Rechnernetze II

SoSe 2020

Roland Wismüller
Betriebssysteme / verteilte Systeme
roland.wismueller@uni-siegen.de
Tel.: 0271/740-4050, Büro: H-B 8404

Stand: 25. Mai 2020

Rechnernetze II

SoSe 2020

3 Drahtlose Netze

Inhalt

- WLAN (IEEE 802.11)
- Bluetooth (IEEE 802.15)

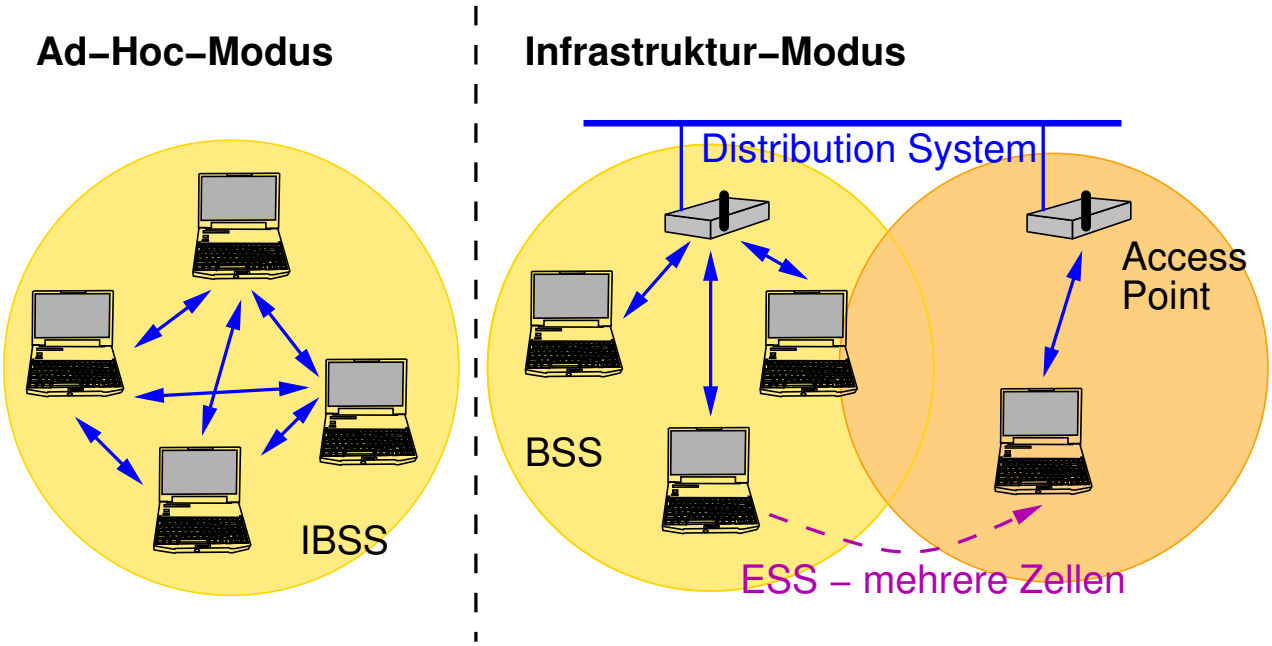
- Tanenbaum, Kap. 1.5.4, **4.4**, **4.6**
- Peterson, Kap. **2.8**
- Axel Sikora: Wireless LAN, Addison Wesley, 2001.
- Jörg Rech: Wireless LANs, 2. Auflage, Heise Verlag, 2006.
- Edgar Nett, Michael Mock, Martin Gergeleit: Das drahtlose Ethernet, Addison-Wesley, 2001.

3.1 WLAN (IEEE 802.11)

Hintergrund

- Drahtlose Netzanbindung von mobilen Geräten
- Sicherungsschicht kompatibel zu Ethernet
- Unterstützung für zwei Betriebsmodi:
  - Ad-Hoc-Modus: Endgeräte kommunizieren direkt
    - IBSS (*Independent Basic Service Set*)
  - Infrastruktur-Modus: Kommunikation über *Access Point*
    - BSS (*Basic Service Set*): eine Funkzelle
    - ESS (*Extended Service Set*): mehrere Funkzellen, über ein anderes Netz (z.B. Ethernet oder auch WLAN) verbunden

WLAN-Betriebsmodi



802.11 Protokollstack

Höhere Schichten					
Logical Link Control (802.2, wie bei Ethernet)					
MAC–Teilschicht: CSMA/CA, MACAW					
802.11 IR / 2.4 GHz FHSS/DSSS 2 Mb/s	802.11a 5 GHz OFDM 54 Mb/s	802.11b 2.4 GHz HR–DSSS 11 Mb/s	802.11g 2.4 GHz OFDM 54 Mb/s	802.11n 2.4/5 GHz OFDM/MIMO – 600 Mb/s	802.11ac 5 GHz OFDM/MIMO – 1.69 Gb/s

Siche–rungs–schicht

Bitüber–tragungs–schicht

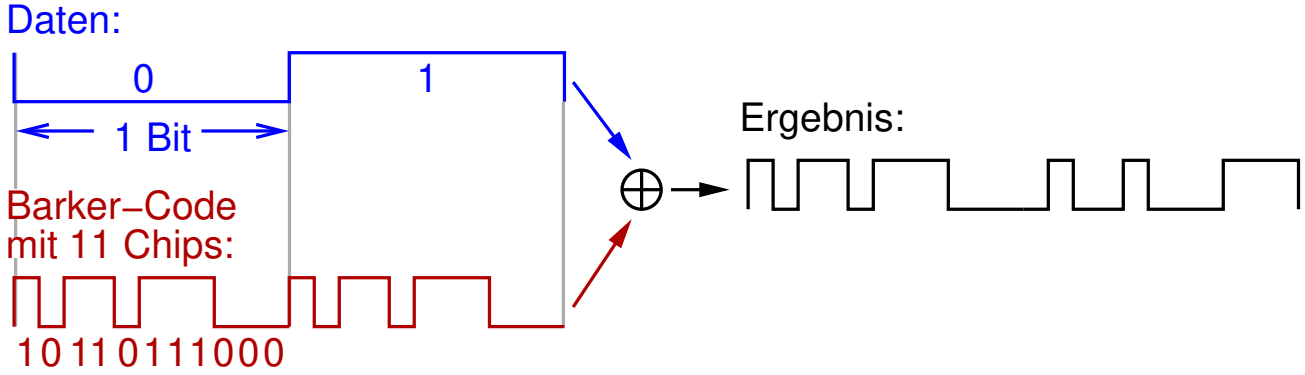
➥ Im Folgenden: Schwerpunkt auf 802.11b und 802.11g

Basis der Funkübertragung: Spreizbandtechnik

- Problem: 802.11 arbeitet in feigegebenen ISM-Bändern
  - ISM: Industrial, Scientific, Medical
  - 2,4 GHz und 5 GHz
- Maßnahme gegen Funkstörungen:
  - Übertragung in möglichst breitem Frequenzband
  - Störungen sind meist schmalbandig
- Techniken:
  - FHSS (*Frequency Hopping Spread Spectrum*)
    - viele Kanäle, Frequenz wechselt pseudozufällig
  - OFDM (*Orthogonal Frequency Division Multiplexing*)
    - im Prinzip ähnlich zu DMT (☞ **1.6**: ADSL)

Basis der Funkübertragung: Spreizbandtechnik ...

- Techniken ...:
  - DSSS (*Direct Sequence Spread Spectrum*)
    - Sendedaten werden mit (fester!) Pzeudozufallsfolge höherer Bitrate XOR-verknüpft
    - Muster leicht aus verrauschtem Signal „herauszuhören“

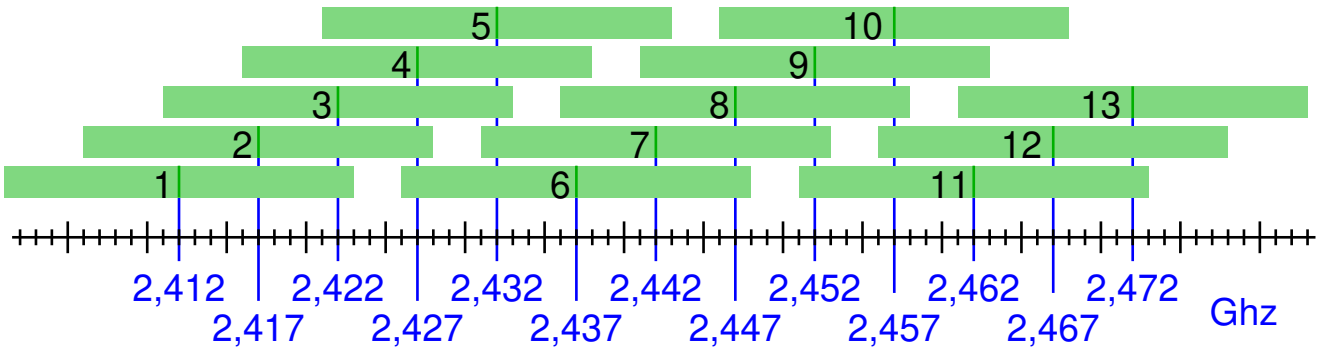


Basis der Funkübertragung: Spreizbandtechnik ...

- Techniken ...:
  - HR-DSSS (*High Rate DSSS*)
    - verkürzte Codelänge: 8 Chips
    - QPSK-artige Modulation
      - 4 Bit / Symbol (für 5.5 Mb/s)
      - 8 Bit / Symbol (für 11 Mb/s)
    - benötigt höheren Rauschabstand

Frequenzbänder im 2.4 GHz Band

- 13 Kanäle (Europa)
- Bandbreite eines Kanals bei 802.11b: 22 MHz
- Kanäle überlappen!
  - bei 802.11b max. 3 nicht überlappende Kanäle möglich



Anmerkungen zu Folie 85:

- In USA sind nur die Kanäle 1-11 erlaubt.
- Japan gestattet auch noch die Verwendung von Kanal 14.
- Ein Mikrowellenherd „sendet“ auf der Frequenz 2,455 GHz und stört somit die Kanäle 9 und 10 erheblich.
- Bei 802.11g sind die Kanäle nur 20 MHz breit, so daß in Europa die Kanäle 1, 5, 9 und 13 überlappungsfrei verwendet werden können.
- Im 802.11n Standard kann sowohl das 2.4 GHz Band als auch das 5 GHz Band verwendet werden. Ausserdem sind auch doppelt so breite Kanäle mit 40 MHz Bandbreite möglich.
- Der 802.11ac Standard verwendet nur das 5 GHz Band. Die Kanäle sind hier 20, 40, 80 oder 160 MHz breit.
- In Europa stehen im 5 GHz Band insgesamt 19 Kanäle mit jeweils 20 MHz Bandbreite zur Verfügung:
  - Kanal 36, 40, 44, ..., 64: 5.150 bis 5.350 MHz
  - Kanal 100, 104, 108, ..., 140: 5.470 bis 5.725 MHz

85-1

3.1.1 Bitübertragungsschicht ...

WLAN nach IEEE 802.11g

- Bruttodatenrate bis 54 Mbit/s (netto max. 50%)
- Verwendet OFDM wegen Mehrfachempfang durch Reflexionen
  - Problem verschärft sich bei höherer Bitrate
  - daher: parallele Übertragung auf mehreren (48) Unterkanälen
- Unterschiedliche Modulationsarten (z.B. QAM-16, QAM-64)
  - Symbolrate: 250 kHz
- Vorwärts-Fehlerkorrektur
  - Code-Rate 1/2, 2/3 oder 3/4 (Nutzdaten / Gesamtdaten)
- Zur Kompatibilität mit 802.11b:
  - 802.11g-Geräte unterstützen i.d.R. auch DSSS

Medienzugriffssteuerung (MAC)

- CSMA/CD ist nicht möglich
  - Funkgeräte arbeiten im Halbduplex-Modus
  - während des Sendens kein Mithören möglich
  - nur Empfänger „erkennt“ Kollision (durch Prüfsumme)
- In IEEE 802.11 zwei Modi für Zugriffssteuerung:
  - DCF (*Distributed Coordination Function*)
    - dezentrales Verfahren (CSMA/CA, MACAW)
  - PCF (*Point Coordination Function*)
    - zentrale Steuerung durch den *Access Point*
  - beide Modi können gleichzeitig genutzt werden

Anmerkungen zu Folie 87:

Inzwischen wird auch an Vollduplex-WLAN geforscht, insbes. an der Univ. Stanford. Der Trick dabei ist, zwei Sendeantennen und eine Empfangsantenne zu verwenden, wobei die Empfangsantenne genau an der Stelle platziert wird, wo sich die Signale der Sendeantennen durch Interferenz (nahezu) auslöschen.

Innerhalb der IEEE gibt es seit Anfang 2013 ein Projekt *High Efficiency WLAN*, das u.a. die Unterstützung von Vollduplex beim WLAN untersucht.

DCF: CSMA/CA

- *Carrier Sense Multiple Access / Collision Avoidance*
  - *Avoidance* heißt hier: **möglichst** vermeiden
  - Kollisionen sind aber immer noch möglich
- Vorgehen im Prinzip wie bei CSMA/CD:
  - Abhören des Mediums, senden sobald Medium frei
- Unterschiede:
  - keine Kollisionserkennung beim Senden
    - Empfänger muß jeden Frame bestätigen (ACK-Frame)
  - vor dem Senden muß das Netz immer mindestens für eine bestimmte Zeit abgehört und als frei erkannt werden:
    - IFS (*Interframe Spacing*)
  - Medium belegt: zufällige Wartezeit zur Kollisionsvermeidung

Anmerkungen zu Folie 88:

Wenn eine Station senden will und das Medium zu diesem Zeitpunkt frei findet, darf sie nach Ablauf des IFS senden (wenn während dieser Zeit das Medium noch frei blieb).

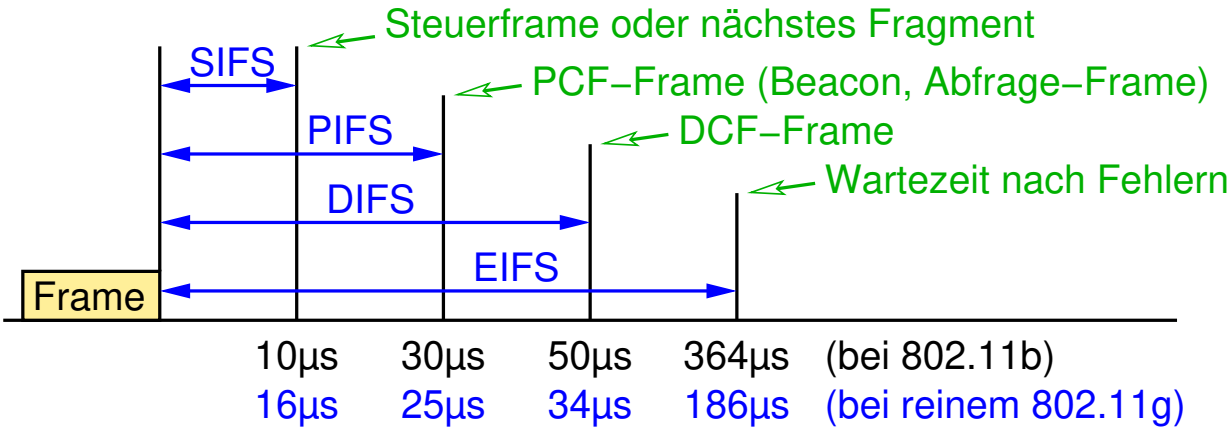
Wenn eine Station senden will und das Medium belegt findet, muß sie nach dem Freiwerden des Mediums das IFS und zusätzlich noch eine Backoff-Zeit abwarten. Ist während dieser ganzen Zeit das Medium weiterhin frei geblieben, darf die Station senden.

Die Backoff-Zeit ist beim ersten Sendeversuch $n \cdot 20\mu s$, wobei $n \in [0, 31]$ zufällig gewählt wird. Die Obergrenze dieses Intervalls wird bei jedem erneuten Sendeversuch (Wiederholung des Frames nach Ausbleiben eines ACKs) verdoppelt, wobei das Maximum 1023 beträgt.

Durch die zufällige Backoff-Zeit wird die Wahrscheinlichkeit verringert, daß nach dem Freiwerden des Mediums mehrere Stationen gleichzeitig zu senden beginnen (was eine Kollision zur Folge hätte)

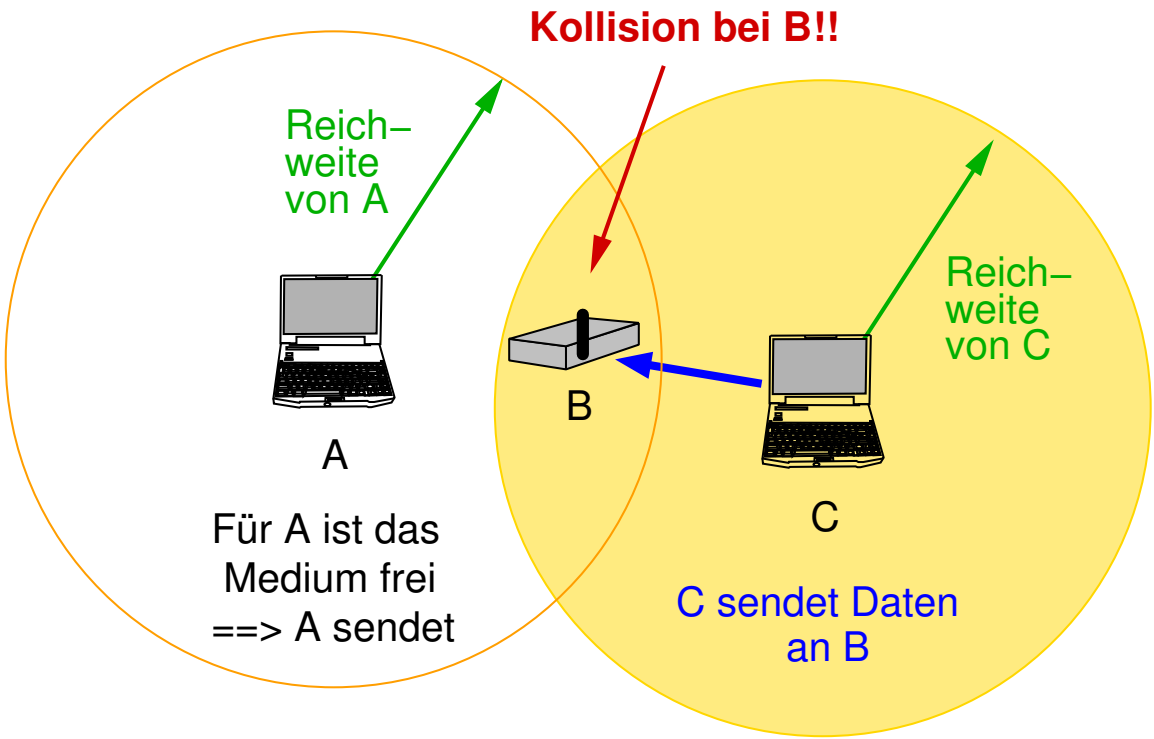
Interframe Spacing (IFS)

- Gibt an, wie lange eine Station das Medium mindestens als frei erkennen muß, bevor sie senden darf
- Unterschiedliche IFS-Zeiten für verschiedene Frame-Typen
  - damit: Realisierung unterschiedlicher Prioritäten



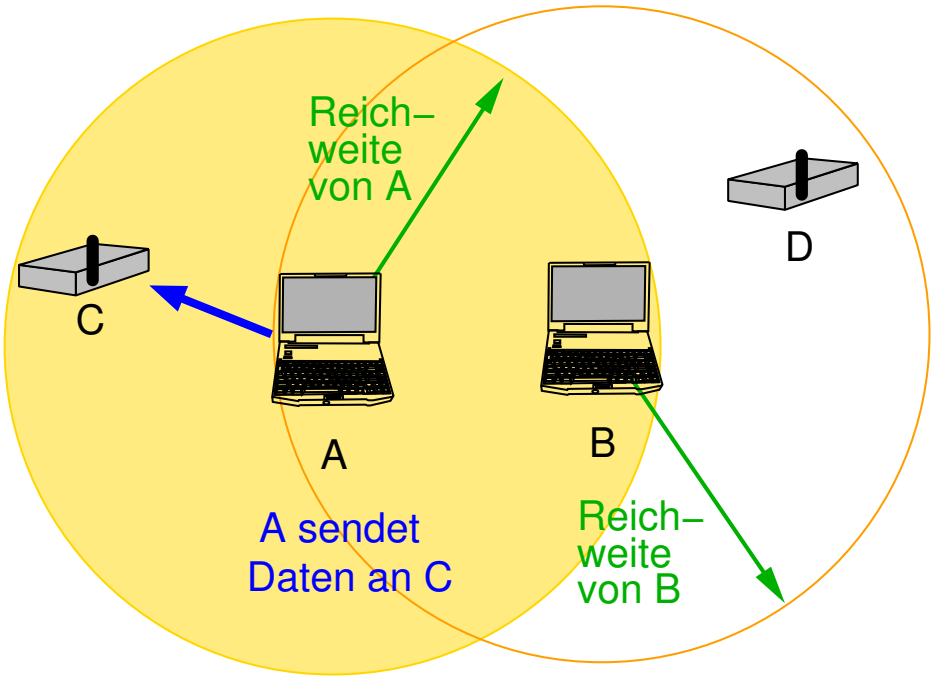
(Animierte Folie)

Das Hidden-Station-Problem



(Animierte Folie)

Das Exposed-Station-Problem



B will an D senden, glaubt aber, daß dies eine Kollision hervorruft

Das MACA - Protokoll (*Multiple Access, Collision Avoidance*)

1. Sender sendet RTS (*Request To Send*) an Empfänger
2. Empfänger antwortet mit CTS (*Clear To Send*)
   - ➥ CTS-Frame enthält Dauer der Übertragung
3. Sender sendet Daten

- ➥ Wer RTS hört, sendet nicht, bis CTS übertragen sein sollte
  - ➥ Zeit ergibt sich aus Framelängen und Signallaufzeit
- ➥ Wer CTS hört, sendet nicht vor Ablauf der Übertragungsdauer
  - ➥ löst *Hidden Station* Problem
- ➥ Wer CTS nicht hört, kann gleichzeitig senden
  - ➥ löst *Exposed Station* Problem
- ➥ Wenn zwei RTS kollidieren, kommt kein CTS $\Rightarrow$ *Backoff*

Anmerkungen zu Folie 92:

In der Situation von Folie 90 können auch bei MACA zwei RTS-Frames kollidieren: C sendet RTS an B, A kann diese Sendung nicht hören und sendet ebenfalls. Es kommt zur Kollision bei B. Es stellt sich also die Frage, warum (bzw. wann) MACA eine Verbesserung der Situation bringt.

Die Antwort ist die Tatsache, daß Datenframes i.a. länger sind als ein RTS-Frame. Die Wahrscheinlichkeit, daß eine andere Station während der Übertragung des Frames zu senden beginnt, ist damit bei einem (kurzen) RTS-Frame kleiner als bei einem (langen) Daten-Frame.

Falls trotzdem eine Kollision auftritt, geht zudem bei MACA nicht so viel Zeit verloren, da neu der kurze RTS-Frame statt eines langen Datenframes neu übertragen werden muß.

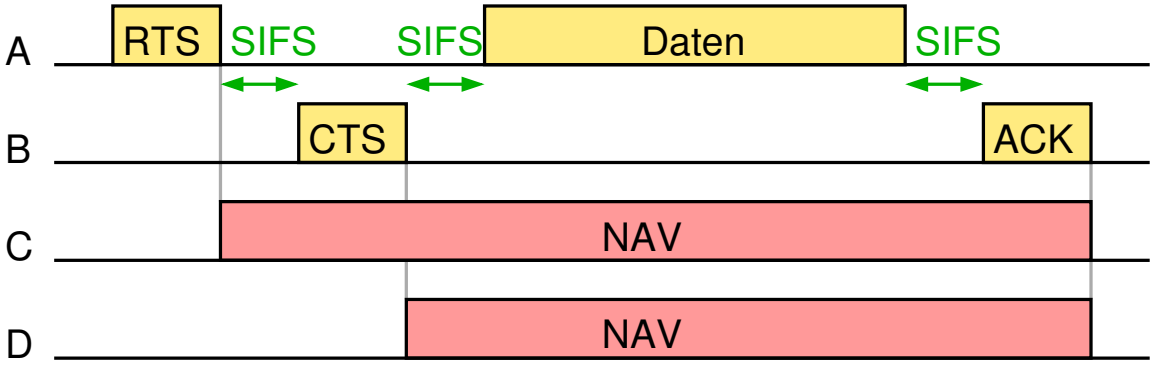
Da MACA auch einen Overhead bedingt, rentiert sich das Protokoll daher nur bei der Übertragung langer Frames.

3.1.2 Sicherungsschicht ...

MACAW - Erweiterung von MACA für WLAN

- Einführung von ACKs, um Neuübertragung durch Sicherungsschicht zu ermöglichen
  - schneller, da kürzere Timeouts als z.B. bei TCP
- Modifikationen gegenüber MACA:
  - Empfänger bestätigt Empfang der Daten mit ACK
  - Station, die RTS hört, darf nicht senden, bis ACK übertragen wurde
    - Übertragung könnte mit ACK kollidieren
  - auch RTS-Frame enthält Dauer der Übertragung
- 802.11 verwendet MACAW zum Versenden längerer Frames
  - für kurze Frames: einfaches CSMA/CA

MACAW - Beispiel

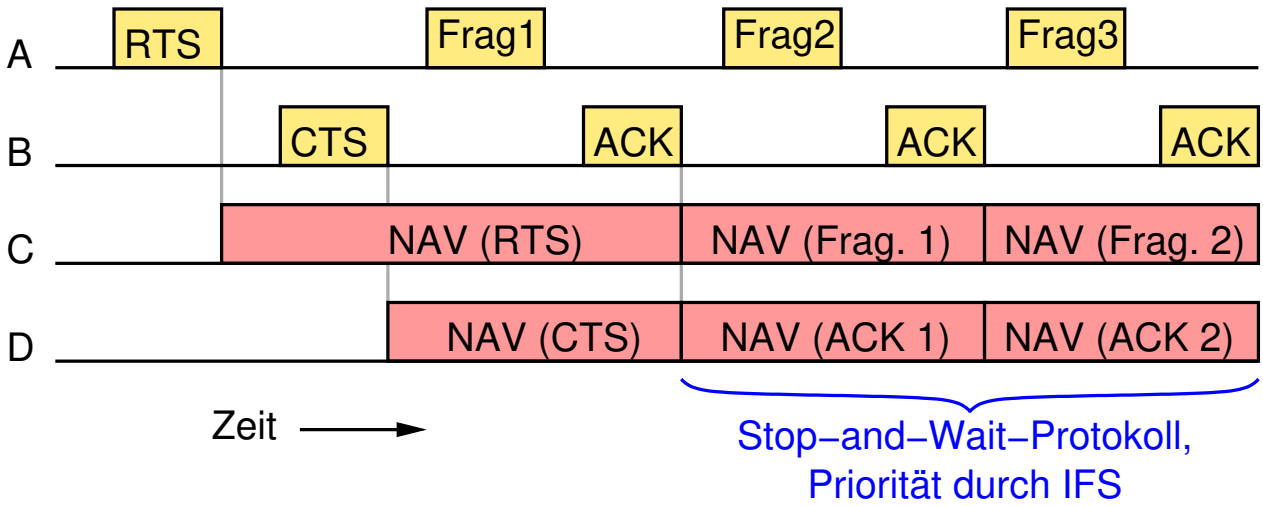


B und C sind in Reichweite von A, D nicht

NAV: *Network Allocation Vector* (Netz ist belegt, kein Senden)

Fragmentierung

- Frames können in mehreren Fragmenten übertragen werden
  - erhöht Effizienz bei hoher Bitfehlerrate



Anmerkungen zu Folie 95:

Der Vorteil dieses Vorgehens ist, daß das Medium nicht für die gesamte Zeit im Voraus reserviert werden muß. Zum einen kann dadurch die Reservierung dynamisch verlängert werden, um Fragemente neu zu übertragen, zum anderen wird das Medium bei einem Abbruch der Übertragung früher wieder freigegeben.

3.1.2 Sicherungsschicht ...

Koexistenz von 802.11b und 802.11g

- Problem: 802.11b-Station erkennt nicht, daß 802.11g-Station sendet
- Lösung: *Protection*-Mechanismus
  - wird vom *Access-Point* aktiviert, wenn dieser eine 802.11b-Station erkennt
- Zwei Verfahren:
  - **CTS-to-Self:** 802.11g-Station sendet vor der eigentlichen Übertragung ein CTS mit DSSS, das das Medium reserviert
  - **RTS/CTS:** RTS, CTS und ACK werden mit DSSS übertragen, nur Datenframes werden mit OFDM gesendet
- Nachteil: Nutzdatenrate sinkt deutlich ($\sim$ 10-15 Mbit/s)

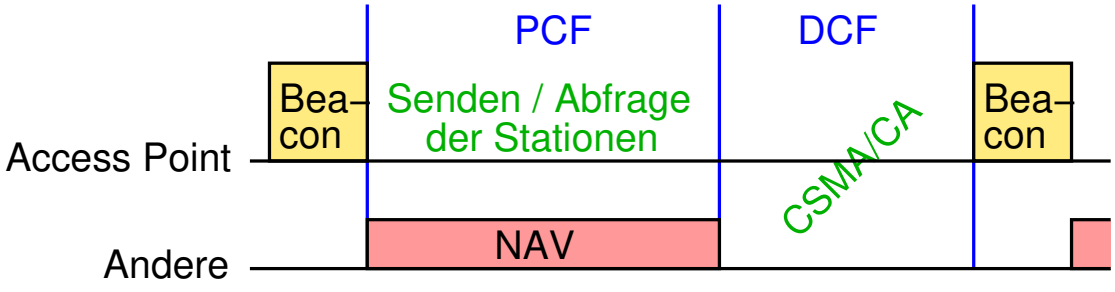
Anmerkungen zu Folie 96:

- Wenn der *Access Point* eine 802.11b-Station erkennt, sendet er seine *Beacon*-Frames mit DSSS und setzt dort ein spezielles *Use-Protection*-Feld, um allen anderen Stationen die Anwesenheit von 802.11b-Geräten anzuzeigen.
- Zum RTS/CTS-Verfahren: Da (z.B. bei Fragmentierung) auch normale Datenframes das Medium über den NAV reservieren können, werden bei den Datenframes tatsächlich auch die Header mit DSSS übertragen. Lediglich der Nutzdatenteil wird mit OFDM gesendet.

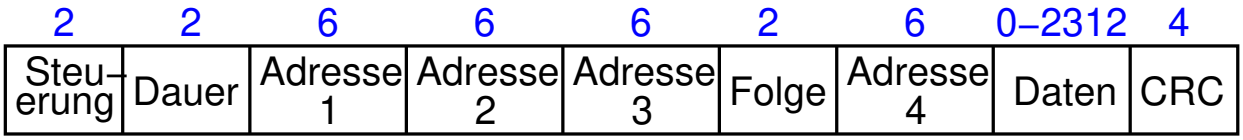
3.1.2 Sicherungsschicht ...

PCF: TDMA (*Time Division Multiple Access*)

- *Access Point* sendet regelmäßig *Beacon*-Frame als Broadcast
  - enthält verschiedene Systemparameter
  - kann Medium für bestimmte Zeit reservieren (über NAV)
    - in dieser Zeit: Stationen, die sich für PCF angemeldet haben, werden vom *Access Point* einzeln abgefragt
  - danach: normaler DCF-Betrieb bis zum nächsten *Beacon*



Frame-Format (für Daten-Frames)



- **Steuerung**: Frame-Typ, Frame von/an *Distribution System*, Verschlüsselung, *Power Management*, ...
- **Dauer**: für Belegung des Kanals über NAV
- **Adresse 1-4**: IEEE 802 MAC-Adressen
  - Quell- und Ziel-Rechner
  - BSS-ID bzw. Quell- und Ziel-*Access-Point*
- **Folge**: Numerierung von Fragmenten

Anmerkungen zu Folie 98:

Die genaue Nutzung der Adreßfelder ist wie folgt:

To DS	From DS	Address 1	Address 2	Address 3	Address 4
0	0	DA	SA	BSSID	N/A
0	1	DA	BSSID	SA	N/A
1	0	BSSID	SA	DA	N/A
1	1	RA	TA	DA	SA

SA = Quellrechner, DA = Zielrechner,
RA = Ziel-*Access-Point*, TA = sendender *Access-Point*,
BSSID = MAC-Adresse des *Access-Points*

Die letzte Zeile kennzeichnet einen Frame, der zwischen zwei *Access-Points* verschiedener Funkzellen eines ESS ausgetauscht wird (wobei als *Distribution System* auch das WLAN verwendet wird).

Nicht in jedem Frame sind alle Adressfelder enthalten. Z.B. fehlt das Feld „Address 4“, wenn es nicht benötigt wird. ACK-Frames enthalten nur das Feld „Address 1“ mit der Zieladresse.

3.1.3 WLAN Sicherheit

Sicherheitsmechanismen

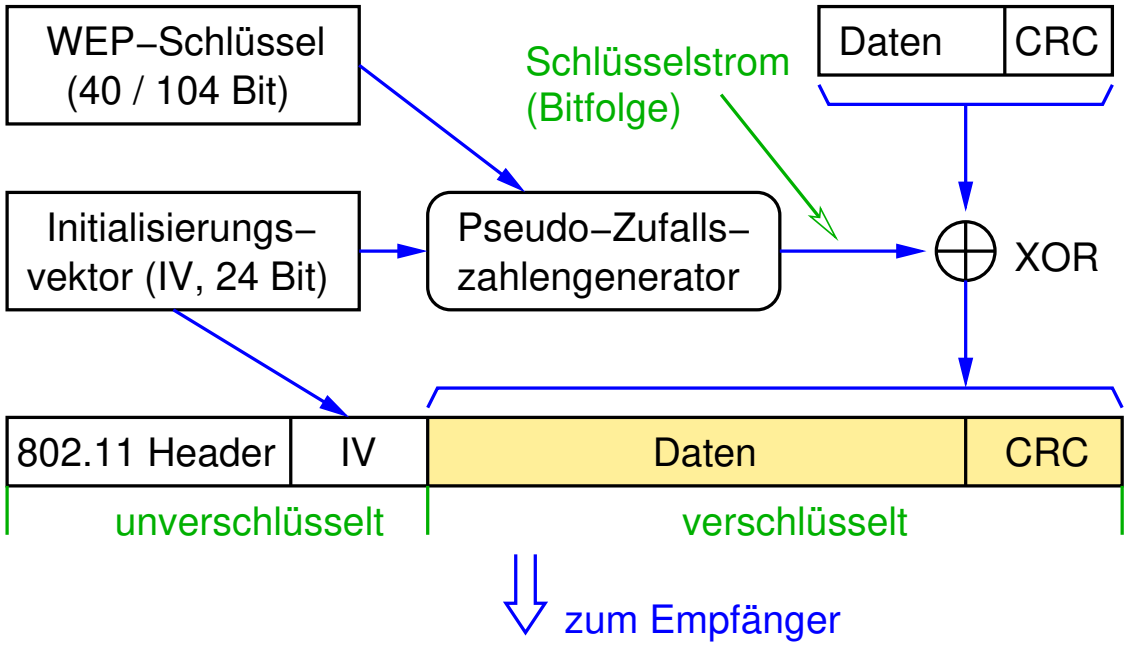
- ESSID (*Extended Service Set IDentifier*): Name des Netzes
  - muß i.a. zum Anmelden an *Access Point* bekannt sein
  - wird i.d.R. vom *Access Point* im *Beacon*-Frame mitgesendet
  - viele WLAN-Karten akzeptieren auch „*any*“
- Authentifizierung über MAC-Adresse
  - Basisstation hat Liste der erlaubten MAC-Adressen
  - viele WLAN-Karten erlauben Änderung der MAC-Adresse!
- Verschlüsselung
  - WEP (*Wire Equivalent Privacy*, IEEE 802.11)
    - 40 (bzw. 104) Bit Schlüssel, veraltet
  - WPA und WPA2 (*Wi-Fi Protected Access*, IEEE 802.11i)
    - deutlich bessere Sicherheit als WEP

3.1.3 WLAN Sicherheit ...

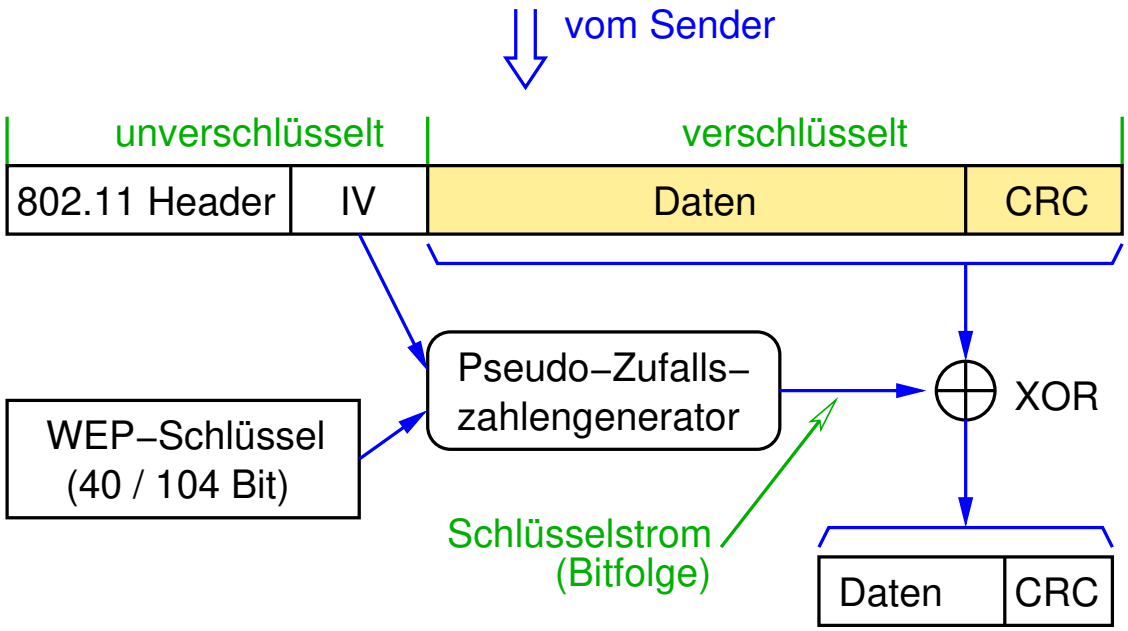
WEP: Funktionsweise

- Basis: symmetrische Verschlüsselung mit RC4 Stromchiffre
  - Daten werden mit Pseudozufalls-Bitfolge EXOR-verknüpft
  - Bitfolge kann aus Schlüssel und Initialisierungsvektor (IV) eindeutig bestimmt werden
  - Schlüssel (40 bzw. 104 Bit) muß allen Stationen bekannt sein
  - Initialisierungsvektor wird für jede Übertragung neu gewählt und (unverschlüsselt) mitübertragen
- Authentifizierung der Teilnehmer durch *Challenge-Response* -Protokoll

WEP-Verschlüsselung beim Sender



WEP-Entschlüsselung beim Empfänger



WEP: Schwachstellen

- Verschlüsselung ist angreifbar (Problem: Schlüsselerzeugung)
- Verschlüsselung erfolgt immer direkt mit WEP-Schlüssel
  - macht Schlüssel durch Kryptoanalyse angreifbar
- CRC ist bezüglich $\oplus$ linear $\Rightarrow$ Angreifer kann nach Manipulation der Daten verschlüsselten CRC neu berechnen
- IV ist zu kurz: wiederholt sich nach wenigen Stunden
  - wiederholte Verwendung desselben Schlüsselstroms
  - Schlüsselstrom kann durch Klartextangriff ermittelt werden
    - *Challenge-Response* - Protokoll bei Authentifizierung!
- WEP ist unsicher! $\Rightarrow$ WPA bzw. WPA2 verwenden!!!

Anmerkungen zu Folie 103:

Die Linearität des CRC bedeutet:

$$CRC(x \oplus y) = CRC(x) \oplus CRC(y)$$

Zusammen mit der Eigenschaft der RC4-Stromchiffre

$$E(m \oplus x) = E(m) \oplus x$$

läßt dies eine gezielte Manipulationen der (verschlüsselten) Nachricht zu, bei der auch der (verschlüsselte) CRC-Wert so modifiziert wird, daß der Empfänger die Manipulation nicht erkennen kann (siehe Übungsaufgabe!).

IEEE 802.11i: verbesserte Sicherheitsstandards

- Bessere Verschlüsselung als WEP, sichere Integritätsprüfung
  - Ziel: schrittweiser Übergang unter Weiterverwendung vorhandener Hardware
  - daher Übergangslösung über Firmware-Update
    - ersetze WEP-Verschlüsselung durch TKIP
    - zusätzlich: Integritätsprüfung über Hash-Funktion
      - MIC: *Message Integrity Check*
  - endgültige Lösung (erfordert neue Hardware)
    - AES-CCMP (*Advanced Encryption Standard*)
- Verbesserte Authentifizierung (inkl. Schlüsselmanagement)
  - über Authentifizierungsserver (IEEE 802.1X, EAP)
  - oder über *Pre-Shared Key* (PSK)

WPA, WPA2: Quasi-Standard der Wi-Fi Alliance

- Die IEEE-Standardisierung dauerte zu lange ...
  - WPA entspricht (in etwa) Übergangslösung von IEEE 802.11i
  - WPA2 entspricht (in etwa) IEEE 802.11i
- Jeweils zwei Modi: *Personal* und *Enterprise*

WPA-Variante		**WPA**	**WPA2**
Personal-Mode	Authentifizierung	PSK	PSK
	Verschlüsselung	TKIP/MIC	AES-CCMP
Enterprise-Mode	Authentifizierung	802.1X/EAP	802.1X/EAP
	Verschlüsselung	TKIP/MIC	AES-CCMP

Authentifizierung mit 802.1X und EAP

- 802.1X: Authentifizierung über einen zentralen Server
  - RADIUS-Server (*Remote Authentication Dial-In User Service*)
  - Vorteil: zentrale Administration des Zugangs

- EAP: *Extensible Authentication Protocol* (RFC 2284)
  - zum Austausch der Authentifizierungsnachrichten

Ablauf von Authentifizierung und Schlüsselaustausch

- Client muß gegenüber Authentifizierungsserver seine Identität nachweisen
  - Challenge/Response, z.B. mit Paßwort oder X.509 Zertifikat
- Dabei gleichzeitig: Aushandlung eines Schlüssels
  - PMK: *Pairwise Master Key*
  - wird vom Server auch an *Access Point* geschickt
- Client und *Access Point* bilden aus PMK einen nur ihnen bekannten Schlüssel für diese Sitzung
  - PTK (*Pairwise Transient Key*), für Punkt-zu-Punkt-Kommunik.
- *Access Point* sendet an Client einen Gruppenschlüssel
  - GTK (*Group Transient Key*), verschlüsselt mit PTK
  - für Broadcast- und Multicast-Kommunikation

Anmerkungen zu Folie 107:

- Der *Access Point* implementiert dabei ein *Dual-Port*-Konzept: solange der Client sich nicht authentifiziert hat, leitet der Access Point Frames dieses Clients nur an den Authentifizierungsserver weiter.
- 802.1X ist in dieser Einsatzumgebung unsicher, da der Access Point sich nicht authentifiziert. Somit kann ein unautorisierter Access Point in den Besitz der *Credentials* des Clients kommen. Besser ist daher die Verwendung von PEAP, bei dem Client und Authentifizierungsserver über einen TLS-Tunnel kommunizieren.

Quelle: C. Eckert, IT-Sicherheit, 3. Auflage, S. 835 ff

3.1.3 WLAN Sicherheit ...

Authentifizierung mit PSK (*Pre-Shared Key*)

- PSK wird über Hashfunktion aus Passphrase und SSID gebildet
  - Passphrase wird auf allen Stationen manuell eingetragen
- PSK übernimmt die Rolle des PMK bei Auth. über 802.1X/EAP
  - d.h., Client und *Access Point* bilden aus PSK den PTK
    - unter Einbeziehung von MAC-Adresse und Zufallszahlen
- Nur, wenn Client und *Access Point* denselben PSK besitzen, erhalten sie denselben PTK und können kommunizieren
- PSK wird nicht für die Kommunikation verwendet
  - weniger Angriffspotential, um PSK zu ermitteln
  - trotzdem ist bei Kenntnis des PSK ein Entschlüsseln der Kommunikation anderer Clients möglich
    - Voraussetzung: Schlüsselaustauch wird abgehört

Anmerkungen zu Folie 108:

Der PTK berechnet sich aus dem PSK, je einem *Nonce*-Wert (Zufallszahl) des Clients und des *Access Point*s sowie den MAC-Adressen von Client und des *Access Point*. Da die beiden *Nonce*-Werte beim Schlüsselaustausch im Klartext übertragen werden, kommt man durch Abhören des Schlüsselaustauschs in den Besitz der gesamten Information, die benötigt wird, um aus dem PSK den PTK für den jeweiligen Client zu berechnen und dessen Kommunikation zu entschlüsseln.

Bei der Authentifizierung mit 802.1X gibt es diese Möglichkeit nicht, da bereits für jeden Client ein eigener *Pairwise Master Key* verwendet wird.

Weitere Informationen dazu finden Sie unter

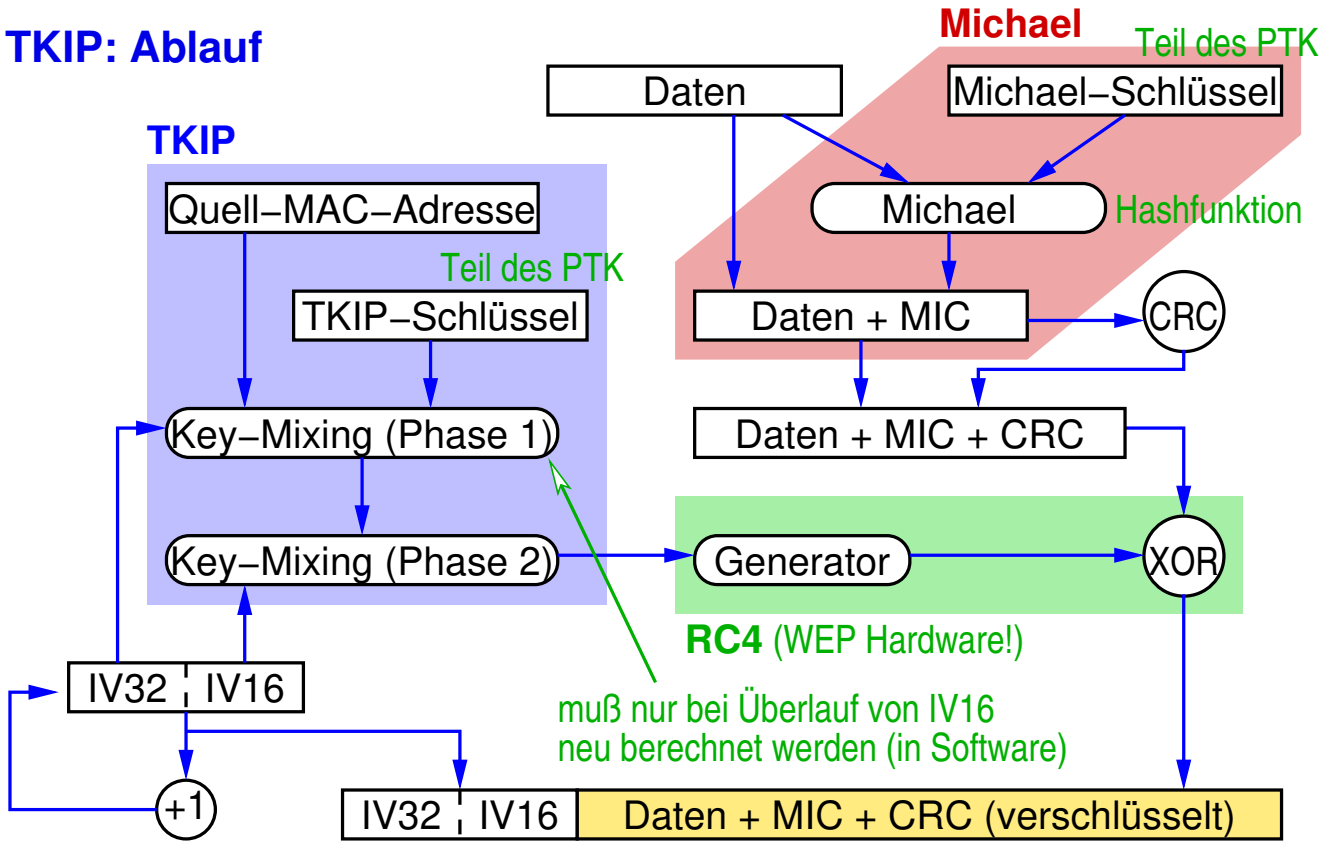
- http://en.wikipedia.org/wiki/IEEE_802.11i-2004
- http://security.stackexchange.com/questions/8591/are-wpa2-connections-with-a-shared-key-secure
- https://wiki.wireshark.org/HowToDecrypt802.11

3.1.3 WLAN Sicherheit ...

TKIP *Temporary Key Integrity Protocol*

- Übergangslösung für Verschlüsselung
  - Verwendung der WEP-Hardware mit neuer Software
- RC4 Verschlüsselung wie bei WEP
- Unterschiede:
  - Initialisierungsvektor (IV) mit 48 Bit
  - IV wird nach jedem Paket inkrementiert, Empfänger prüft Sequenz (Replayschutz)
  - 128 Bit langer TKIP-Schlüssel (Teil des PTK)
    - unterschiedliche Schlüssel für jeden Client
    - zusätzlich: Quell-MAC-Adresse fließt in RC4-Seed mit ein
  - Integritätsschutz (MIC): Hashfunktion mit Schlüssel (Michael)
    - getrennte Schlüssel je Übertragungsrichtung

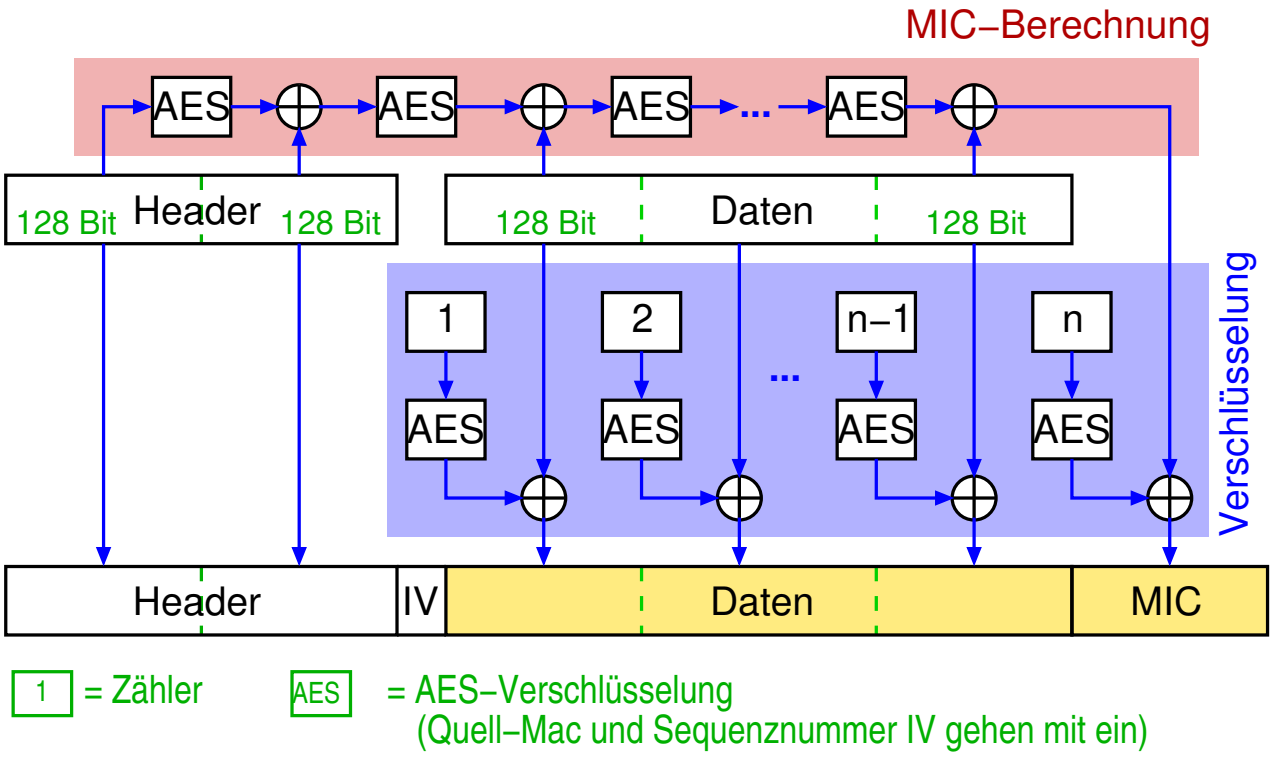
TKIP: Ablauf



AES-CCMP

- AES: vom NIST standardisiertes Verschlüsselungsverfahren
- AES-CCMP = AES *CTR/CBC-MAC Protocol*
  - AES im Zähler-Modus, MIC mittels *Cipher Block Chaining*
  - Integritätsprüfung (Datenteil + Teile des Headers) und Verschlüsselung (Datenteil + MIC)
    - ein gemeinsamer Schlüssel mit 128 Bit
  - benötigt neue Hardware
- 48 Bit Paketzähler mit Sequenzprüfung beim Empfänger
  - Sequenznummer geht mit Quell-MAC-Adresse in Verschlüsselung und Integritätsprüfung mit ein
  - Replayschutz

AES-CCMP: Ablauf (vereinfacht)



Anmerkungen zu Folie 112:

In den MIC fließt auch ein Nonce-Wert (bestehend u.a. aus Quelladresse und Paketzähler des Frames) mit ein, da für die Verschlüsselung und den MIC derselbe Schlüssel verwendet wird, was ansonsten eine potentielle Schwachstelle darstellen würde.

Der Zählermodus zur Verschlüsselung hat zwei Vorteile:

- erhöhte Sicherheit, da auch bei gleichen Klartext-Blöcken verschiedene Chiffre-Blöcke entstehen
- höhere Performance, da die verschlüsselten Zählerwerte schon vorab berechnet werden können

Die Zähler starten dabei nicht (wie im Bild dargestellt) mit dem Wert 1, sondern ebenfalls mit einem Nonce-Wert.

WPA / WPA2 / IEEE 802.11i: Fazit

- AES-CCMP: Sicherheit nach Stand der Technik
- TKIP und Michael: Zwischenlösung für alte Hardware
  - bessere Verschlüsselung als WEP
    - paarweise geheime Schlüssel + Gruppenschlüssel, regelmäßiger Schlüsselwechsel, längerer IV
  - verbesserter Integritätsschutz (Hashwert mit Schlüssel)
  - Replayschutz (durch IV als Sequenznummer)
- PSK: für private / kleine WLANs
  - einfache Nutzung, aber Zugangsberechtigung nicht mehr ohne weiteres entziehbar
- IEEE 802.1X / EAP: für professionellen Einsatz
  - zentrale, flexible Benutzerverwaltung

Anmerkungen zu Folie 113:

Seit Juni 2018 gibt es von der Wi-Fi Alliance eine Spezifikation für WPA3, die bekannte Schwachstellen von WPA2 vermeidet. Insbesondere wurde die Authentifizierung verbessert, um den bei WPA2 möglichen „Key Reinstallation Attack“ (KRACK) zu unterbinden. Unter anderem muß sich bei WPA3 auch der Access Point authentifizieren; offline Wörterbuchattacken auf schwache Passwörter sollten so bei WPA3 nicht mehr möglich sein. Allerdings sind auch bei WPA3 inzwischen Schwachstellen bekannt geworden (siehe `https://wpa3.mathyvanhoef.com/`).

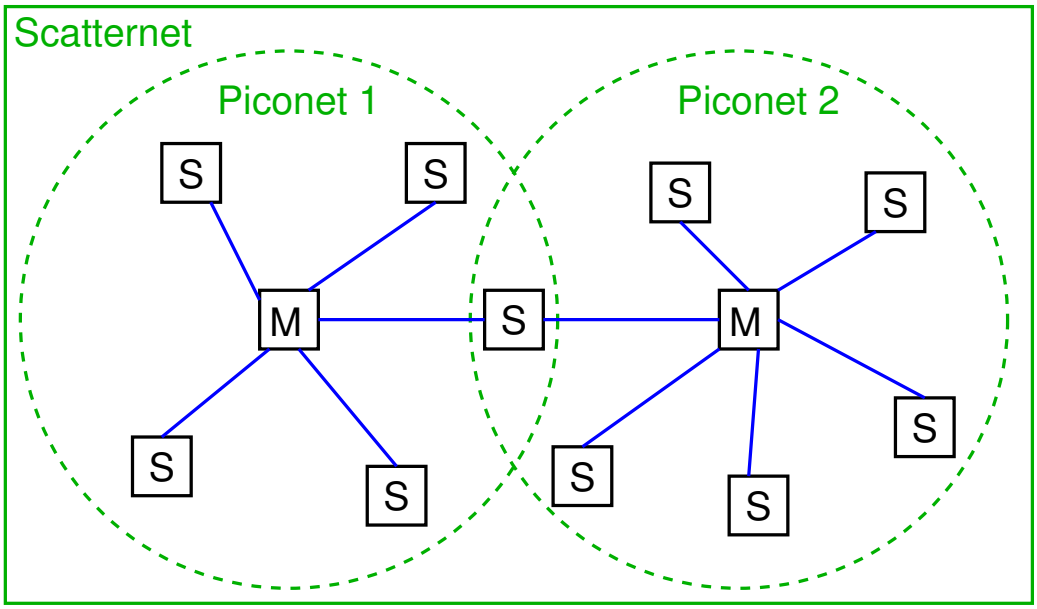
3.2 Bluetooth

3.2.1 Bluetooth Classic

- Ursprüngliches Ziel: Verbindung von Mobiltelefonen mit anderen Geräten (PDA, ...)
  - geringer Stromverbrauch ist wesentlich
  - geringe Reichweite (10 m)
- Definition durch Gruppe mehrerer Unternehmen (1994 -)
  - untere Schichten in IEEE Standard 802.15 übernommen
- Bluetooth definiert Protokollstapel bis zur Anwendungsschicht
  - Zusammenarbeit der Geräte auf Anwendungsebene!
  - Profile für verschiedene Anwendungsbereiche
- benannt nach König Harald II. Blaatand (940-981)
  - vereinte Dänemark und Norwegen

3.2.1 Bluetooth Classic ...

Architektur eines Bluetooth-Netzes



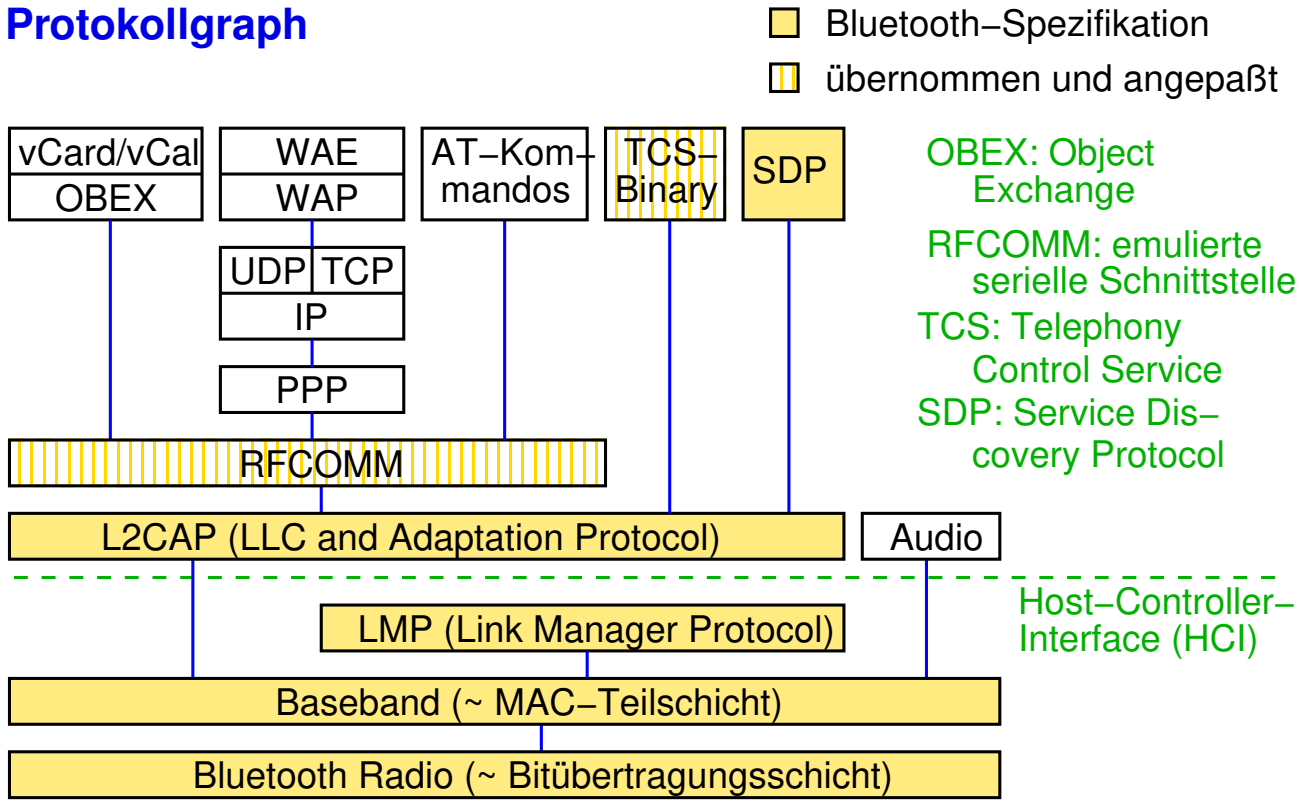
M: Master S: Slave

Architektur eines Bluetooth-Netzes ...

- Grundstruktur: Piconet
  - ein Master, bis zu 7 aktive Slaves
  - zusätzlich bis zu 255 „geparkte“ Slaves (Stromspar-Modus)
  - Medienzugang vollständig durch Master gesteuert (Zeitmultiplex)
- Mehrere Piconets können zu Scatternet verbunden werden
  - Verbindung über gemeinsamen Slave-Knoten als Bridge

(Animierte Folie)

Protokollgraph



Anmerkungen zu Folie 117:

- LMP: Netzverwaltung
  - Verbindungsaufbau zwischen Stationen
  - Authentifizierung, Verschlüsselung
  - Energiesparmodi, Gerätezustände
- L2CAP: Übertragung von Nutzdaten
  - verbindungsorientierte und verbindungslose Dienste
- SDP: erlaubt Abfrage zur Verfügung stehender Dienste
- TCS: Telephondienste
  - Auf- und Abbau von Gesprächen
- AT-Kommandos: zur Steuerung von Modems, Mobiltelefonen und FAX
- WAP: Wireless Application Protocol
- WAE: Wireless Application Environment (Anwendungsschicht von WAP)

3.2.1 Bluetooth Classic ...

Funkschicht

- 2,4 GHz ISM Band
- 79 Kanäle á 1 MHz
- Frequenzsprungverfahren (FHSS)
  - 1600 Umschaltungen/s (alle 625 μs)
  - Sprungfolge wird vom Master vorgegeben
- Frequenzmodulation, Brutto-Datenrate 1 Mbit/s
- Auch 802.11b/g/n verwendet 2,4 GHz Band
  - gegenseitige Störungen!

Anmerkungen zu Folie 118:

Die Daten auf dieser Folie gelten für Version 1.1. Version 2.0+EDR erlaubt eine maximale Netto-Datenrate von 2,1 Mbit/s. Diese wird durch andere Modulationsverfahren mit 2 bzw. 3 Bit pro Abtastung erreicht.

Version 3.0+HS erlaubt über eine Erweiterung des Protokoll-Stacks die Nutzung eines WLAN-Links, der über Bluetooth aufgebaut wird, um bis zu 24 MBit/s zu übertragen.

In der aktuellen Version 4.0 erlaubt *Bluetooth low energy* (BLE) zusätzlich den schnelleren und damit ernergieparenden Aufbau von Links.

3.2.1 Bluetooth Classic ...

Basisband-Schicht (MAC)

- Zeitmultiplex-Verfahren
  - Master beginnt Senden in geraden Zeitschlitzen
  - Slaves beginnen in ungeraden Zeitschlitzen
    - nur nach Erhalt eines Frames vom Master
  - Frames können 1, 3 oder 5 Zeitschlitze lang sein
    - 240 Bit Nutzdaten bei 1 Zeitschlitz
    - 2744 Bit bei 5 Zeitschlitzen
      - mehr als 5 * 240 Bit wegen Übergangszeit bei Frequenzwechsel und Frame-Header

Basisband-Schicht (MAC)

- Übertragung über logische Kanäle (*Links*)
  - ACL (*Asynchronous Connectionless Link*)
    - paketvermittelte Daten, *best effort*
    - pro Slave max. 1 Link
  - SCO (*Synchronous Connection Oriented*)
    - für Echtzeitdaten (Telefonie)
    - feste Zeitschlitze für jede Richtung
    - Vorwärts-Fehlerkorrektur, keine Neuübertragung
      - Code-Raten 1/3, 2/3 und 3/3 (Nutz- / Gesamtdaten)
      - bei 1/3: Daten werden dreimal wiederholt, *Voting*
    - pro Slave max. 3 Links, 64000 Bit/s pro Link
    - Duplex-SCO-Link mit max. Redundanz lastet Netz aus!

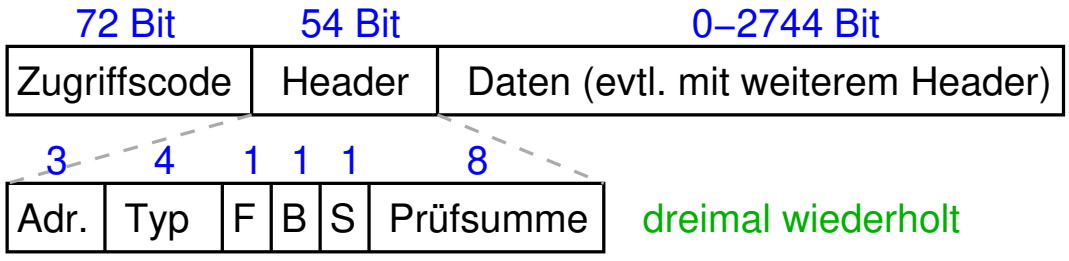
Anmerkungen zu Folie 120:

Ein Duplex-SCO-Link mit maximaler Bitrate und maximaler Redundanz benötigt eine Datenrate von 64000 Bits/s * 3 (Redundanz) * 2 (Duplex) = 384000 Bit/s.
Bei 1600 Frames pro Sekunde und einer Framelänge von 240 Bits stehen auf der anderen Seite auch genau 240 Bit/Frame * 1600 Frames/s = 384000 Bit/s zur Verfügung.

L2CAP-Schicht

- *Logical Link Control Adaptation Protocol*
- Fragmentierung und Wiederzusammenbau von Paketen
  - Pakete bis 64 KB
- Multiplexen und Demultiplexen
  - Weitergabe von Paketen an höhere Protokolle
- Aushandlung / Verwaltung von Dienstgüte-Anforderungen
  - z.B. maximale Paketgröße

Frame-Format



- **Zugriffscode** identifiziert Master (d.h. Piconet)
- 3-Bit **Adresse** (7 Slaves + Broadcast durch Master)
- **Typ**: ACL, SCO, Polling, Fehlerkorrektur, Zeitschlitze, ...
- **F**: Flußkontrolle (Empfangspuffer ist voll)
- **B**: Bestätigung (ACK)
- **S**: Sequenzbit (*Stop-and-Wait*-Verfahren)

Sicherheit

- 3 Modi: keine Sicherheit, Sicherheit auf Diensteebene, Authentifizierung und Verschlüsselung auf Link-Ebene
- Bei erster Verbindungsaufnahme: *Pairing*
  - beide Geräte benötigen identische PIN (1-16 Bytes, fest installiert bzw. Benutzereingabe)
- Aus PIN werden Schlüssel berechnet: 8(!) - 128 Bit
- Authentifizierung und Verschlüsselung mit unterschiedlichen Chiffren (SAFER+ bzw. E0-Stromchiffre)
- Schwächen:
  - feste Geräteschlüssel möglich (für alle Verbindungen)
  - nur Geräte-, keine Benutzer-Authentifizierung
  - kein Replay-Schutz

Anmerkungen zu Folie 123:

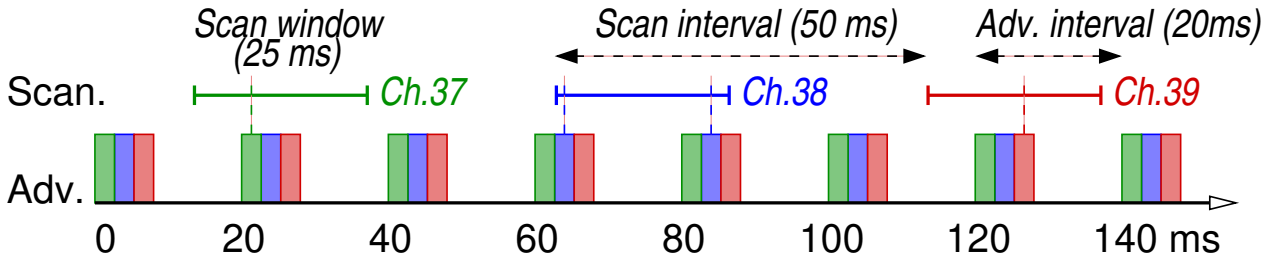
Im Sicherheitsmodus 3 (*Link-Level Enforced Security*) ist die Verschlüsselung vor Version 2.1 optional. Ab Version 2.1 ist die Verschlüsselung bei allen Diensten vorgeschrieben, ausser bei SDP (Service Discovery Protocol) Diensten.

3.2.2 Bluetooth Smart (BT Low Energy, BT 4.x)

- Entwicklung seit 2001 durch Nokia, seit 2007 Bluetooth SIG
- Nicht kompatibel mit 2.x und 3.x, als Ergänzung
- Ziel: möglichst geringer Energieverbrauch, preisgünstig
- Kurze Nachrichten (max. 20 Byte), Datenrate max. 1 Mb/s
- Einfache Sterntopologie (keine Scatternets)
- Anwendungen z.B.:

Sicherungsschicht

- Ziel: Funkgerät ist nur möglichst kurz eingeschaltet
  - Energieverbrauch: Empfangsbereitschaft ≈ Senden!
- *Advertising* und *Scanning*
  - Peripheriegerät (*Advertiser*) sendet periodisch Broadcasts
    - auf 3 reservierten Kanälen
    - Intervall: 20ms - 10,24s; mit oder ohne Nutzdaten / Adresse
  - *Scanner* hört Kanäle periodisch ab



Anmerkungen zu Folie 125:

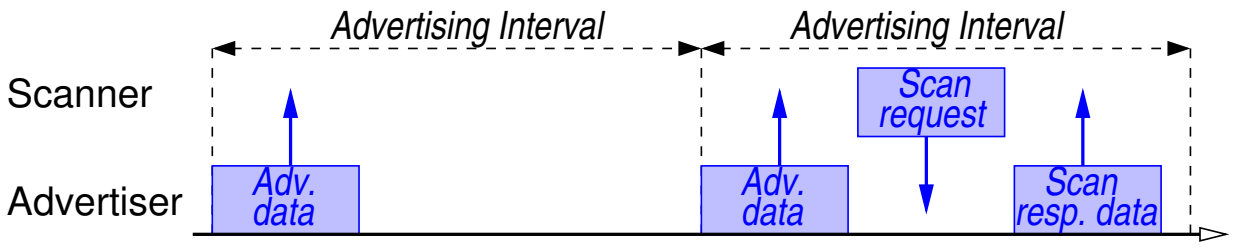
BLE unterscheidet zwei Rollen für Geräte: *Peripheral* und *Central*. Ein *Peripheral*-Gerät kann z.B. ein Armband zur Pulsmessung oder ein *Beacon* zur Indoor-Lokalisierung sein, das *Central*-Gerät ist typischerweise ein Smartphone.

Normalerweise ist das *Peripheral*-Gerät der *Advertiser* bzw. Server, das *Central*-Gerät der *Scanner* bzw. Client.

3.2.2 Bluetooth Smart (BT Low Energy, BT 4.x) ...

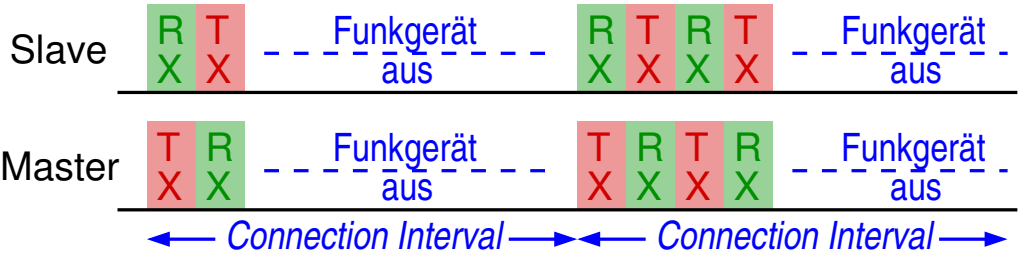
Sicherungsschicht ...

- Aktives Scannen
  - *Advertiser* bleibt nach Versenden der *Advertising*-Daten noch kurz empfangsbereit
  - *Scanner* kann so noch weitere Daten anfordern
  - aber: keine Übertragung von Nutzdaten zum *Advertiser*



Sicherungsschicht ...

- Verbindungsaufbau
  - erlaubt weiteren Datenaustausch, insbes. vom *Scanner* zum *Advertiser*
  - *Scanner* antwortet auf *Advertising*-Paket mit *Connection Request*, u.a. mit
    - Sprungfolge für *Frequency Hopping* (37 Kanäle)
    - *Connection Interval*: wann wird Funkgerät eingeschaltet?



  - Verschlüsselung möglich (bis 128 Bit AES)

Anmerkungen zu Folie 127:

Ein *Peripheral* (der *Advertiser*) kann bei BLE zu jeder Zeit höchstens eine Verbindung haben. Sobald eine Verbindung hergestellt wird, stoppt das *Peripheral* das *Advertising* und ist damit für andere nicht mehr sichtbar.

Attribut-Protokoll und Attribut-Profil

- Server geben Attribute an Clients bekannt
  - Größe max. 20 Bytes
- Attribute werden über UUIDs (16 bzw. 128 Bit) identifiziert
- Operationen:
  - *Discover*/*Find*, Lesen, Schreiben, Benachrichtigung
- *Generic Attribute Profile*: höhere Abstraktion
  - Profil definiert Menge von *Services*
    - z.B. *Heart Rate Profile*: *Heart Rate* + *Dev. Info. Service*
  - *Service* enthält *Characteristics*
  - *Characteristic* enthält Wert und Metadaten (Eigenschaften, Beschreibung)

3.3 Zusammenfassung / Wiederholung

WLAN (IEEE 802.11)

- LLC-Teilschicht identisch zu Ethernet
- Ad-hoc und Infrastruktur-Modus
- Spreizbandtechnik
  - *Frequency Hopping*, *Orthogonal Frequency Division Multiplexing*, *Direct Sequence*
  - Ziel: Reduzierung der Störempfindlichkeit
- 802.11b: Überlappende Kanäle im 2,4 GHz ISM-Band
- Zwei MAC Varianten:
  - verteilte Kontrolle: CSMA/CA-Protokolle (MACAW)
  - zentrale Kontrolle: Zuteilung von Zeitschlitzen

WLAN (IEEE 802.11)

- *Hidden / Exposed Station* Probleme
- MACAW
  - MACA: RTS / CTS-Protokoll
    - Reservierung des Mediums für bestimmte Zeit (NAV)
  - MACAW: Einführung von Bestätigungsframes
- IFS zur Priorisierung von Frameklassen
- Sicherheit:
  - WEP: veraltet, kein ausreichender Schutz
  - WPA und v.a. WPA2 bieten gute Sicherheit
- Aktuell: IEEE 802.11n, MIMO-System, max. 600 Mbit/s; bzw. 802.11ac, MIMO-System, max. 1.69 Gbit/s pro Verbindung

Anmerkungen zu Folie 130:

Der 802.11n Standard arbeitet mit denselben Modulationsarten und derselben Spreizbandtechnik (OFDM) wie der 802.11g Standard. Zur Erhöhung der Bitrate gibt es allerdings einige Erweiterungen:

- Statt 48 Unterkanäle werden auf einem 20 MHz-Kanal 52 Unterkanäle verwendet.
- Es können bei 802.11n auch zwei benachbarte 20 MHz-Kanäle mit insgesamt 108 Unterkanälen verwendet werden.
- Es können mehrere (maximal 4) Sende- und Empfangsantennen werwendet werden (MIMO). Dadurch kann die Bitrate (theoretisch) vervierfacht werden: Der zu sendende Datenstrom wird gleichmäßig auf die (maximal) 4 Sendeantennen aufgeteilt. Jede der (maximal) 4 Empfangsantennen erhält dann eine (lineare!) Überlagerung der vier Sendesignale: $R_i = \sum_j W_{ij} S_j$, wobei S_j das j-te Sendesignal ist und W_{ij} den Kanal zwischen der j-ten Sende- und der i-ten Empfangsantenne beschreibt. Man erhält so ein lineares Gleichungssystem mit 4 Gleichungen und 4 Unbekannten, das gelöst werden kann, wenn die Ausbreitungswege unterschiedlich genug (d.h. linear unabhängig) sind.

Der 802.11ac Standard verwendet ebenso wie 802.11n die MIMO-Technik, ist aber in einigen Punkten weiter optimiert:

- Die Kanalbreite beträgt 80 MHz, optional sind auch 160 MHz möglich.
- Es können bis zu 8 Sende- und Empfangsantennen werwendet werden.
- MU-MIMO ermöglicht es einem *Access Point*, downstream bis zu 4 Clients gleichzeitig zu versorgen, wobei sich die aggregierte Bandbreite entsprechend erhöht.
- Als Modulation wird optional bis zu QAM-256 mit Coderaten von 3/4 und 5/6 verwendet, gegenüber QAM-64 mit Coderate 5/6 bei 802.11n.

Daneben gibt es noch den 802.11ad Standard für das 60 GHz Band und 802.11ah für das Frequenzband von 750-930 MHz.

3.3 Zusammenfassung / Wiederholung ...

Bluetooth

- Vernetzung mobiler Geräte (Handy, PDA), Kabelersatz
- Piconet: Master + max. 7 aktive Slaves
- definiert vollständigen Protokollstapel + Anwendungsprofile
- Funkschicht: 2,4 GHz ISM Band, Frequenzsprungverfahren
- MAC: Zeitmultiplex, zentral durch Master gesteuert
- Vorwärtsfehlerkorrektur, hohe Redundanz
- Sicherheit: optional, ausreichend, aber (theoretisch) angreifbar
- Bluetooth Smart: energiesparende Datenübertragung von „Sensorknoten“