WLAN & Bluetooth

STEFAN HERBST
5BHIFS
05.10.2017

WLAN

Was ist WLAN?

- = Wireless Local Area Network
- Lokales Funknetz
- Standardisierung 1997
- IEEE 802.11: „Kommunikation in Funknetzwerken“

Wer ist das IEEE?

- = Institute of Electrical and Electronics Engineers
- Berufsverband von Ingenieuren
- Gründung 1963 – „zur Förderung techologischer Innovationen zum Nutzen der Menschheit“
- Verabschiedung von Standards in den Bereichen Elektrotechnik und Informationstechnik
- Operiert in über 160 Ländern
- Über 430.000 Mitarbeiter
- Über 1300 verabschiedete Standards

Übertragungstechnik

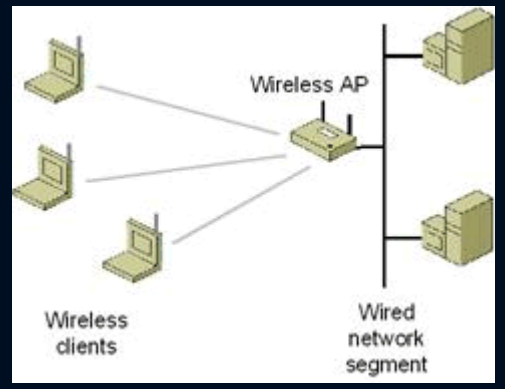
- Elektromagnetische Wellen
- Unterschiedliche Frequenzbereiche
- OFDM
- Hohe Bandbreite auf niedrigen Frequenzen
- OSI-Schicht II

Betriebsmodi

- Infrastruktur-Modus
- Ad-hoc-Modus
- WDS

Infrastruktur-Modus

- Ähnlich dem Mobilfunknetz
- Senden von „Beacons“
- Erleichterter Verbindungsaufbau
- Überwachung der Empfangsqualität
- Aber: Keine Garantie auf gute Verbindungsqualität!



Probleme im Infrastruktur-Modus

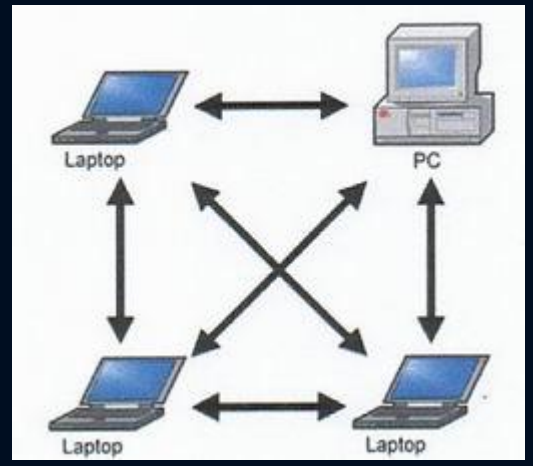
- Frequenzüberlappung mehrerer Stationen
  - Gegenseitige Störung
- Kein automatisches Handover
  - Client sucht erst bei Verbindungsabbruch nach neuer Station

Lösungen für Infrastruktur-Modus

- Implementierung einer „Kontrollinstanz“
  - Kommunikation mit allen Basisstationen
  - Initiierung von Handover
- Arbeit an „Lightweight Access Point Protocol“
  - Offener Standard
  - Noch in Diskussion
  - Zentrale Frage: „Welches Gerät soll welche Funktion übernehmen?“
- momentan nur proprietäre Lösungen

Ad-hoc-Modus

- Alle Stationen gleichwertig
- Schneller Aufbau
- Endgeräte übernehmen Koordinierung



Einschränkungen im Ad-hoc-Modus

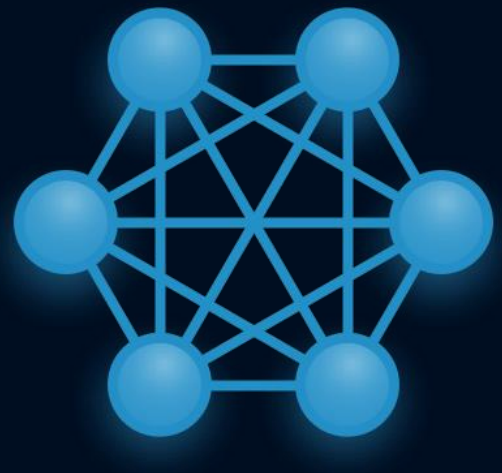
- Keine Paketweiterleitung
  - Kein Informationsaustausch von Netzwerkinformationen
- Physischer Abstand zwischen Geräten muss gering sein
  - Empfänger muss in direkter Reichweite liegen

Erweiterungen für Ad-hoc-Modus

- Ausstattung einzelner Geräte mit Routing-Funktion
- Indirekte Weiterleitung möglich

- Aufwertung durch Software-Verwaltung in Forschung
  - Viele experimentelle Protokolle
  - Standardvorschläge: Wireless Mesh Protocol oder IEEE 802.11s

Mesh networking



- „vermaschtes“ Netz
- Jeder Client ist Knotenpunkt
- Peer-to-peer-Verschlüsselung im gesamten Netzwerk
- Erprobung in amerikanischen Großstädten
- Internet 2.0

WDS

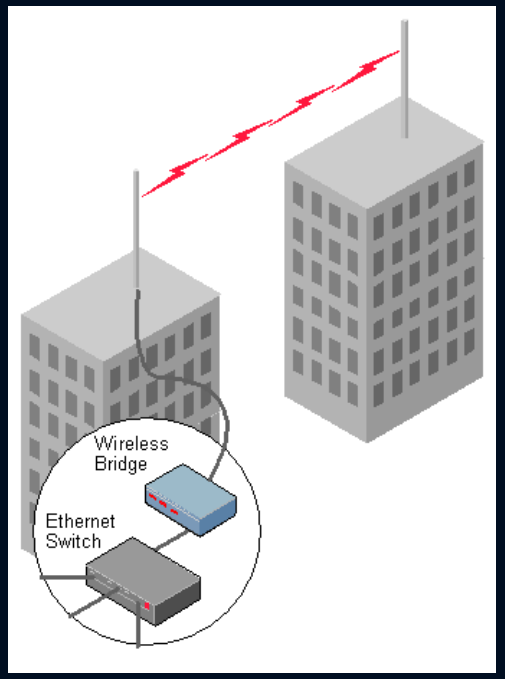
- = Wireless Distribution System
- Verfahren zur Adressierung von WLANs
- Ermöglicht anspruchsvolle Netzwerktopologien
- 1999 in aller Kürze definiert
- Definition lässt genaue Nutzung offen
- Basis für Netzwerk mit mehreren Basisstationen
- Dynamischer Stationswechsel (Handover)

WLAN-Repeater

- Nimmt Signale auf
- Verstärkt diese
- Sendet sie weiter
- Räumliche Erweiterung des Drahtlosnetzwerks
- „Transparent“

Bridge

- Trennung eines großen Netzwerks mit viel Datenverkehr
- Koordiniert Datenverkehr
- Bessere Netzwerkeffizienz
- Weniger Kollisionen
- Geringere Fehleranfälligkeit
- Nur sinnvoll bei viel Intranet-Traffic



Unterschiede Repeater - Bridge

- Repeater hat „verstärkende“ bzw. „erweiternde“ Funktion
  - Erweitert Netzwerk
  - Verstärkt Signal
- Bridge hat „koordinierende Funktion“
  - Koordiniert Datenverkehr
  - Steigert Netzwerkeffizienz

Versionsgeschichte & Übertragungsraten

Standard	Jahr	Frequenz	Bandbreite	Max. Datenrate
IEEE 802.11-1997	1997	2.4 GHz	20 Mhz	2 Mbit/s
IEEE 802.11a	1999	5,0 GHz	20, 40 MHz	54 Mbit/s
IEEE 802.11b	1999	2,4 GHz	22, 40, 80 MHz	11 Mbit/s
IEEE 802.11g	2003	2,4 GHz	20, 40 MHz	54 Mbit/s
IEEE 802.11-2007	2007	2,4 GHz / 5,0 GHz	20,22,40,80 MHz	54Mbit/s
IEEE 802.11n	2009	2,4 GHz / 5,0 GHz	20, 40 MHz	600 Mbit/s
IEEE 802.11p	2010	5,0 GHz	20, 40 MHz	54 Mbit/s
IEEE 802.11-2012	2012	2,4 GHz / 5,0 GHz	20,22,40,80 MHz	600Mbit/s
IEEE 802.11ac	2013	5,0 GHz	20, 40, 80, 160 MHz	6936 Mbit/s
IEEE 802.11ad	2016	60 GHz	1760 MHz	6930 Mbit/s
IEEE 802.11ah	2016	0,9 GHz	2000 MHz	347 Mbit/s

Frequenzbereiche & Kanäle

- **2,4 GHz**
  - 14 Kanäle (numeriert 1-14)
  - 4 Überlappungsfrei nutzbar bei Kanalbreite 20 MHz
- **5 GHz**
  - 24 Kanäle
  - Unregelmäßig numeriert zwischen 36 und 165
- **60 GHz**
  - 4 Kanäle zwischen 58,32 GHz und 65,88 GHz
  - Vorläufige Angaben, noch nicht normiert

Sendeleistung

- **2,4 GHz**
  - 100 mW in allen Ländern ausgen. USA
  - Bis zu 1000 mW in USA
- **5,0 GHz**
  - Sendeleistung kanalabhängig
  - Kanal 36-64: 100 mW in allen Ländern ausgen. USA, Australien, China
  - Kanal 100-140: 200 mW in allen Ländern ausgen. USA, Australien, China
  - Kanal 149-165: 25 mW in allen Ländern ausgen. USA, Australien, China
  - Für USA, Australien und China keine Beschränkung

Reichweite

- Abhängig von Sendeleistung
- Bei 2,4 GHz und 100 mW bzw. 5,0 GHz und 200 mW
  - 30 bis 100 m auf freier Fläche
  - Mehrere Kilometer mit Antennen auf Sichtkontakt
- 60 GHz (IEEE 802.11ad)
  - Bis zu 10 m
- 0.9 GHz (IEEE 802.11ah)
  - Bis zu 1000 m

Sicherheit

- WEP
- WEPplus
- EAP
- Kerberos
- WPA
- WPA 2
- IEEE 802.11i

WEP

- = Wired Equivalent Privacy
- Schlüssellänge: 40 Bit
- Algorithmus: RC4
- Einführung mit IEEE 802.11 1997
- Bereits 2001 „gebrochen“

Erweitungen zu WEP

- WEPplus:
  - erschwert Finden von schwachen Initialisierungsvektoren in WEP
  - Noch immer kein sicherer Algorithmus
- WPA
  - TKIP
  - PSK
  - EAP
- Kerberos: Authentifizierung über Kerberos-Server
  - Unterbindung von man-in-the-middle-Attacken

WPA

- WiFi Protected Access (WPA) 2002
  - 48 Bit Schlüssellänge
  - TKIP (=Temporal Key Integrity Protocol)
    - Jedes Datenpaket hat eigenen Schlüssel
    - RC4+kryptographische Hashfunktion+MAC-Adresse
    - Seit 2009 unsicher
  - PSK (Pre Shared Key)
    - Schlüssel vor Kommunikation bekannt
    - Geheimer Austausch vor Kommunikation zwischen Sender und Empfänger
    - Nicht für Internetanwendungen geeignet → Public Key Verfahren
- EAP (Extensible Authentification Protocol)

IEEE 802.11i & WPA2

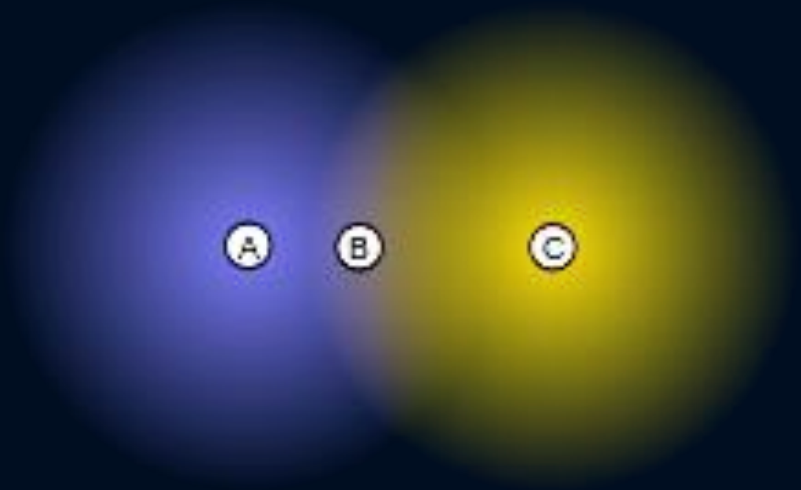
- Aktueller Sicherheitsstandard
- Advances Encryption Standard (AES)
- Schlüssellänge: 256 Bit (AES-256) bei WPA 2
- Verschlüsselungsalgorithmus gilt als sicher, aber
- Attacken (Bruteforce, Wörterbuch, etc.) auf Passwörter möglich

CSMA/CA

- Vermeidung von Kollisionen
- „listen-before-talk"-Mechanismus
- Medium horcht (Carrier Sense)
- Medium frei → Backoffzeit auswürfeln und danach senden
- Medium belegt → Stopp bis Ablauf von NAV, nach DIFS erneut senden
- Nach Empfang wartet Empfänger Sendezeit von CTS ab, danach wird gesendet
- Bei Kollision durch gleiches Backoff → Timeout, nach EIFS wird erneut gesendet

Das „Hidden Terminal“ Problem

- A und B wollen kommunizieren
- Werden von C gestört
- C sieht A nicht und denkt, B wäre frei
- Folge: Kollisionen
- Lösung: RTS/CTS
- C darf erst nach Empfang von CTS senden

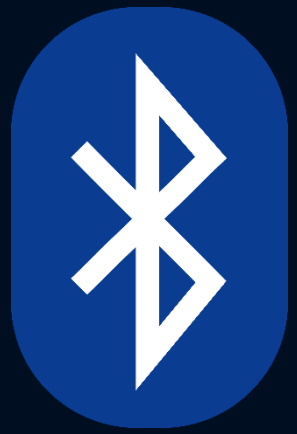


Zukunft von WLAN

- Optimum zwischen Reichweite und Bandbreite
- Multi-Gigabit-Speeds (WiGig)
- Public Wifi via 802.11ad

Bluetooth

Was ist Bluetooth?



- WPAN (=Wireless Private Area Network)
- Datenübertragung über kurze Distanz per Funktechnik
- Entwickelt 1994
- Seit 1998 in Besitz der Bluetooth Special Interest Group
- IEEE 802.15.1 (heute nicht mehr unterstützt)

Ursprung

- Früher „Short link radio technology
- 1989 von Nils Rydebeck (Ericsson CTO) erfunden
- Ziel: Kabellose Kopfhörer
- Kabellose Alternative zu RS-232

Bluetooth Special Interest Group

- Interessensgemeinschaft aus über 30.000 Unternehmen
- 1998 gegründet
- Gründer: Ericsson, IBM, Intel, Nokia, Toshiba
- Eigentümer des Warenzeichens
- Herausgeber der Spezifikationen

Übertragungstechnik

- 2,4 GHz
- UHF Mikrowellen
- Aufteilung von Datenpaket auf 79 Kanäle mit je 1 MHz
- 40 Kanäle mit je 2 MHz bei Bluetooth LE
- Frequence hopping
- Verschlüsselte Übertragung
- Master-Slave-Prinzip

Leistungsklassen

- **Klasse I**: Bis zu 100m Reichweite bei 100mW
- **Klasse II**: Bis zu 10m Reichweite bei 2,5mW
- **Klasse III**: Bis zu 1m Reichweite bei 1mW
- **Klasse IV**: Bis zu 0,5m Reichweite bei 0,5mW

Versionsgeschichte & Übertragungsraten

Version	Jahr	Datenrate	Reichweite
1.0	1999	0,7322 Mbit/s	Bis 10m
1.1	2001	0,7322 Mbit/s	Bis 10m
1.2	2003	1 Mbit/s	Bis 10m
2.0+EDR	2004	2,1 Mbit/s	Bis 100m
2.1+EDR	2007	2,1 Mbit/s	Bis 100m
3.0+HS	2009	24 Mbit/s	Bis 100m
4.0	2010	24 Mbit/s	Bis 100m
4.1	2013	24 Mbit/s	Bis 100m
4.2	2014	24 Mbit/s	Bis 100m
5.0	2016	48 Mbit/s	Bis 400m

Entwicklung

- Konkurrenzkampf mit WLAN ah
- Wachstum im IoT-Markt (Bluetooth 5.0)
- Bluetooth LE bei IoT-Geräten

- Momentan klarer Marktnachteil, da WLAN weiter verbreitet
- Vorteil: WLAN ah noch nicht vollständig standardisiert

Quellen

- https://de.wikipedia.org/wiki/Wireless_Local_Area_Network
- https://de.wikipedia.org/wiki/IEEE_802.11
- https://de.wikipedia.org/wiki/Orthogonales_Frequenzmultiplexverfahren
- http://whatis.techtarget.com/definition/multi-carrier-modulation-MCM
- https://de.wikipedia.org/wiki/Institute_of_Electrical_and_Electronics_Engineers
- https://de.wikipedia.org/wiki/Optimized_Link_State_Routing
- https://de.wikipedia.org/wiki/Optimized_Link_State_Routing
- https://de.wikipedia.org/wiki/Freies_Funknetz
- https://de.wikipedia.org/wiki/Vermaschtes_Netz
- https://de.wikipedia.org/wiki/Wireless_Distribution_System
- http://www.itbusinessedge.com/blogs/data-and-telecom/the-age-of-wigig-is-almost-here.html
- https://de.wikipedia.org/wiki/IEEE_802.11p
- https://de.wikipedia.org/wiki/IEEE_802.11ad
- https://de.wikipedia.org/wiki/IEEE_802.11ah
- https://de.wikipedia.org/wiki/IEEE_802.11i
- https://en.wikipedia.org/wiki/IEEE_802.15
- https://de.wikipedia.org/wiki/Wireless_Personal_Area_Network
- https://de.wikipedia.org/wiki/Bluetooth
- https://en.wikipedia.org/wiki/Bluetooth
- https://en.wikipedia.org/wiki/Frequency-shift_keying#Gaussian_frequency-shift_keying

Quellen (2)

- https://en.wikipedia.org/wiki/Phase-shift_keying
- https://en.wikipedia.org/wiki/Ultra_high_frequency
- https://de.wikipedia.org/wiki/Bluetooth_Low_Energy
- http://blueapp.io/blog/history-of-bluetooth/
- https://de.wikipedia.org/wiki/Extensible_Authentication_Protocol
- https://de.wikipedia.org/wiki/Pre-shared_key
- https://de.wikipedia.org/wiki/Temporal_Key_Integrity_Protocol
- https://de.wikipedia.org/wiki/Wi-Fi_Protected_Access
- https://de.wikipedia.org/wiki/Kerberos_(Informatik)
- https://de.wikipedia.org/wiki/WEPplus
- https://de.wikipedia.org/wiki/Wired_Equivalent_Privacy
- https://www.golem.de/news/broadcom-sicherheitsluecke-angriff-ueber-den-wlan-chip-1704-127151.html
- https://www.pcwelt.de/ratgeber/Hacker-Angriff-aufs-WLAN-WLAN-Sicherheit-5632681.html
- https://www.computerwoche.de/a/modernes-wlan-hacking,2521564
- http://www.wlanrepeater.org/ratgeber/unterschied-router-repeater-bridge/
- https://de.wikipedia.org/wiki/Carrier_Sense_Multiple_Access/Collision_Avoidance
- https://de.wikipedia.org/wiki/Interpacket_Gap
- https://de.wikipedia.org/wiki/Wireless_Access_Point
- https://www.ieee.org/standards/index.html

Ende

VIELEN DANK FÜR IHRE AUFMERKSAMKEIT!