lösungen (WLAN)



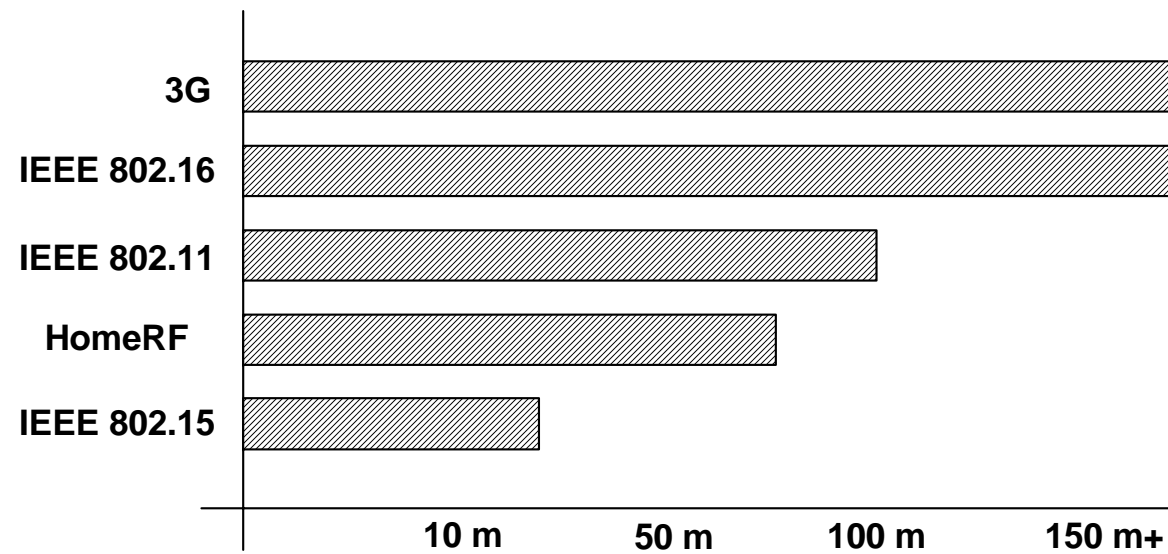
- Es existieren gegenwärtig fünf kommerzielle Wireless-LAN-Lösungen
 - **802.11 (WLAN)** können entweder in Client-/Host-Konfiguration (PCF) oder in einer Peer-to-Peer-Konfiguration (DCF) arbeiten, jedoch nicht gleichzeitig in beiden Konfigurationen.
 - **HomeRF** ist eine Wireless-Netzwerk-Technologie, die speziell auf Netzwerke im Hausbereich abzielt. HomeRF basiert auf verschiedene Sprach- und Datenstandards und nutzt das 2,4 GHz ISM-Wireless Band mit dem Frequenz-Hopping-Spread-Spectrum (FHSS) aus.
 - **802.15 WPAN**, das Wireless-Personal-Area-Network basierend im wesentlichen auf Bluetooth arbeiten im 2,4 GHz-ISM Band und benutzen Time-Division-Multiple-Access (TDMA).
 - **802.16 WMAN**, das Wireless-Metropolitan-Area-Network wurde 1998 ins Leben gerufen, hat sich mittlerweile zum Wi-MAX Standard weiterentwickelt.
 - **802.20 Vehicular mobility**



Wireless Reichweiten



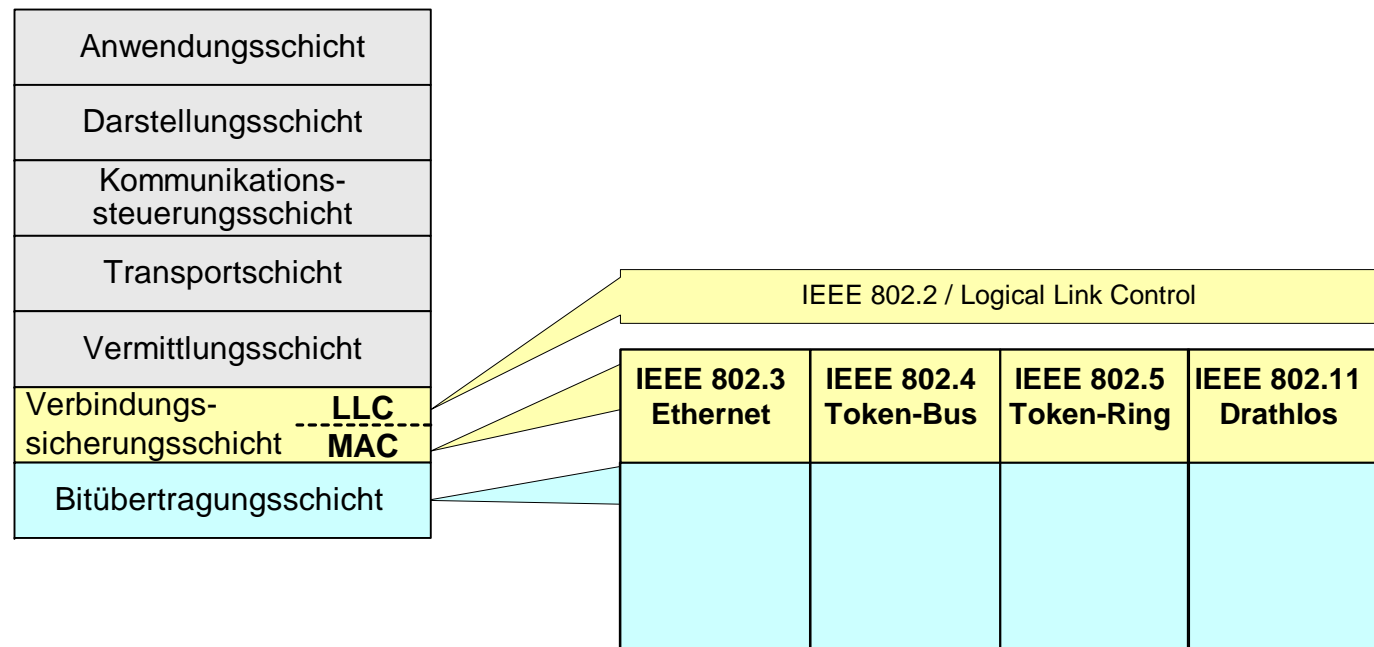
- Reichweitenvergleich zwischen Zell-basierter und Wireless LAN-Lösungen





IEEE 802.11 Standard im OSI-Modell (1)

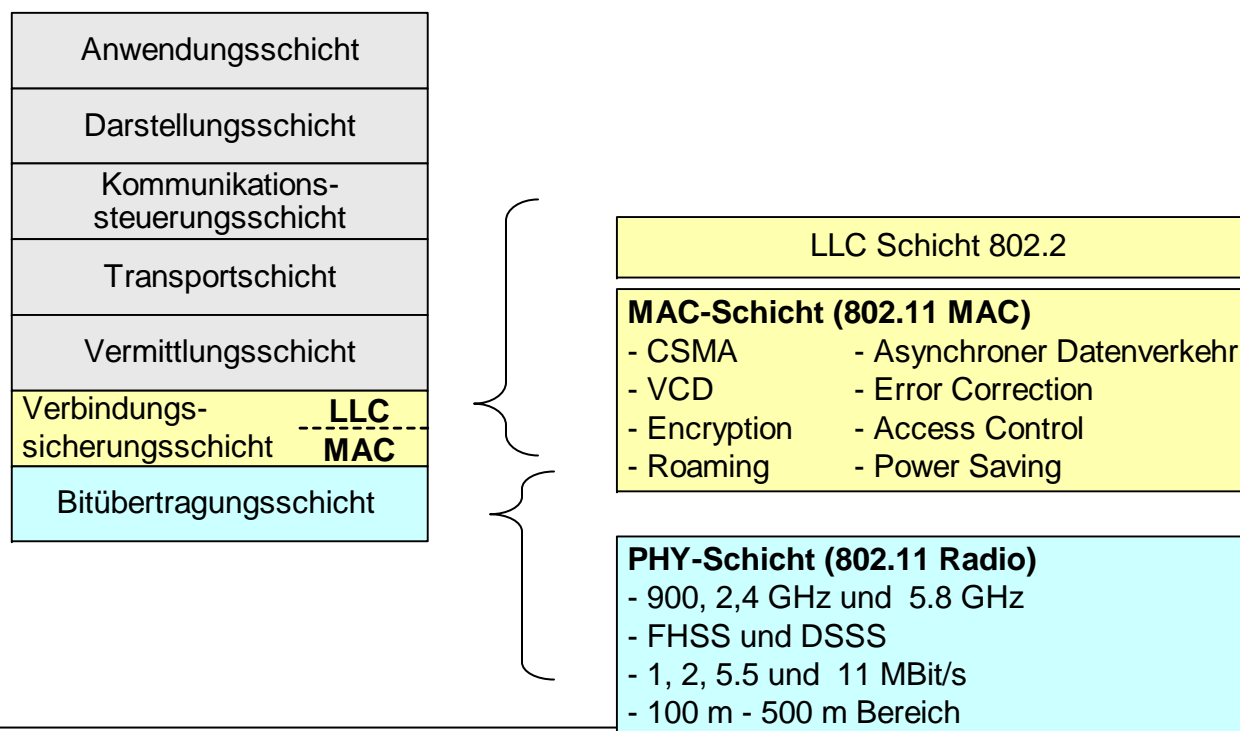
- Der 802.11 Standard fügt sich als Ergänzung ins OSI-Modell für die
 - Verbindungssicherungsschicht (MAC) und für die
 - Bitübertragungsschicht ein.





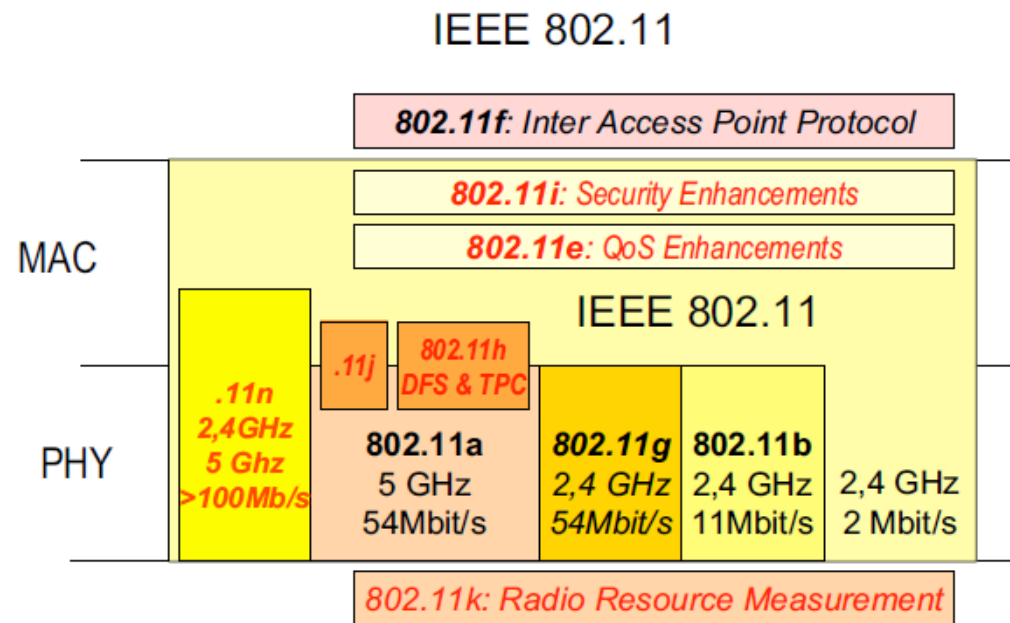
IEEE 802.11 Standard im OSI-Modell (2)

- Die gelbe und blaue Schicht stellen IEEE 802.11 Ergänzungen dar.





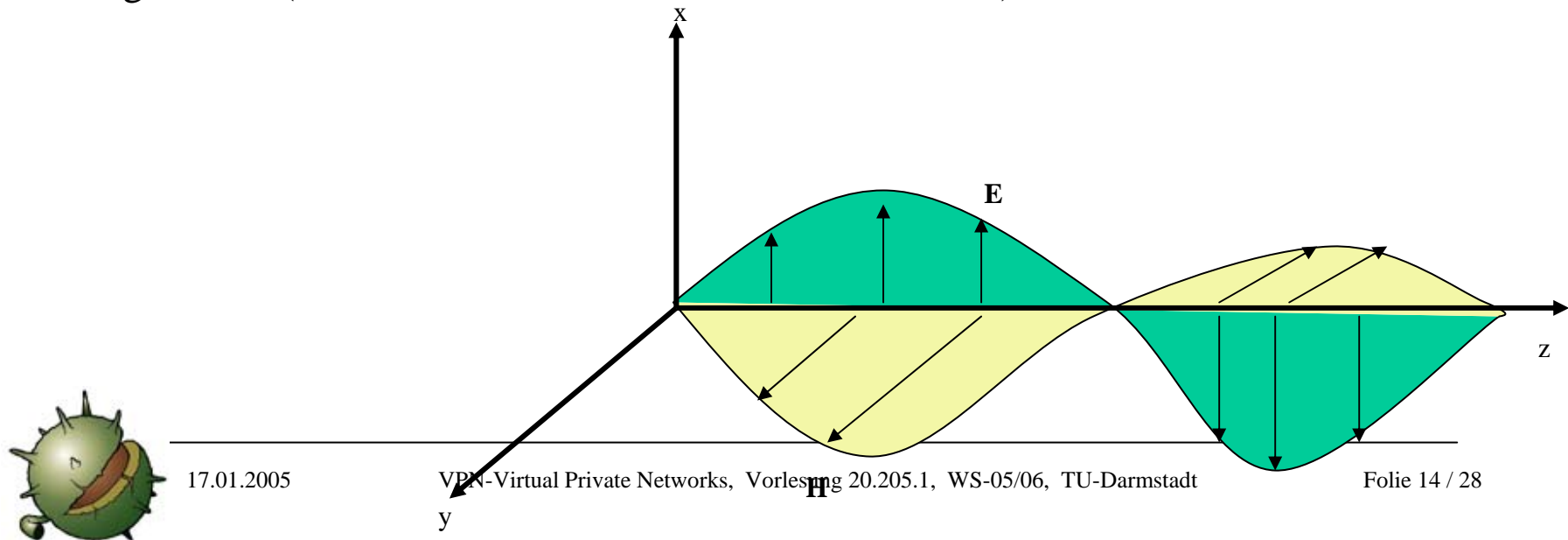
IEEE 802.11 Standard im OSI-Modell (3)





Wellenfänger und transversale Ausbreitung (I)

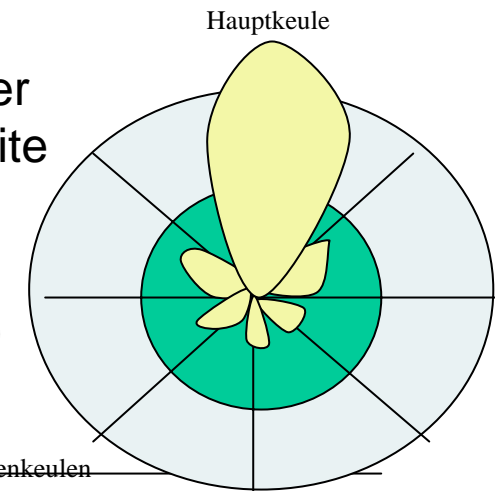
- 1886 hat Heinrich Hertz demonstriert, dass mit elektrischen und magnetischen Felder sich Nachrichten übertragen lassen.
- Das elektrische Feld steht dabei stets senkrecht auf dem magnetischen Feld und beide stehen senkrecht zur Ausbreitungsrichtung.
- Im Fall des WLAN wird, wie im Mobilfunk, zumeist vertikal polarisiert gesendet (der Strahler einer Antenne steht senkrecht).





Wellenfänger und transversale Ausbreitung (II)

- Das Richtdiagramm einer Antenne gibt für die horizontale und vertikale Ebene an, wie gut in jede Raumrichtung gesendet und empfangen wird: Je schmaler die Keule, desto höher der Gewinn in Vorzugsrichtung.
- Ausgehend von der idealen Vorstellung eines isotropen Strahlers, wird die Wellenenergie in Form einer Kugeloberfläche ausgesandt, die dazu führt, dass bei Verdoppelung der Distanz, der Empfänger nur noch ein Viertel des Signal empfängt. D.h. bei Verdoppelung der Sendeleistung wird keineswegs die doppelte Reichweite erzielt.
- WLAN funkt nur dann gut, wenn die sogenannte Fresnel-Zone (ein gedachter Fussballförmiger Körper) zwischen Sender und Empfänger weitgehend hindernisfrei ist.





WLAN-Spezifikation (1)

- Der IEEE-802.11-Wireless-LAN-Standard startete 1998 und beabsichtigte ursprünglich, ein drahtloses Äquivalent zum Ethernet zu bilden.
- **Die IEEE-802.11-Wireless-LAN Spezifikation bietet generell:**
 1. **Wireless Verbindungen für traditionelle LAN-Geräte, z.B.: Workstation, Server, Drucker, etc.**
 2. **Eine allgemeine, standardisierte Media-Access-Control-(MAC)-Schicht.**
 - **CSMA/CA Collision Avoidance mit einem verteilten Ansatz (DCF) über einen Zufalls-Backoff-Timer (Ähnlich dem 802.3 Ethernet (CSMA/CD)).**
 - **Unterstützt TCP/IP, UDP/IP, IPX, Netbui, etc.**
 - **Virtual-Collision-Detection-(VCD)Option.**
 - **Fehlerbehebung und Zugriffsteuerung durch positive Bestätigung von Paketen und erneuten Übertragungen.**
 - **Verschlüsselte Kommunikation mit WEP-Verschlüsselung**
 - **Roaming**
 - **Stromsparschemen für nicht aktive Geräte**
 - **Schnittstellen zu Betriebssystemen.**





WLAN-Spezifikation (2)

- **Die IEE-802.11-Wireless-LAN Spezifikation bietet generell:**
 3. **Eine von der Implementierung abhängige Bitübertragungsschicht.(Physical Layer)**
 - **Unterstützt drei Funkfrequenz-Spread-Spectrum-Techniken (FHSS, DSSS und HRDSS)**
 - **Spezifiziert, welche der Techniken in Europa, Nordamerika und Japan verwendet werden.**
 - **Unterstützung für 2,4-GHz und 5-GHz-ISM-Bänder.**
 - **Unterstützung für Zugriffsgeschwindigkeiten von 1 Mbit/s, 2 Mbit/s, 5,5 Mbit/s, und 11 Mbit/s mit weiteren Geschwindigkeiten in zukünftigen Releases des Standards.**
 - **Basis-Multivendor-Interoperabilität.**





IEEE 802.11 (MAC-Schicht / Zugriffsschicht)

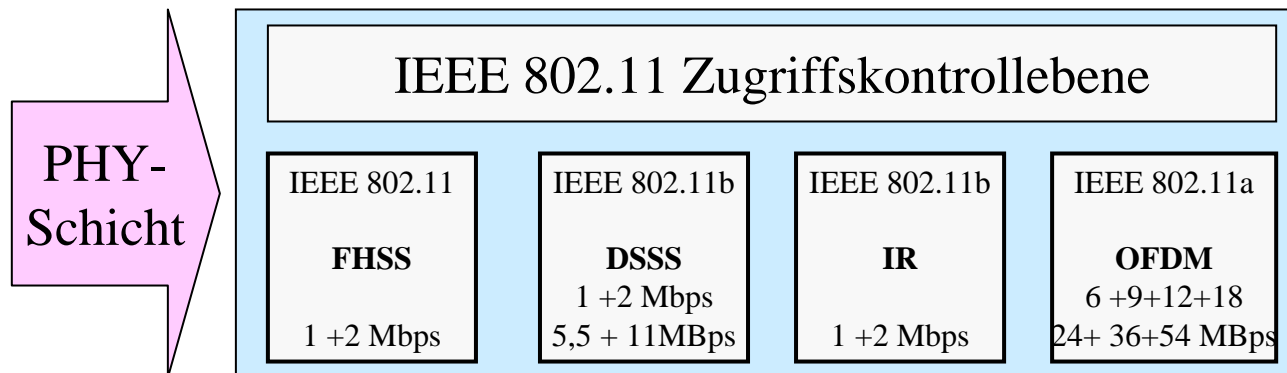
- Wie das Ethernet ist das Funkmedium ein Broadcast Medium.
- Innerhalb einer Zelle kann somit zu einem Zeitpunkt immer nur eine Station senden. Senden dennoch mehrere Stationen führt dies zu Kollisionen.
 - Der Zugriff auf das Medium muss so geregelt werden, dass Kollisionen möglichst vermieden werden.
 - Treten dennoch Kollisionen auf, so müssen diese erkannt und erneut die betroffenen Frames gesendet werden.
- Beim Ethernet ist dies durch das CSMA/CD geregelt. Eine Station die ein Frame senden möchte, prüft ob das Medium frei ist und beginnt sofort zu senden. Kommt es zu Kollisionen, legen die beteiligten Stationen eine unterschiedlich lange Zwangspause ein.
- Beim WLAN ist dies durch das CSMA/CA geregelt. Da auf der physikalischen Ebene auf dem Funkmedium keine Kollisionen erkannt werden können, werden kurze Request-to-Send/Clear-to-Send Kontroll Frames vor der Übertragung einer Nachricht geschickt. Die auf eine Übertragung wartenden Stationen beginnen hier nicht sofort den Sendevorgang, sobald das Medium frei ist, sondern starten einen Zufalls-Backoff-Timer.





IEEE 802.11 (PHY-Schicht / Bitübertragung)

- Die Architektur der physikalischen Ebene des IEEE 802.11 Standard erlaubt verschiedene Ebenen unterhalb einer einheitlichen Zugriffskontrolle.
 - Die Frequenz Hopping Spread Spectrum (FHSS) Technologie
 - Die Direct Sequenz Spread Spektrum (DSSS) Technologie
 - Die Infrarot Technologie
 - Die Orthogonal Frequenz Division Multiplexing (OFDM) Technologie





Frequenz Hopping Spread Spectrum (FHSS) (1)

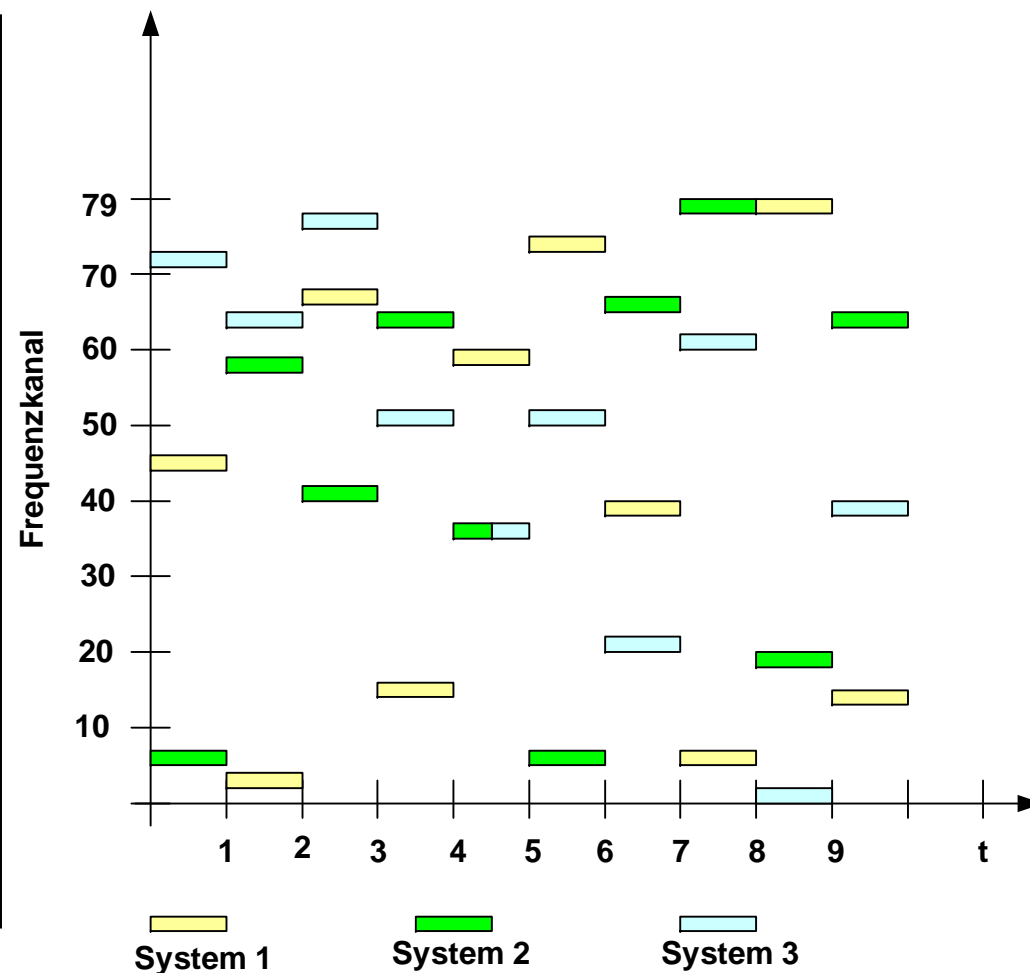
- Beim FHSS wechselt die Frequenz des Trägersignals unter Verwendung eines schnellen Frequenz-Synthesizers in einem vordefinierten Muster von einer Frequenz auf die nächste in einem schnellen Rhythmus. Die Endstation und der AP einigen sich auf am Anfang der Übertragung auf das zu verwendende Muster (Code)
 - Im Frequenzband (2,4000 – 2,4833 GHz) werden 79 Kanäle mit jeweils 1 MHz Bandbreite definiert.
 - Die Reihenfolge der 79 Kanäle wird durch 79 Hopping-Sequenzen festgelegt, die nur dem jeweiligen Sender und Empfänger bekannt sind.
 - Eine Kollision tritt nur dann auf, wenn zwei Systeme einen der 79 Kanäle gleichzeitig benutzen.
 - Bis zu 13 FHSS-Systeme können mittels CDMA gemeinsam in einem Empfangsbereich arbeiten.
 - Höhere Datenraten (als 2 Mbps) kann man bei FHSS-Systemen nicht erreichen, da der Bereich von 2,4-GHz-Band nicht erweitert werden kann.
 - Roaming ist in FHSS-Systemen sehr aufwendig.





Frequenz Hopping Spread Spectrum (FHSS) (2)

- Die farbigen zeigen unterschiedliche Systeme die teilweise in Kollision zu einander stehen. Ein Kanal darf höchstens 400 ms benutzt werden und zwei aufeinanderfolgend benutzte Kanäle müssen einen Abstand von 6 MHz haben.
- Als Erkennungscode in dem CDMA-Verfahren dienen die Hopping-Frequenzen.



Direct Sequenz Spread Spektrum (DSSS) Technologie (1)



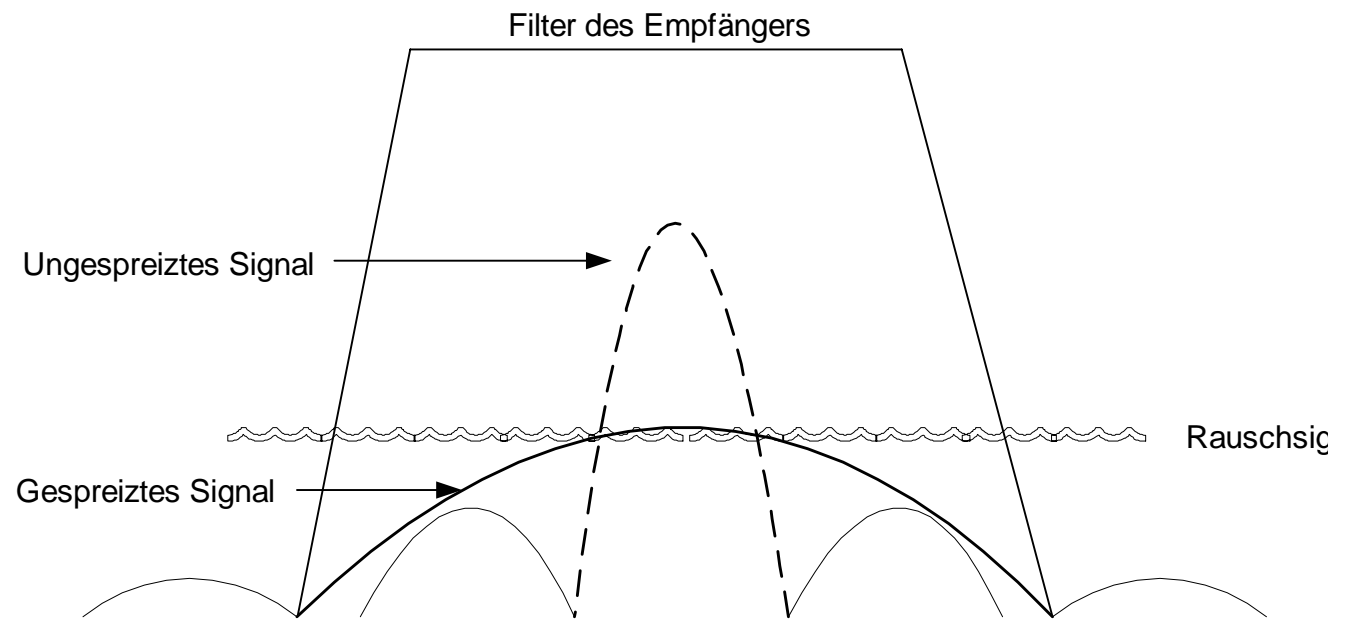
- Das Grundprinzip bei DSSS besteht darin, ein Signal zu spreizen (Spread-Spectrum)
- Ein schmalbandiges Signal wird durch einen Code in ein breitbandiges Signal umgewandelt. Es wird dazu ein Pseudo-Noise Code (PN-Code) eingesetzt.
- Im Gegensatz zu FHSS-Systemen wird das Signal hier jedoch nicht zeitlich auf verschiedene Kanäle versetzt, sondern durch den PN-Code direkt in ein breitbandiges Signal umgewandelt und kontinuierlich auf diesem Band versendet.
- Die Spreizung wird durch Modulo-2-addition des PN-Codes mit dem übertragenden Datenbit erreicht.
- Einhergehend damit wird die Intensität des breitbandigen Signals derart reduziert, dass sie unterhalb der Rauschgrenze liegt.
- Somit ist die Störung für andere Systeme minimal und das Signal kann nur noch von einem Empfänger erkannt werden, der den PN-Code kennt.



Direct Sequenz Spread Spektrum (DSSS) Technologie (2)

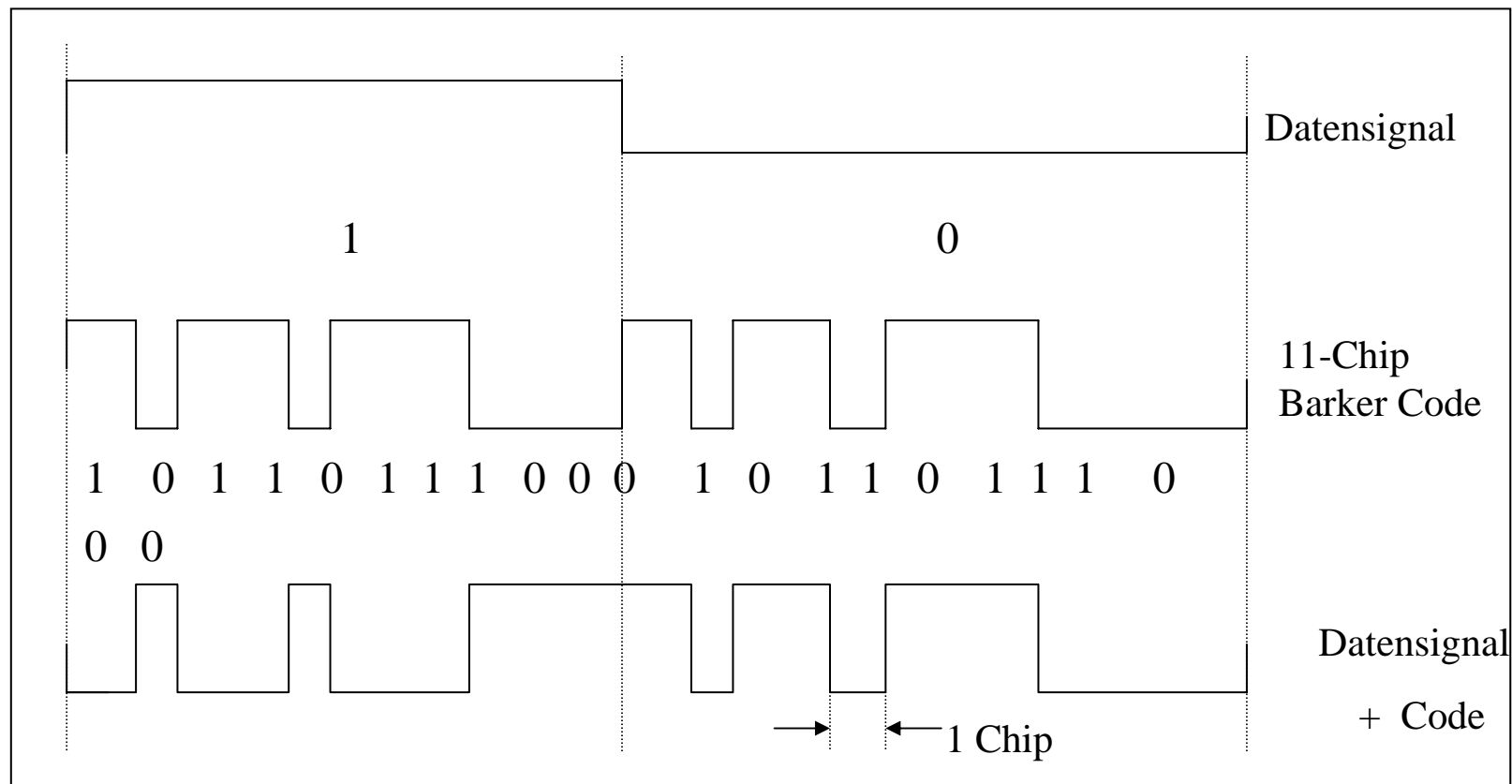


- Das Frequenzband ist in 13 Kanäle in Europa unterteilt. Die Center Frequenzen haben einen Abstand von jeweils 5 MHz.
- Ein PN-Code besteht aus sogenannten Chips.
- Für IEEE-DSSS-Systeme mit Übertragung von 1 bzw. 2 Mbps besteht aus dem 11-Chip Barker Code.
10110111000



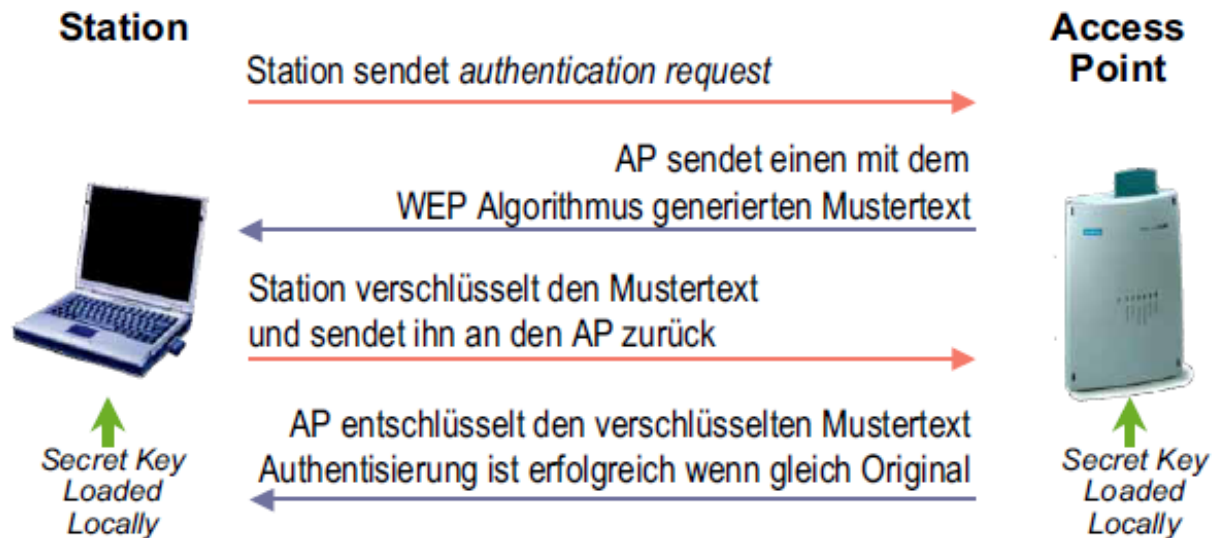


Signalspreizung durch PN-Code





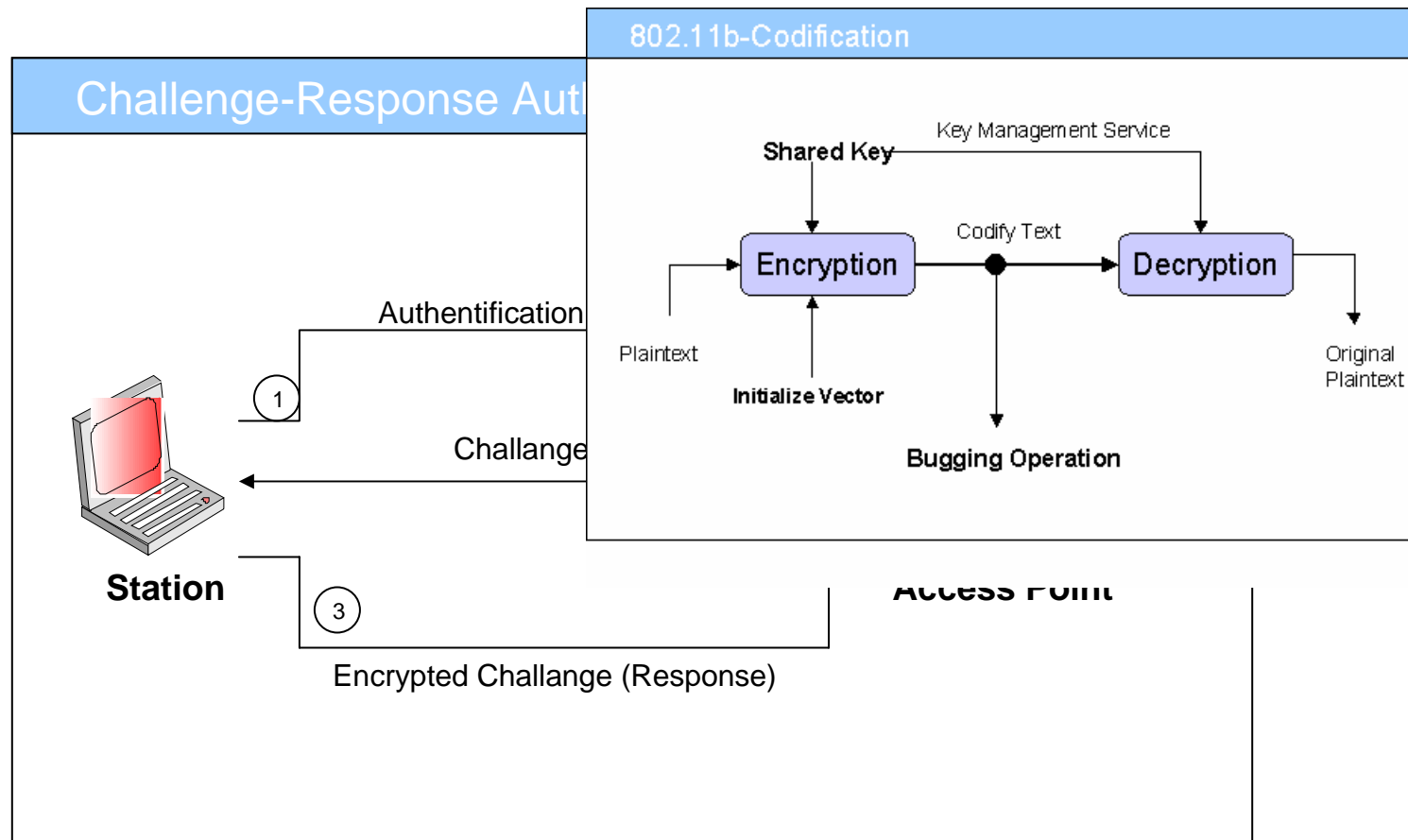
WEP Verlauf (*Shared Key*)



- ❑ Shared key Authentisierung benötigt den WEP Algorithmus
- ❑ Schlüsselmanagement ist in IEEE802.11 nicht spezifiziert
- ❑ Die Authentisierung erfolgt nur einseitig



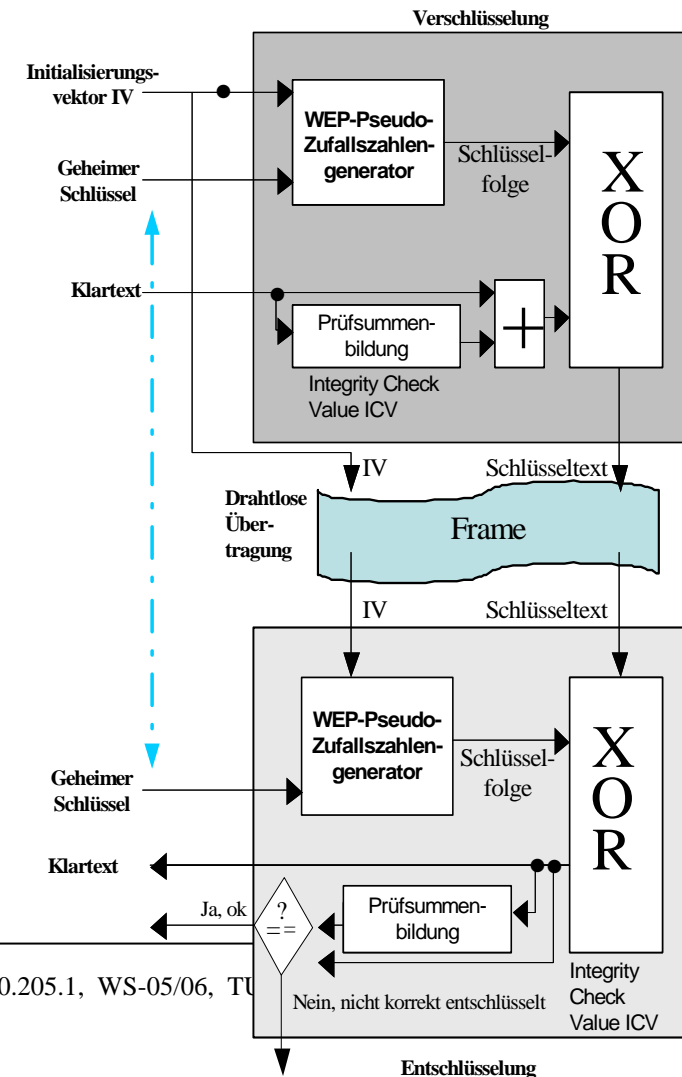
WEP (wired equivalent privacy)





Wired Equivalent Privacy (WEP)

- Es wird ein gemeinsamer Schlüssel genutzt (Shared Key)
- IEEE 802.11 lässt offen wie die Schlüssel zu den Stationen gelangen.
- Ausgehend von einem Schlüssel und einem (zufällig bestimmten) Initialisierungsvektor (Seed) mit Hilfe eines Generators für Pseudozufallszahlen eine Folge von Bytes bestimmt wird, mit denen der Klartext des Datenteils bitweise über XOR verknüpft wird.
- Der Generator arbeitet mit RC4-Algorithmus, der für eine Eingabe eine zufällige, aber bei der derselben Eingabe exakt reproduzierbare, beliebig lange Folgen von Bytes.
- Der IV (24 Bit-Feld) wird unverschlüsselt mitgeschickt
- Die verschlüsselte Prüfsumme (ICV) wird ebenfalls mitgeschickt.





Shared Key Authentisierung, RC4

- ❑ Ziel von 802.11 war eine “Wired Equivalent Privacy” (WEP)
 - Weltweit verwendbar
- ❑ 802.11 bietet einen Authentisierungsmechanismus
 - zur Unterstützung der Zugangskontrolle.
 - sieht “OPEN”, “Shared Key” und proprietäre Verfahren vor
- ❑ Shared key Authentisierung basiert auf WEP
 - Beschränkt sich auf Station-zu-Station, nicht Ende-zu-Ende.
 - Benützt den RC4 Algorithmus mit:
 - ⇒ *40 bit secret key*
 - ⇒ *und einen 24 bit IV der mit den Daten mitgeschickt wird.*
 - ⇒ *beinhaltet einen ICV für die Integritätsprüfung.*





Nachteile von WEP

- ❑ WEP ist bei jeder Schlüssellänge unsicher
 - IV zu klein, Schutz vor IV Wiederverwendung fehlt
 - Angriffsmöglichkeit bei bekanntem Klartext
- ❑ Keine Benutzerauthentisierung
 - Nur das Netzwerkinterface wird authentisiert
- ❑ Keine gegenseitige Authentisierung
 - Nur die Stations authentisieren sich gegenüber dem AP
- ❑ Fehlende Schlüsselverwaltung
 - Kein Standard zum Austausch der Schlüssel während des Betriebs
 - Schlüsselverwaltung für einen grosseren Nutzerkreis schwierig
- ❑ WEP ist auf keinen Fall eine Einrichtung für absolute Sicherheit,
 - ... aber kann in manchen Gelegenheiten nützlich sein.
- ❑ IEEE P802.11 hat vor 4 Jahren eine Arbeitsgruppe zur Verbesserung der Sicherheit von WLAN eingerichtet.
 - Die Task Group 802.11i hat ihre Arbeit nun abgeschlossen.





WPA (Wi-Fi Protected Access)

- The Wi-Fi Alliance is a nonprofit international association formed in 1999 to certify interoperability of wireless Local Area Network products based on IEEE 802.11 specification. Currently the Wi-Fi Alliance has over 200 member companies from around the world, and over 1000 products have received Wi-Fi® certification since certification began in March of 2000. The goal of the Wi-Fi Alliance's members is to enhance the user experience through product interoperability.
- But all security is not created equal. While WPA is more secure than WEP, it is less secure than 802.11i. In order of increasing security, I would rate the various 802.11 algorithms as follows: WEP, WPA group key only, WPA pre-shared key, WPA pair-wise key, and 802.11i robust security network (RSN). Group key refers to an environment where all devices share the same key. Pre-shared key refers to a key or pass phrase that is entered on all access points and clients that will be used to create unique pair-wise keys for each mobile client and AP. Pair-wise keying creates unique keys for every mobile client device, derived from information in the [RADIUS](#) authentication.





Robust Security Network (IEEE 802.11i)

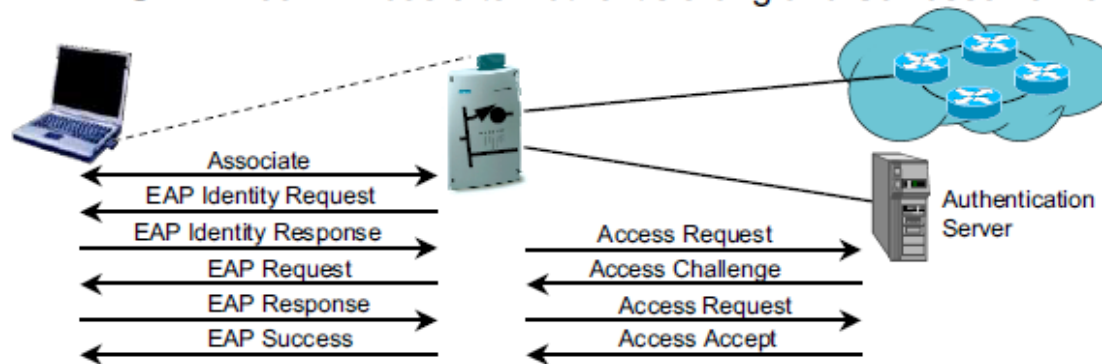
Zusätzliche Verbesserungen zu bestehenden Funktionen:

❑ Datenverschlüsselung:

- TKIP (Temporal Key Integrity Protocol) um mit RC4-basierter Hardware höhere Sicherheitsanforderungen zu erfüllen, und
- WRAP (Wireless Robust Authenticated Protocol) basierend auf AES (Advanced Encryption Standard) und CCMP

❑ Management der gesicherten Verbindung:

- RSN Verhandlungen zur Errichtung des Sicherheits-Kontexts
- IEEE802.1X basierte Authentisierung und Schlüsselverwaltung



IEEE 802.11i Sicherheitsanforderungen an den Datentransport



- ❑ Kein Transport ungesicherter Datenpakete
- ❑ Authentisierung der Nachrichtenquelle
 - Vermeidung von Betrug
- ❑ Serialisierung der Pakete
 - Detektierung von Wiederholungen
- ❑ Vermeidung der Schlüsselwiederverwendung
 - 48 bit Sequenznummer
- ❑ Schutz der Quell- und Zieladresse
- ❑ Einsatz von starker Verschlüsselungstechnik
 - für den Schutz von Vertraulichkeit und Integrität





TKIP: Temporal Key Integrity Protocol

- ❑ Zur Maskierung der Schwächen von WEP auf existierender AP Hardware
- ❑ Ist als Hülle für den WEP-Algorithmus konstruiert
 - Kann vollständig in Software implementiert werden
 - Macht Gebrauch von existierender WEP Hardware
 - Betreibt WEP als Komponente
- ❑ *Die Lösung erfüllt die Ansprüche an einen guten Standard!*
 - *niemand ist damit wirklich voll zufrieden*
- ❑ TKIP verwendet zwei Arten von Schlüssel
 - 1x 128 bit für die Verschlüsselung der Daten; AP und STA verwenden den selben Schlüssel
 - 2x 64-bit für den Schutz der Integrität: AP und STA verwenden unterschiedliche Schlüssel



Zweck der Phasen



- ❑ Discovery
 - Bestimmung von potentiellen Kommunikationspartnern
 - Der AP informiert die STAs über die Sicherheitsfeatures
- ❑ Authentication basierend auf 802.1X
 - Zentrale Verwaltung der Zugangskontrolle im AS
 - Endgültige Entscheidung der STA über den Verbindungsaufbau
 - Gegenseitige Authentisierung zwischen STA und AS
 - Erzeugung des *Master Key* als Abfallprodukt der Authentisierung
 - Erzeugung des *Authorization token* aus dem *Master Key*
- ❑ RADIUS-basierende Schlüsselübergabe
 - AS übergibt den Session-Key (PMK) zu dem dazugehörigen AP
- ❑ Key management mittels 802.1X
 - Bindung des PMK zur STA und zum AP
 - Bestätigung dass beide, der AP und die STA den PMK besitzen
 - Die Erzeugung von frischen Arbeitsschlüsseln (PTK)
 - Überwachung der Arbeitsfähigkeit der Kommunikationspartner



CCMP



- ❑ Die verbindliche Verschlüsselungslösung für 802.11 auf Dauer
- ❑ Ein vollständig neues Protokoll ohne Verwandtschaft zu WEP
- ❑ Speziell für IEEE 802.11i entworfen
- ❑ Benötigt einen einzelnen 128-bit Schlüssel
 - Der selbe 128-bit Arbeitsschlüssel wird auf AP und STA eingesetzt.
- ❑ Schlüsselkonfiguration durch 802.1X
- ❑ CCMP verwendet CCM um
 - Datenpakete zu verschlüsseln
 - ausgewählte Header-Felder vor Verfälschung zu sichern
- ❑ CCM = Counter Mode Encryption mit CBC-MAC Data Origin Authenticity mit einem einzigen Schlüssel
 - Verlangt einen 128 bit block cipher – IEEE 802.11i verwendet AES
 - Die Anforderungen von AES verlangen neue AP Hardware
 - Die Anforderungen von AES können neue Hardware bei Handheld-Geräten bedingen, aber nicht bei PCs



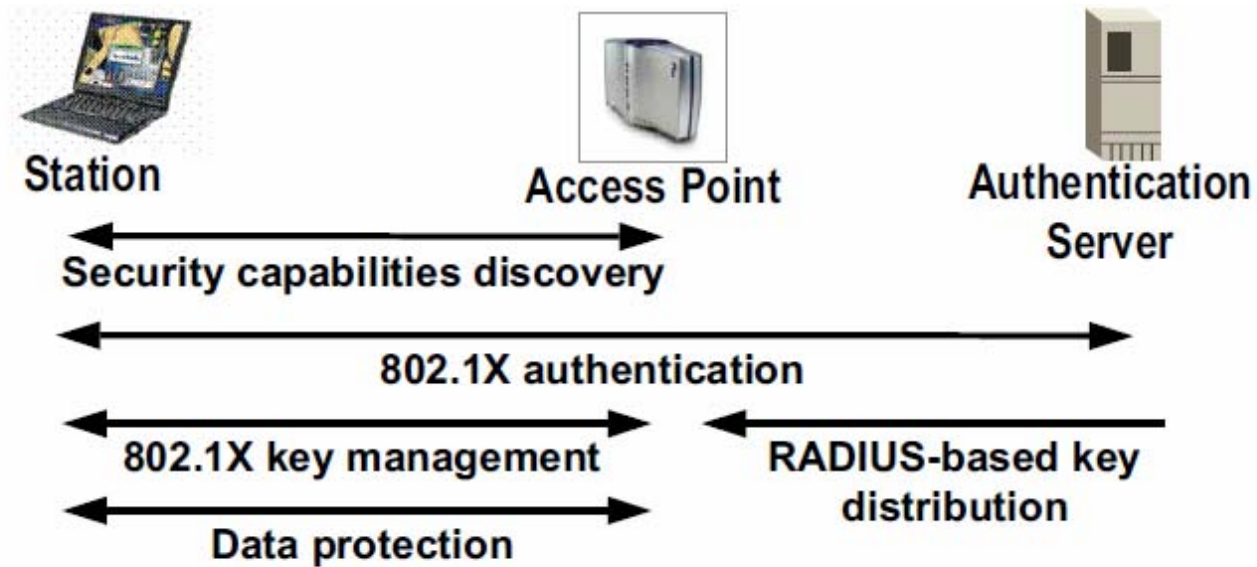


Zusammenfassung: Datentransport

	<u>WEP</u>	<u>TKIP</u>	<u>CCMP</u>
<i>Cipher</i>	RC4	RC4	AES
<i>Key Size</i>	40/104 bits	128 bits Encr. 64 bit auth	128 bits
<i>Key Life</i>	24-bit IV, wrap	48-bit IV	48-bit IV
<i>Packet Key</i>	Concat.	Mixing Fnct.	Not Needed
<i>Integrity</i>			
<i>Data</i>	CRC-32	Klartext	CCM
<i>Header</i>	None	Klartext	CCM
<i>Replay</i>	None	Use IV	Use IV
<i>Key Mgmt.</i>	None	EAP-based	EAP-based



802.11 Betriebsablauf für die Einrichtung einer gesicherten Verbindung



Ablaufphasen

- *Discovery*
- *Authentication*
- *Key Management*

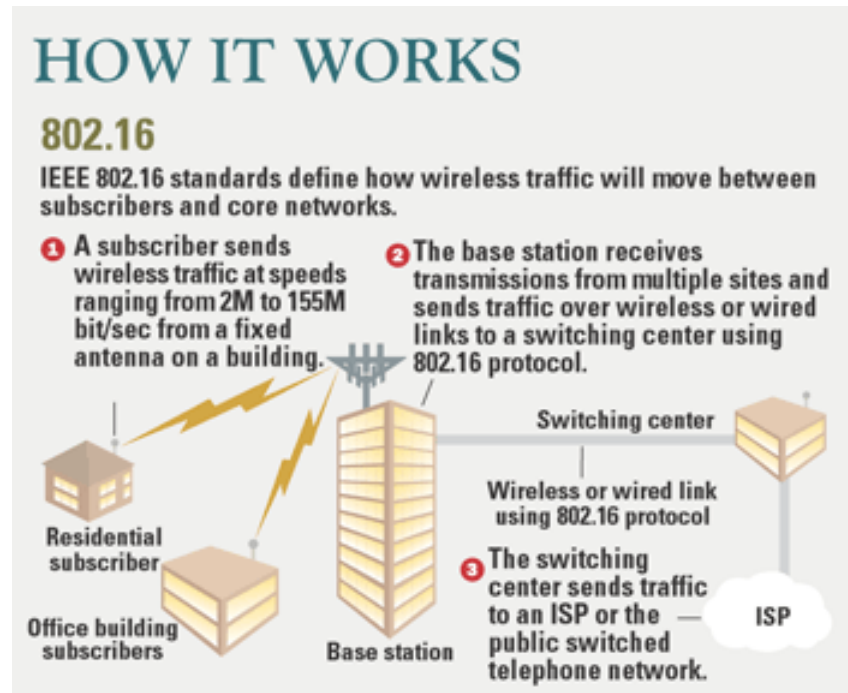
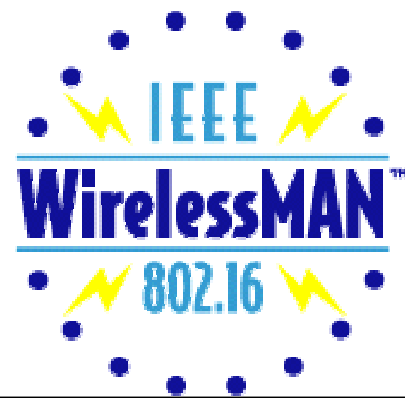


WiMax

(Worldwide Interoperability for Microwave Access)



- Basierend auf den IEEE 802.16.1, IEEE 802.16.2 und IEEE 802.16.
- Operiert im Bereich von 2 – 66 Ghz,
- Ist eine Point-to-Multipoint Architektur
- Reichweite bis ca. 18 KM mit 2M - 155 Mbit/sec
- Zielt auf die „Last Mile“ ab



Übungen



- Frage: Was ist der Unterschied zwischen CSMA/CA und CSMA/CD?
- Frage: Welche Leistungsunterschiede (Reichweite und Übertragung) gibt es zwischen den 3G-Netzen und Wi-Max. Welche Technologie wird sich nach Ihrer Meinung am Markt durchsetzen und warum?
- Frage: Warum ist ein „Roaming“ in FHSS-Netzen problematisch und worauf ist dies zurückzuführen?





Literatur

- <http://www.tu-darmstadt.de/vv/20.183.1>
- **Barnes, C. et al.: Die Hackerbibel für Wireless LANs, MITP-Verlag 2002, ISBN 3-826-0930-1**
- **Nett, E; Mock, M; Gergeleit, M.: Das drahtlose Ethernet, Addison-Wesley-Verlag 2001, ISBN 3-8272-1741-X**
- **IEEE Standard 802.11: Wireless LAN Medium Access Control (MAC) and Physical (PHY) specifications, 1997.**
- **ISO/IEC 8802.11, 1999: ANSI/IEEE Standard 802.11 Wireless LAN Medium Access Control (MAC) and Physical (PHY) specifications, 1999.**
- **IEEE Standard 802.11a-1999 Supplement to IEEE 802.11: High Speed Physical Layer in the 5 GHz-Band.**
- **IEEE 802.11b-1999 Supplement to IEEE 802.11: High Speed Physical Layer in the 2,4 GHz-Band.**

