

Kapitel 6 – Bluetooth

Vorlesung Mobilkommunikation Wintersemester 2016/17
Prof. Dr. Oliver Waldhorst (HS Karlsruhe), Markus Jung

INSTITUT FÜR TELEMATIK





Mobiles TCP



Mobile Ad Hoc Netze



Mobile IP



WLAN, **Bluetooth**



GSM, UMTS, LTE



Mobilitätsmanagement



Medienzugriff



Drahtlose Übertragung

Motivation WPANs

■ WPAN – Wireless Personal Area Network

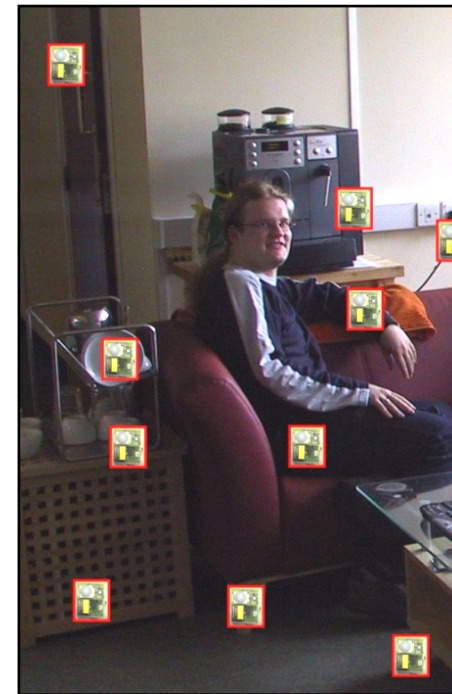
- Vernetzung von Geräten in einem relativ kleinen räumlichen Bereich um einen oder mehrere Menschen

■ Beispiele

WPAN in Büroumgebung zur Vernetzung mehrerer fester und mobiler Geräte



WPAN in Heimumgebung zur Vernetzung verschiedener Geräte und Sensoren



[6.7]

Charakteristika von WPANs

- Drahtlose Kommunikation
 - i.A. über Funk (oder Infrarot)
- Begrenzte Reichweite
 - Kommunizierende Geräte können meist keine große räumliche Distanz zueinander haben (i.d.R. bis zu wenigen 10 Metern)
- Begrenzte Batteriekapazität
 - Mechanismen zum Energiesparen kommt große Bedeutung zu
 - Geringe Sendeleistung und dadurch begrenzte Reichweite
- Automatische Konfiguration
 - Plug-and-Play
 - Ohne Systemadministrator und ohne manuelle Eingriffe
- Fehlende oder eingeschränkte Multipoint-zu-Multipoint-Fähigkeit
- Geräte haben evtl. reduzierte Fähigkeiten
- Kostengünstiges Hardwaredesign
 - Massenprodukte zu geringen Preisen

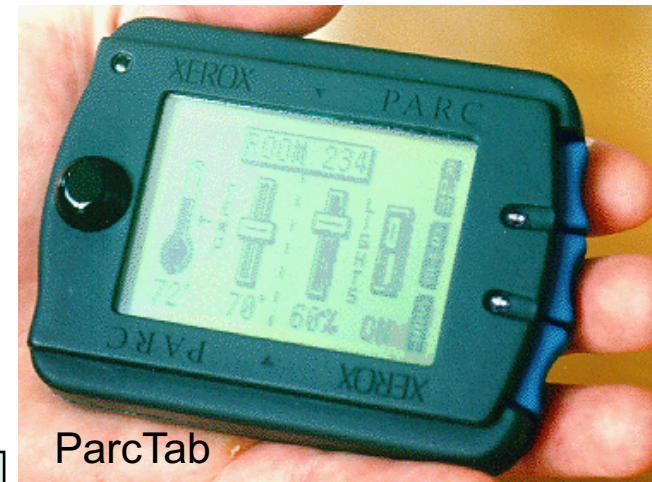
Verschiedene WPAN-Technologien

■ ...in ubiquitären Systemen

- Häufig Entwicklung „eigener“ Technologien zur Vernetzung
 - Z.B. TeCO (Smart-Its), FU Berlin (ScatterWeb)
 - Laser, z.B. „Smart Dust“ (Berkeley)

■ Standardisierte Technologien

- RFIDs
- Infrarot
 - Proprietär, ParcTab (Xerox PARC)
 - IRDA, z.B. iCricket (MIT)
- Funk (IEEE Arbeitsgruppe 802.15)
 - Bluetooth
 - ZigBee



ParcTab

- Vereinigung von Industriepartnern
 - 1998 schließen sich die Firmen Ericsson, Nokia, IBM, Intel und Toshiba zur Bluetooth Special Interest Group (Bluetooth SIG) zusammen.
 - Ericsson verfolgte die Ideen bereits seit etwa 1994
- Ziel
 - Entwicklung eines kostengünstigen Standards für Funkübertragung über geringe Distanzen
 - Preis der Bluetooth-Chips sollte in Groß-Serien bei einigen Dollars liegen
 - Kostengünstige Massenproduktion

*Verschiedene
Bluetooth-Geräte*



... zur Namensgebung

- Nach Harald dem I., Wikingerkönig von Dänemark, 911-970, genannt „Blauzahn“

- Gerüchten zu folge litt er an einer chronischen Krankheit, die seine Zähne blau färbte ...
- Christianisierte Dänemark
- Vereinte das Volk Dänemark



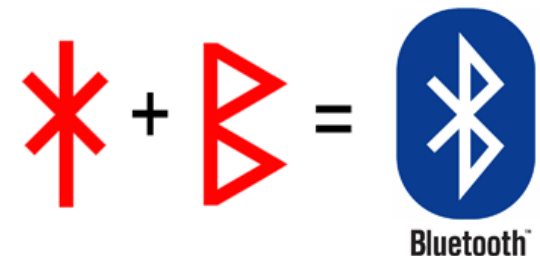
- Bluetooth vereinigt Kommunikation verschiedener Kleingeräte

- Mobiltelefone, PDAs, Sensoren etc.

- Bluetooth-Logo

- Enthält die Runen „H“ und „B“

HARALD BLÅTAN
*†R††††† ††††††††††



Anwendungsbeispiele

- Austausch von Visitenkarten
 - PDA versendet Visitenkarten an PDAs der Geschäftspartner
- Anforderungen
 - Drahtlose Übertragung
 - Keine Vorkonfiguration, einfach Bedienbarkeit
 - Geringe Bandbreite
 - Geringe Reichweite
 - Energiesparend, da Batteriebetrieb



Anwendungsbeispiele

■ Drahtlose Kopfhörer

- Kommunikation zwischen Handy und Kopfhörer

■ Anforderungen

- Robuste Kommunikation
- Gute (Audio-)Qualität
- Abhörsicherheit, Authentifizierung und Verschlüsselung
- Geringe Reichweite
- Energiesparend



■ Übertragung von Fotos an den Fotodrucker

- Kommunikation zwischen Handy oder Kompaktkamera und Fotodrucker

■ Anforderungen

- Drahtlose Übertragung
- Fehlerfreie Übertragung
- Automatische Konfiguration
- Authentifikation, Zugriffsschutz
- Geringe Reichweite
- Energiesparend



Anwendungsbeispiele

■ Viele andere Szenarien

- u.a. zur Kommunikation zwischen PCs, PDAs über „Profile“ mit ...
- Bluetooth heute in Vielzahl von Geräten standardmäßig integriert



Handy, „Headset“



Drucker



HiFi



GPS-Empfänger



Gamepad

Tastatur,
Maus



Anforderungen an Bluetooth

- Anwendungsbeispiele führen direkt zu einigen wichtigen Anforderungen, die von Bluetooth erfüllt werden sollten.
 - Automatische Konfiguration
 - Auffinden von Geräten in Kommunikationsreichweite
 - Konfiguration von Bluetooth-Netzen
 - Auffinden von Diensten, welche die Geräte anbieten
 - Unterstützung unterschiedlicher Anwendungsanforderungen hinsichtlich Dienstgüte und Zuverlässigkeit
 - Garantierte Dienstqualität für Sprachkommunikation zwischen zwei Geräten
 - Einstellung von Dienstgüteparametern
 - Sicherheit der drahtlosen Kommunikation
 - Dienste zur Authentifizierung und Verschlüsselung

- Verwendung des lizenzfreien ISM-Bands (2,4 GHz)
 - Aufteilung in 79 Kanäle (bis 2001 nur 23 in Frankreich, Spanien und Japan)
 - Teilt sich Medium mit u.A. WLAN oder Mikrowellen
 - **Frequenzsprungverfahren** zum Frequenzspreizen → sehr robust
- Datenrate (Bluetooth 1.1)
 - max. 1 Mbit/s brutto (723 kBit/s netto)
- Drei unterschiedliche Klassen
 - Klasse 1: 100 mW (Entfernungen bis 100 m)
 - Klasse 2: 2,5 mW (Entfernungen bis 10 m)
 - Klasse 3: 1 mW (Entfernungen bis 10 cm)
- Zusammenfassung

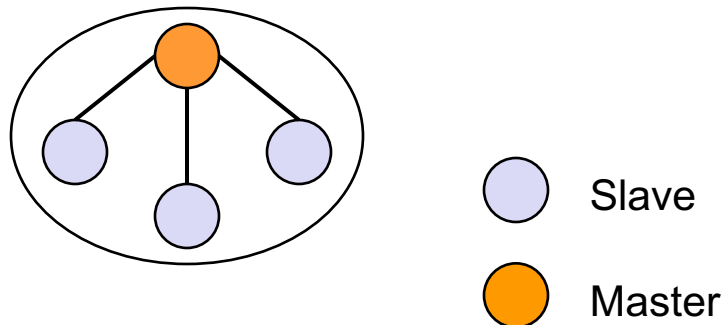
Eigenschaft	Klasse 1	Klasse 2	Klasse 3
Reichweite	100 m	10 m	10 cm
Ausgangsleistung	100mW	2,5 mW	1 mW
Frequenzen	2400-2483,5 MHz (ISM-Band)		
Datenraten	Brutto max. 1 Mbits/s, netto max. 723 kbit/s		

Netzarchitektur - Piconetz

■ Grundform: Piconetz

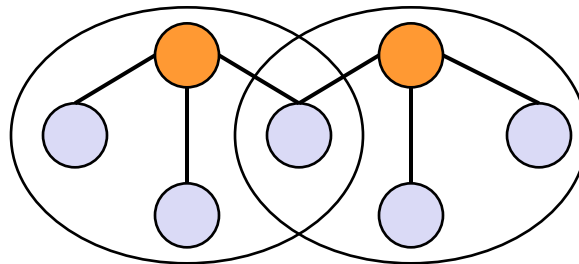
- 1 Master
 - verteilt Senderecht an die Slaves
- 1 bis 7 Slaves
 - können nur über den Master miteinander kommunizieren
 - keine direkte Kommunikation zwischen Slaves möglich
- Jedes Gerät im Piconetz ist entweder Master oder Slave
 - Gerät, das ein Piconetz aufbaut wird zunächst automatisch zum Master
 - Master kann während des Betriebs wechseln

Skizze eines Piconetzes

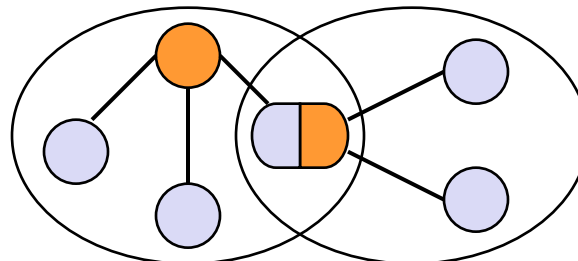


Netzarchitektur - Scatternetz

- Für größere Netze: Scatternetz
 - Überlappung mehrerer Piconetze
 - Genau 1 Master pro Piconetz !
 - 1 Knoten kann
 - in mehreren Piconetzen Slave sein



- aber nur in einem Piconetz als Master fungieren

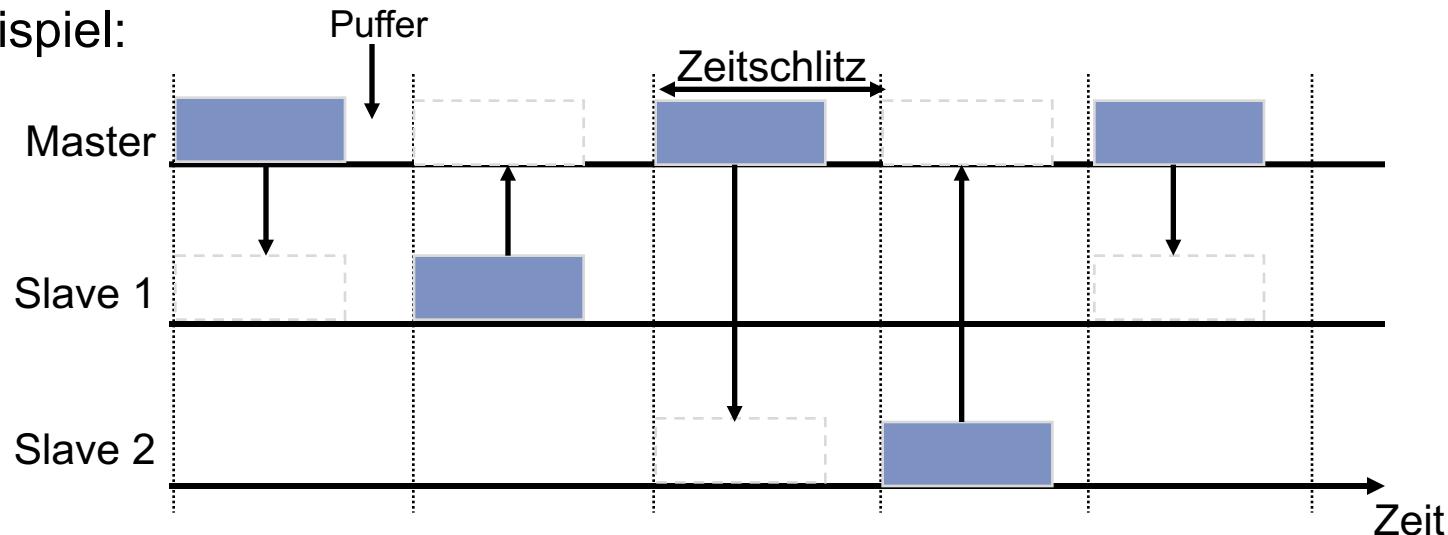


Slave in einem
Piconetz und Master
in einem anderen

Master steuert Übertragung

- Verwendung von Time Division Duplex (TDD)
 - Variante von TDMA
 - Übertragung ist in Zeitschlitz gegliedert
 - Dateneinheiten beanspruchen typischerweise einen Zeitschlitz
 - Es existieren auch Dateneinheiten die 3 oder 5 Zeitschlitz benötigen
 - Zeitschlitz werden wechselweise von Master und Slave genutzt
 - Master nutzt ungerade Zeitschlitz, Slaves nutzen gerade Zeitschlitz
 - Slave darf erst antworten, wenn der Master ihn aufgefordert hat
 - So werden Kollisionen beim Medienzugriff vermieden
 - Master kann abwechselnd Daten an verschiedene Slaves schicken

■ Beispiel:





FHSS in Bluetooth

- Ziel
 - Robuste Kommunikation zwischen Bluetooth-Geräten
- Bandspreizen durch **Frequency Hopping Spread Spectrum**
 - Frequenzwechsel erfolgen zwischen Zeitschlitzten bzw. zwischen Dateneinheiten
 - Bei Dateneinheiten, die länger als ein Zeitschlitz sind, wird die Frequenz beibehalten. Ansonsten wechselt die Frequenz nach jeder Dateneinheit.
 - Dabei wird ursprüngliches Schema beibehalten
 - Bei einer Dateneinheit von 3 Zeitschlitzten wird danach von der Frequenz f_k zu Beginn der Übertragung auf die Frequenz f_{k+3} gewechselt
 - Vorteil: Alle Stationen können an ihrer gewohnten Sequenz festhalten und müssen nicht über die Übertragung längerer Dateneinheiten informiert sein.
 - Häufigkeit der Frequenzwechsel: 1600-mal pro Sekunde
 - 1 Zeitschlitz dauert also $1/1600 \text{ s} = 625 \mu\text{s}$
- Vorteil
 - Einzelne gestörte Frequenzen stören nicht die gesamte Übertragung
 - Ab Bluetooth 1.2 durch adaptives Frequenzspringen weiter verbessert, da es sich an Störungen anpassen kann.

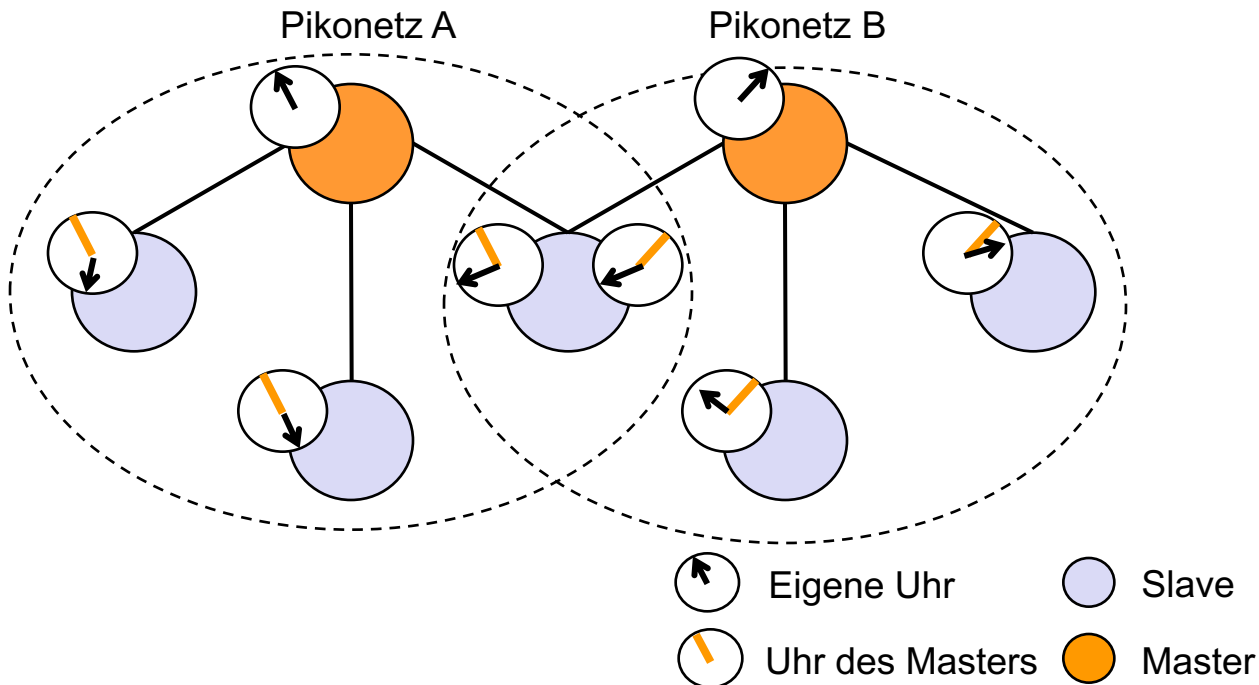


Frequenzspringen

- Problem: Welche Sequenz von Frequenzen wird genutzt?
 - Master und Slave müssen **synchronisiert** sein, d.h.
 - gleiche Sequenz der Frequenzen und
 - gleiche Phase innerhalb der Sequenz
 - Sequenz selbst vom Master vorgegeben
 - Abfolge der Frequenzen (Sprung-Sequenz oder „Hopping-Sequenz“) ist eine Pseudo-Zufallszahlenfolge
 - Sprung-Sequenz berechnet aus der **Geräteadresse des Masters**
 - „Phase“ innerhalb der Sequenz bestimmt durch die **Uhr des Masters**
 - Damit kennen Master und Slave jeweils dieselbe aktuelle Frequenz
 - Die Sprung-Sequenzen in verschiedenen Piconetzen unterscheiden sich
 - ... Master kann also nicht in zwei oder mehr Piconetzen agieren sondern ist auf eines beschränkt!

Synchronisation in Scatternetzen

- Zur Phasenerkennung der Sprung-Sequenz, muss jeder Slave die Uhren aller seiner Master kennen



- Problem unterschiedliche Sprungfrequenzen: Ein Slave kann immer nur in einem Piconetz aktiv sein
 - Abmelden im alten Netz
 - Anmelden im aktiven Netz



Wie werden Piconetze gebildet?

- Aufbau von Piconetzen in zwei Phasen
 - Kennenlernen der Geräte in Reichweite
 - Prozess: Inquiry-Prozedur
 - Kennenlernen der Geräteadressen und Uhren
 - Einladen eines (bereits bekannten) Gerätes ins Piconetz
 - Prozess: Paging-Prozedur
 - Verbindungsaufbau, Vergabe der Adressen im Piconetz, ...

Inquiry-Prozedur

- Aufgabe: Finden von anderen Geräten
- Probleme
 - Neue Geräte, die nicht Mitglied im Piconetz sind, können nicht der dortigen Sprung-Sequenz folgen
 - Sie kennen auch nicht die aktuelle Phase innerhalb der Sprung-Sequenz
- Vorgehensweise
 - Geräte folgen speziellen **Inquiry-Sprungsequenzen**
 - Besteht aus 32 Frequenzen (bzw. 16 davon für Spanien ...)
 - Sind allen Geräten auch ohne Mitgliedschaft in einem Piconetz bekannt
 - Alle Geräte hören auf Untermenge aus 16 dieser Frequenzen mit ihrer speziellen Sequenz
 - Sequenz wird durch jeweilige Geräteadresse bestimmt

Inquiry-Prozedur

- Suchende und hörende Geräte nutzen **unterschiedliche Häufigkeiten des Springens**
 - Suchendes Gerät sendet **Inquiry-Dateneinheiten** mit hoher Frequenz
 - Wählt alle 312,5 μ s eine neue Frequenz
 - D.h. 2 Inquiry-Dateneinheiten pro Zeitslot
 - Hörende Geräte wählen alle 1,28 s eine neue Frequenz
 - Hören dort jeweils für 18 Zeitschlitze, also 11,25 ms
- Hörende Geräte antworten unter anderem mit ihrer **Geräteadresse**, ihrer **Uhr** und ihrer Geräteklasse
 - Dadurch gelingt späteres Paging schneller



... immer sichtbar?

■ Beobachtung

- Die Inquiry-Prozedur erfordert, dass das Bluetooth-Gerät sichtbar ist ... wollen wir das immer?
 - Privatsphäre
 - Angriffe auf Fehlerhafte Bluetooth-Implementierungen, z.B. BlueSnarf, Chaos, BlueBug, ...
 - Auslesen von Adressbüchern
 - Initiieren von Telefongesprächen
 - ...?

■ ...don't panic

- Anwender kann das Verhalten seines Bluetooth-Gerätes beeinflussen
- Bluetooth-Geräte ermöglichen Unsichtbarkeit
 - Keine Antwort auf Inquiries
 - Verbindungsaufbau über Paging dennoch möglich
 - Keine Sicherheitsgarantie! Geräteadresse kann man erraten...



Paging-Prozedur

- Aufgabe: Ein Gerät soll in ein Piconetz eingeladen werden
- Voraussetzung
 - Geräteadresse des einzuladenden Gerätes ist bekannt
 - Hierfür sorgt die Inquiry-Prozedur
 - Bekannte Uhrzeit beschleunigt Paging-Prozedur
- Ablauf
 - Einladendes Gerät berechnet Sprungsequenz aus Geräteadresse des einzuladenden Gerätes
 - Besteht aus 32 Frequenzen (bzw. 16 für Spanien ...)
 - Einladendes Gerät berechnet Phase aus (geschätzter) Uhr des einzuladenden Geräts
 - Uhren „driften“ immer etwas auseinander
 - Wenn Uhrzeit (und damit Phase) falsch geschätzt, dann wird in Phase(n) „danach“ oder „davor“ gesucht
 - Beide Geräte nutzen unterschiedliche Wechselgeschwindigkeiten für die Sprungsequenz
 - Einladendes Gerät wählt alle 312,5 μ s eine neue Frequenz und sendet **Paging-Dateneinheiten**
 - Eingeladenes Gerät wählt alle 1,28 s eine neue Frequenz, hört dort für 11,25 ms
 - Das einladende Gerät wird Master der Verbindung

Protokollstapel

■ Vielzahl von Protokollen spezifiziert. Kernspezifikationen

- Protokolle der physikalischen Schicht und der MAC-Schicht
 - Regeln Zugriff auf das drahtlose Kommunikationsmedium (s. vorne)
 - Gliedern sich in die Schichten „Radio“ und „Baseband“
- **Link Manager Protocol (LMP)**
 - Verwaltung von physikalischen Links
 - Regelt Pairing und Verschlüsselung für einen Link
 - Gleicht Uhren ab
 - Führt Master-Slave Rollenwechsel durch
 - Stellt Sendeleistung ein

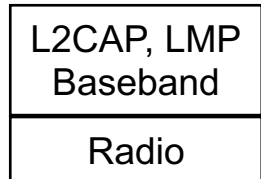
- **Logical Link Control and Adaption Protocol (L2CAP)**
 - Stellt pro Link mehrere Kanäle zur Verfügung
 - Segmentierung und Reassemblierung großer Daten
 - Regelt Dienstgüte

■ Profilspezifikationen

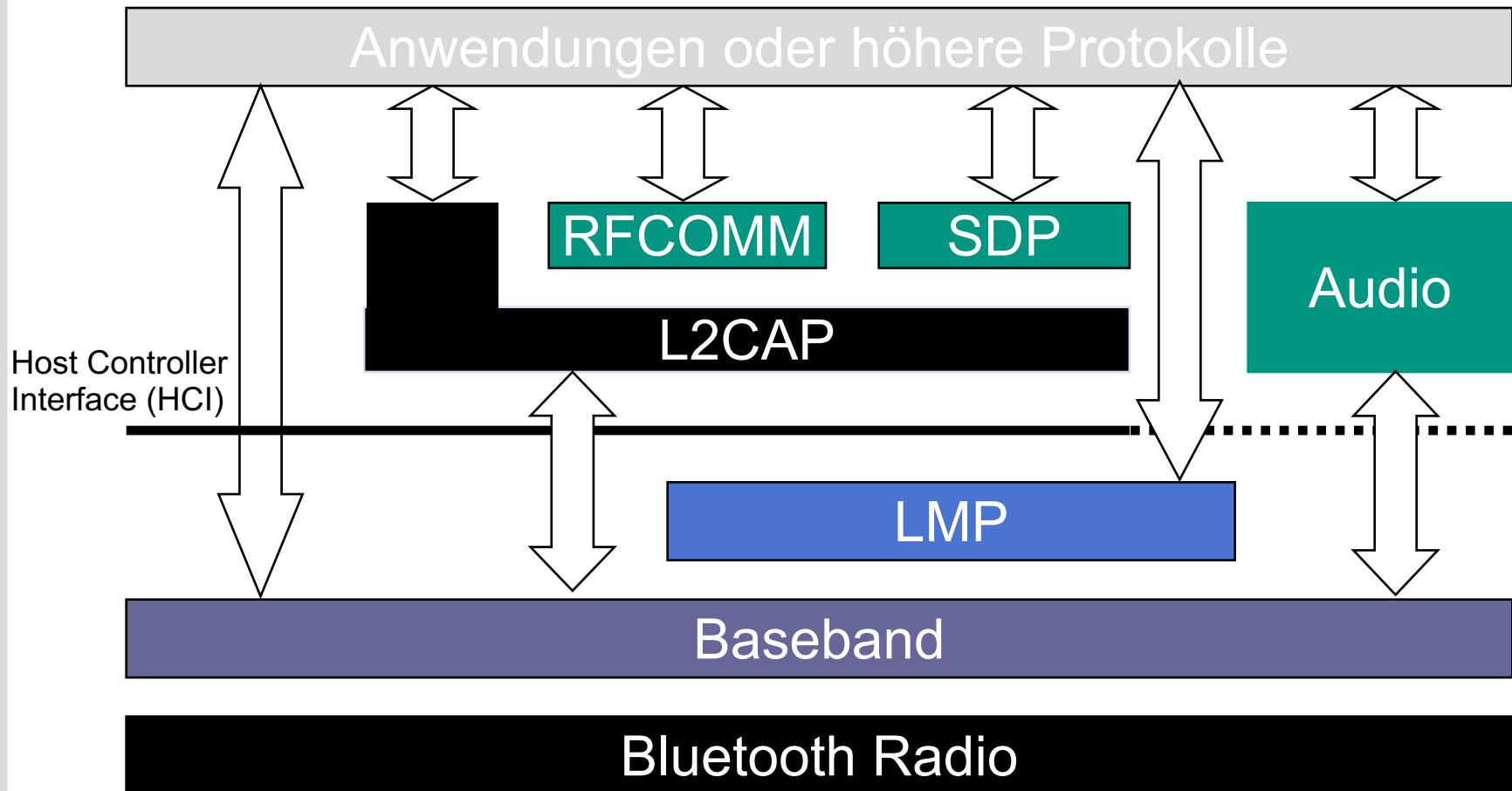
- Protokolle und Funktionen zur Anpassung an Anwendungen

IEEE
802.15.1

ISO/OSI Modell Bluetooth



Protokollstack im Überblick



■ SDP (Service Discovery Protocol)

- Suche nach Diensten anderer Geräte
- Feststellung von Dienstparametern (z.B.: L2CAP PSM, RFCOMM Channel)
- Standardisierte Dienste werden in Profilen beschrieben

■ RFCOMM

- Emulation serieller Schnittstellen
- In der Regel Grundlage weiterer Protokolle (OBEX, PPP, ...)

Basisband-Dateneinheit

- Format der MAC-Dateneinheit, die in einem Zeitschlitz gesendet wird

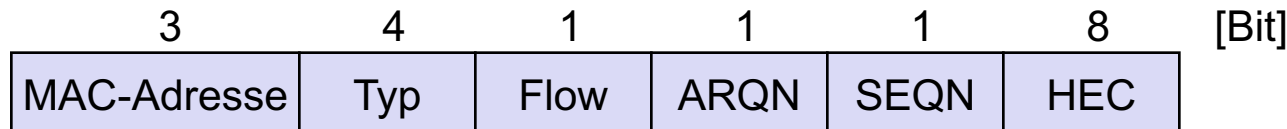


- Unterschiedliche Typen sind möglich
 - Nur Zugangscode, Einsatz z.B. beim Inquiry
 - Zugangscode und Kopf, beim Paging
 - Zugangscode, Kopf und Nutzdaten, bei Datenaustausch
- Zugangscode
 - Identifiziert Piconetz
 - Ist abgeleitet von der Geräteerkennung des Masters
 - Besteht aus
 - Präambel zur Synchronisierung
 - Synchronisationsfeld, das u.A. Zweck der Dateneinheit darstellt
 - Z.B. Inquiry, Paging, normaler Datenaustausch
 - Adresse des Masters bzw. Slaves
 - Anhang, nur vorhanden, falls Nutzdaten folgen

Basisband-Dateneinheit

■ Paketkopf

- **MAC-Adresse:** 3 bit Active Member Address
 - Geräten wird im Piconetz diese temporäre Adresse zugeordnet
 - max. 1 Master- und 7 Slaves adressierbar
- **Typ:** Verbindungstyp, synchron oder asynchron (siehe später!)
- **Flow:** Halt und weiter (Flusskontrolle)
- **ARQN:** ACK bei Anwendung von ARQ-Verfahren
- **SEQN:** Sequenznummer zur Filterung doppelter Pakete
- **HEC:** Prüfsumme über Paketkopf



- **Senden mit 1/3 Vorwärtsfehlerkorrektur (FEC)**
 - Jedes Bit wird dreimal gesendet
 - $3 \times 18 \text{ Bit} = 54 \text{ Bit}$

Verbindungsverwaltung

- Aufgabe des Link Manager Protocols (LMP)
 - Höheren Schichten werden unterschiedliche Typen von Verbindungen bereitgestellt
- Synchronous Connection-Oriented Link (SCO)
 - Symmetrisch, Punkt-zu-Punkt, nur zwischen Master und einem Slave
 - Datenrate immer 64 kbit/s (z.B. Sprachverbindungen)
 - Master reserviert Zeitschlitz („Slots“) in festen Intervallen
 - Verschiedene Typen möglich – Unterschied liegt in Vorwärtsfehlerkorrektur
 - *High Rate Voice 1 (HV1)*: Forward Error Correction (FEC) mit 1/3 Coderate, alle 2 Zeitschlitz ist ein Zeitschlitz reserviert
 - *HV2*: FEC mit 2/3 Coderate, alle 4 Zeitschlitz ist ein Zeitschlitz reserviert
 - *HV3*: ohne FEC, alle 6 Zeitschlitz ist ein Zeitschlitz reserviert
 - Damit selbst bei starker Störung Übertragung möglich

Mögliche Verbindungen

■ Asynchronous Connectionless Link (ACL)

- Punkt-zu-Mehrpunkt, Master fragt mehrere Slaves ab (polling)
- symmetrisch oder asymmetrisch
 - Datenraten bis zu 721 kbit/s
- Verschiedene Typen
 - *Data Medium Rate x (DMx)*: FEC mit 2/3 Coderate; *Data High Rate x (DHx)*: kein FEC
 - X steht für Anzahl aufeinanderfolgender Zeitschlitz, die eine Dateneinheit einnehmen darf (bis zu 5)
 - Es findet kein Frequenzwechsel zwischen diesen Zeitschlitz

LMP – Link Management Protocol

■ Authentifikation und Verschlüsselung

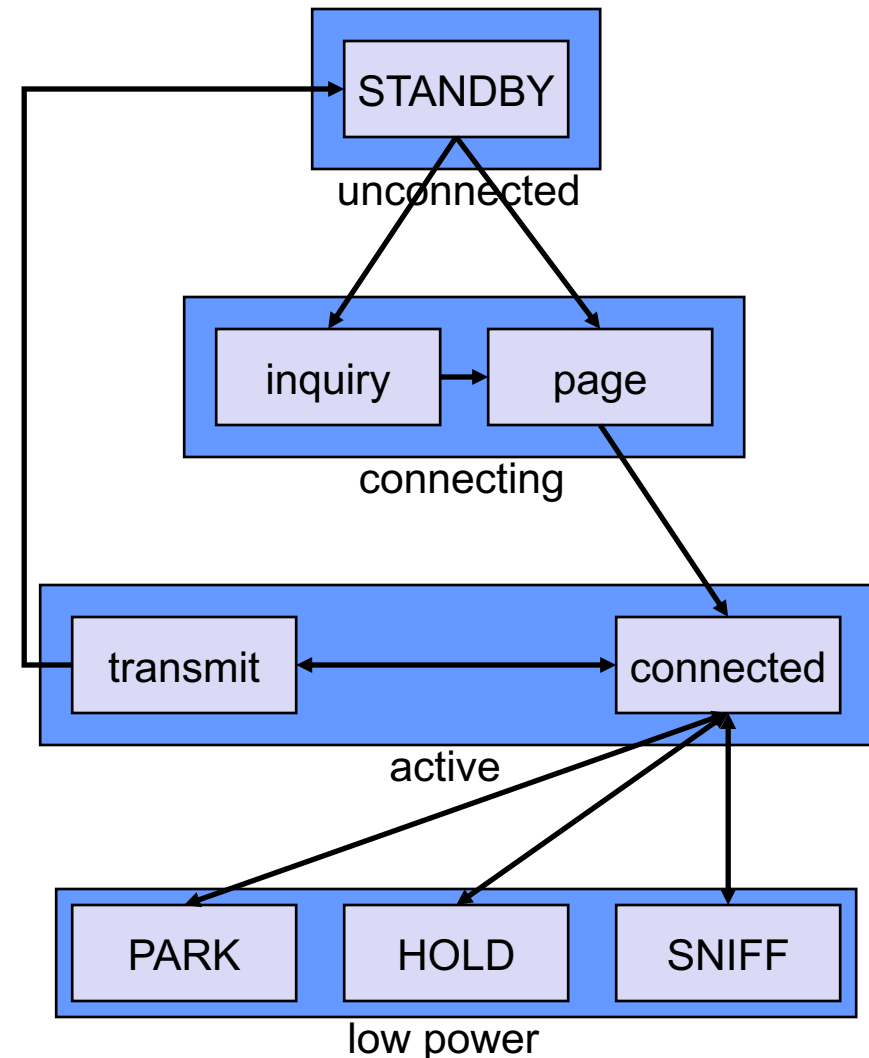
- Authentifikation des Kommunikationspartners („**Pairing**“), da Daten von dritter Seite über die Luftschnittstelle gesendet werden können
 - Basierend auf Challenge-Response-Verfahren
 - Aus „Shared Secret“ (PIN) wird gemeinsamer Schlüssel berechnet
 - Challenge ist 16-Byte-Zufallszahl
- Verschlüsselung der Daten, da diese bei der Übertragung abgehört werden können (optional)
 - Symmetrische Verschlüsselung über SAFER+ (Secure And Fast Encryption Routine)
 - Schlüssel ist variabler Länge (<128 bit) und basiert auf Schlüssel zur Authentifikation

LMP – Link Management Protocol

- Abgleich lokaler Uhren
 - für Frequenzsprung wird exakte Zeitmessung benötigt
 - Für jedes Gerät wird zeitlicher Offset (Unterschied zu eigener Uhr) gespeichert
- Tausch der Master/Slave-Rollen
 - Master wird durch Zusatzaufgaben stärker belastet als der Slave
 - Batterie des Masters wird stärker belastet
- Ändern der Sendeleistung
 - RSSI (Receiver Strength Signal Indicator) misst Empfangspegel
 - ggf. kann Kommunikationspartner aufgefordert werden die Sendeleistung zu erhöhen oder zu drosseln
- Einstellen von Dienstgüte-Parametern (Quality of Service, QoS)
 - Änderung der Dienstgüteparameter als Reaktion auf die Übertragungsqualität
 - z.B. Wahl eines Pakettyps mit höherer FEC-Rate
- Ändern der Betriebsmodi
 - Wechsel zwischen **Connected Mode**, **Sniff Mode**, **Hold Mode** und **Park Mode**

LMP-Betriebsmodi

- Low-Power-Modi können durch Master forciert werden:
- SNIFF
 - Gerät schläft periodisch und hört in größeren Abständen auf Poll-Anfragen vom Master (Intervalle sind variabel)
 - Gerät bleibt aktiver Teil des Piconetzes (behält Active Member Address)
- HOLD
 - Gerät schläft einmalig für „hold time“
 - Gerät bleibt aktiver Teil des Piconetzes (behält Active Member Address)
- PARK
 - Gerät kein aktiver Teil des Piconetzes mehr (erhält **Parked Member Address**)
 - Erhaltung der Synchronisation durch Beacons, die in großen Abständen vom Master gesendet werden



L2CAP

■ Funktionen

- Zerlegen großer Dateneinheiten in mehrere kleine Teile für den Transport (Segmentation and Reassembly – SAR)
 - Konfiguration Basisbandübertragung
 - Sendebestätigungen, Timeouts
 - Konfiguration max. L2CAP-Dateneinheit (MTU) bis 64 kByte
 - Nur Teile *einer* L2CAP-Dateneinheit hintereinander über die Verbindung versendet
- Einstellung von Dienstgüte-Eigenschaften möglich
 - Definition von Dienstgüte-Parametern pro logischem Kanal
 - Dienstgütetyp
 - keine Dienstgüte
 - Best Effort: Vorgaben werden berücksichtigt, jedoch keine Garantien für Einhaltung gegeben
 - Garantie (optional): Einhaltung der eingestellten Parameter wird garantiert
 - Parameter für jeweiligen Dienstgütetyp

L2CAP

- **Bereitstellung mehrerer logischer Kanäle** pro ACL Verbindung
 - Keine Funktionen zur Sicherung des Datenkanals
 - Zuverlässiger Datentransport wird den höheren Protokollen (z.B. PPP) überlassen
 - Identifikation logischer Kanäle durch CID (Channel Identifier)
 - Drei unterschiedliche Kanalarten
 - Signalisierungskanal (CID=1): Signalisierungsnachrichten zwischen L2CAP Instanzen
 - Verbindungslose Kanäle (CID=2): z.B. Rundruf des Masters an alle Slaves
 - Verbindungsorientierte Kanäle (CID≥64): Kanal zwischen zwei Geräten
 - Kanäle zwischen Dienstgeber bzw. Dienstnehmer
 - Verbindungsorientierte Kanäle über CID identifiziert
 - Verbindungslose Kanäle über CID=2 & PSM identifiziert
 - PSM = Protocol and Service Multiplexer, (PSM sind analog zu Ports bei UDP)
 - Well-Known PSMs (z.B.: PSM1 für SDP und PSM3 für RFCOMM)
 - Zuordnung Profil – PSM erfolgt über SDP
 - Nummern werden beim Verbindungsaufbau übertragen

CID	Beschreibung
0x0000	Null
0x0001	Signalisierung
0x0002	Verbindungslose Kanäle
0x0003-0x003F	reserviert
0x0040-0xFFFF	frei verfügbar

PSM	Beschreibung
0x0001	SDP
0x0003	RFCOMM
0x0005	TCS-BIN
<0x1000	reserviert
0x1001-0xFFFF	verfügbar

Bluetooth Versionen

■ Version 1.0

- wurde im Juli 1999 verabschiedet

■ Version 1.1

- Erschien mit einigen Erweiterungen im Dezember 2000
 - Gleichzeitig bis zu 7 Verbindungen betreibbar
 - Messverfahren für Signalstärke hinzugefügt (Received Signal Strength Indicator, RSSI)
- Grundlage der Ausführungen in der Vorlesung

■ Version 1.2

- Unempfindlicher gegen elektromagnetische Störungen
 - Adaptives Frequenzspringen
 - Verbessert Koexistenz mit WLAN
 - Schlechte Frequenzen werden aus Sprungsequenz genommen
 - „Same Channel Communication“
 - Aufeinanderfolgende Zeitschlitze eines Masters und eines Slaves senden auf gleicher Frequenz
 - Gleiche Qualität für beide
 - Frequenzspringen 800-mal pro Sekunde

Bluetooth Versionen

■ Version 2.0

- Im November 2004 verabschiedet
 - „Enhanced Data Rate“ (EDR) mit ca. 3-facher Geschwindigkeit
 - Andere Form der Modulation: „Phase Shift Keying“ anstatt „Gaussian Shift Keying“
 - Bis zu 50% weniger Energieverbrauch

■ Version 2.1

- Im August 2007 verabschiedet
 - Secure Simple Pairing
 - Quality of Service

■ Version 3.0

- Im April 2009 verabschiedet
 - zusätzlicher Highspeed-Kanal auf Basis von IEEE 802.11
 - Anpassung L2CAP notwendig

Bluetooth Versionen

■ Version 4.0

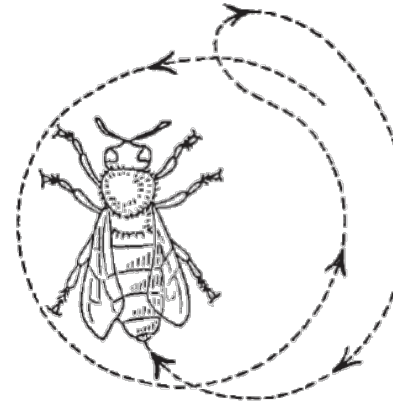
- Im Dezember 2009 verabschiedet
 - Schneller Verbindungsaufbau
 - Entfernungen bis 100m
 - Stromspar-Funktionen

■ Version 4.1

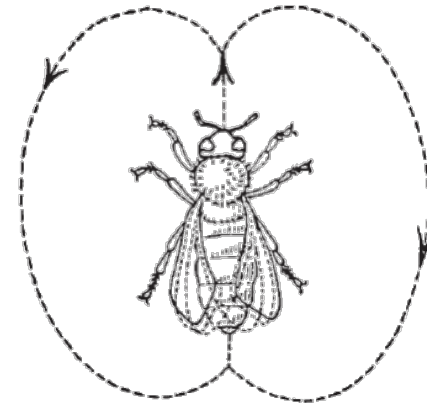
- Im Dezember 2013 verabschiedet
 - Verbesserte Koexistenz mit anderen Technologien (z.B. LTE)
 - Aufrechterhalten von Verbindungen mit weniger manuellen Eingriffen
 - Effizienterer Datenaustausch durch L2CAP Modifikationen
 - Geräte unterstützen mehrere Rollen
 - Aufbau dedizierter L2CAP Verbindungen

Zigbee

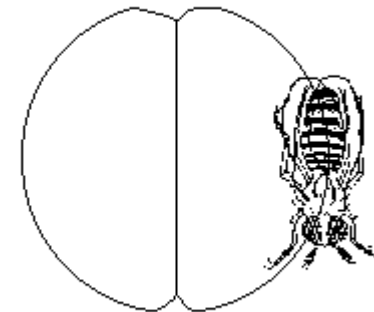
- Name „ZigBee“ stammt aus der Bienensprache
- Bienen teilen Standort neuer Futterquelle dem Stock mit – durch *Zick-Zack-Tanzen*
 - Rundtanz: Futter in Entfernung 50m-150m
 - Schwänzeltanz: Distanz >150m
- Länge des Tanzes Hinweis auf ungefähre Entfernung
 - Untersuchung: 2,5s tanzen entsprechen etwa 2,65 km
 - lineare Abhängigkeit
- Richtung der Quelle wird über Ausrichtung auf der (Tanz-)Geraden bestimmt
 - Quelle genau in Richtung der Sonne – im Stock hochklettern
 - Z.B. 60° links von der Sonne – 60° Grad links hochklettern
- „Empfang“ der Information durch Erfühlen (Dunkelheit im Stock!)



Rundtanz



Schwänzeltanz



ZigBee in a Nutshell



ZigBee™ Alliance

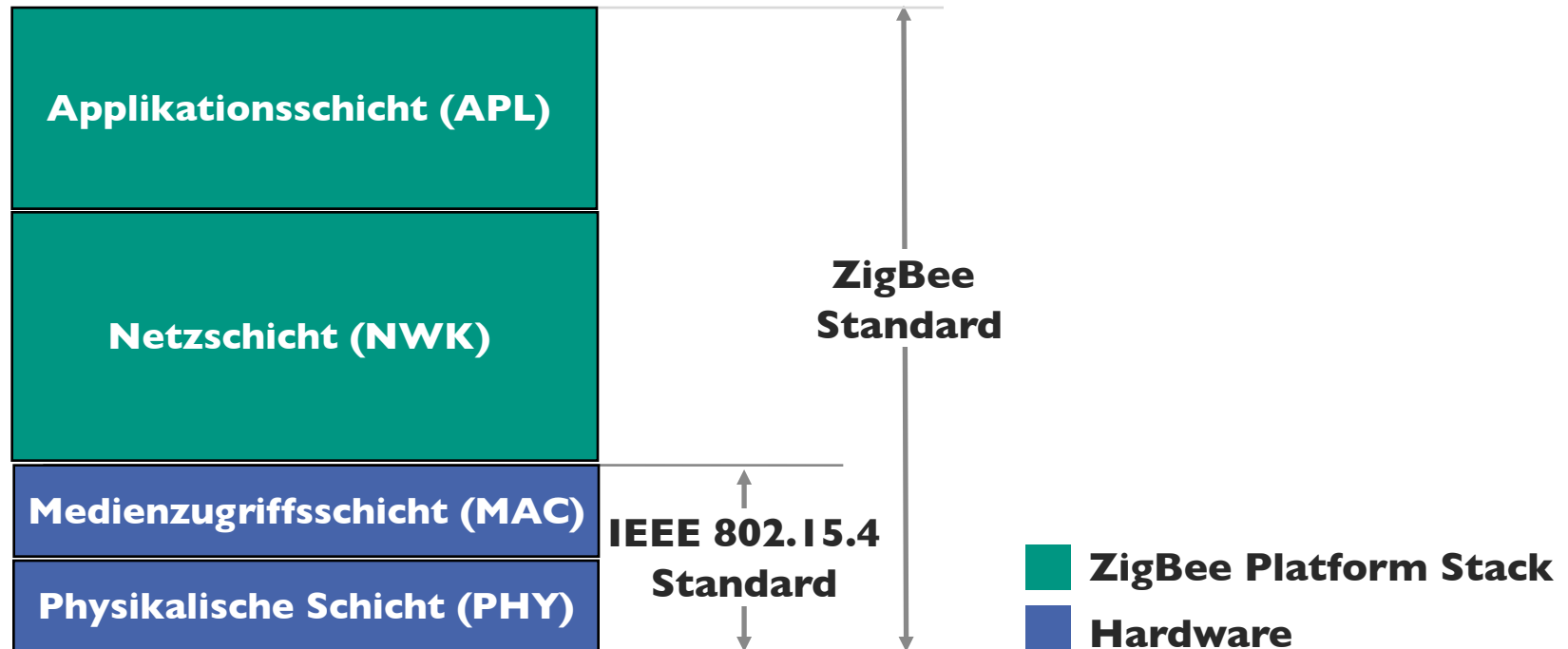
Wireless Control That Simply Works

*“To enable reliable, cost-effective, low-power, wirelessly networked, **monitoring and control** products based on an open global standard.”*

- Die ZigBee Alliance ist ein Firmenkonsortium, zu dem neben den Gründern Honeywell, Motorola, Mitsubishi Electric, Philips und Invensys inzwischen über 120 Partner gehören.
- Gegründet 2002
- Ziel ist Entwicklung eines neuen WPANs mit dem Fokus auf
 - Geringe Komplexität, geringe Kosten, geringer Durchsatz
 - Lange Batterielaufzeit
 - „Meshed Networks“

ZigBee vs. 802.15.4

- ZigBee spezifiziert
 - Höhere Schichten wie z.B. Anwendung und Vermittlung
 - Physikalische Übertragung und Sicherung (in IEEE 802.15.4)



- Bietet Kunden Kompatibilitätstest und Zertifizierungen an.
- Erste Produkte mit ZigBee sind 2005 ausgeliefert worden.

ZigBee Applikationsschicht

■ 3 funktionale Bestandteile

■ Application Support Sublayer (APS)

- Unterstützung von zuverlässigem Datentransfer
- Verwaltung von Gruppenadressen

■ ZigBee Device Object (ZDO)

- Definiert die Rolle eines Gerätes im Netz (Coordinator/Router/Device)
- Entdecken anderer Geräte und derer Anwendungen

■ Application Framework

- Umgebung in der sich die Anwendungen befinden

ZigBee Netzschicht

■ Aufgaben der ZigBee Netzschicht

- Zuweisung von Netzadressen durch Koordinator
- Aufbau und Erhalt von Routen zwischen Geräten
- Routing von Paketen zu Zielgeräten durch Router und Koordinatoren Beitritt zu und Austritt aus einem ZigBee-Netz
- Entdeckung von direkten Nachbarn
- Anwendung von Sicherheitsmaßnahmen auf Netzebene

Kommunikationsmuster und Topologien

■ Von ZigBee vorgesehene Kommunikationsmuster

- Unicast
- Broadcast
- Multicast

■ Mögliche Topologien

- Mesh: Jedes Gerät kann versuchen mit jedem anderen Kontakt aufzunehmen – entweder direkt oder über Router
- Hierarchische Baumtopologie: Unter den Geräten herrschen hierarchische Verwandtschaftsverhältnisse. Das Routing basiert auf einem Baumgraphen.

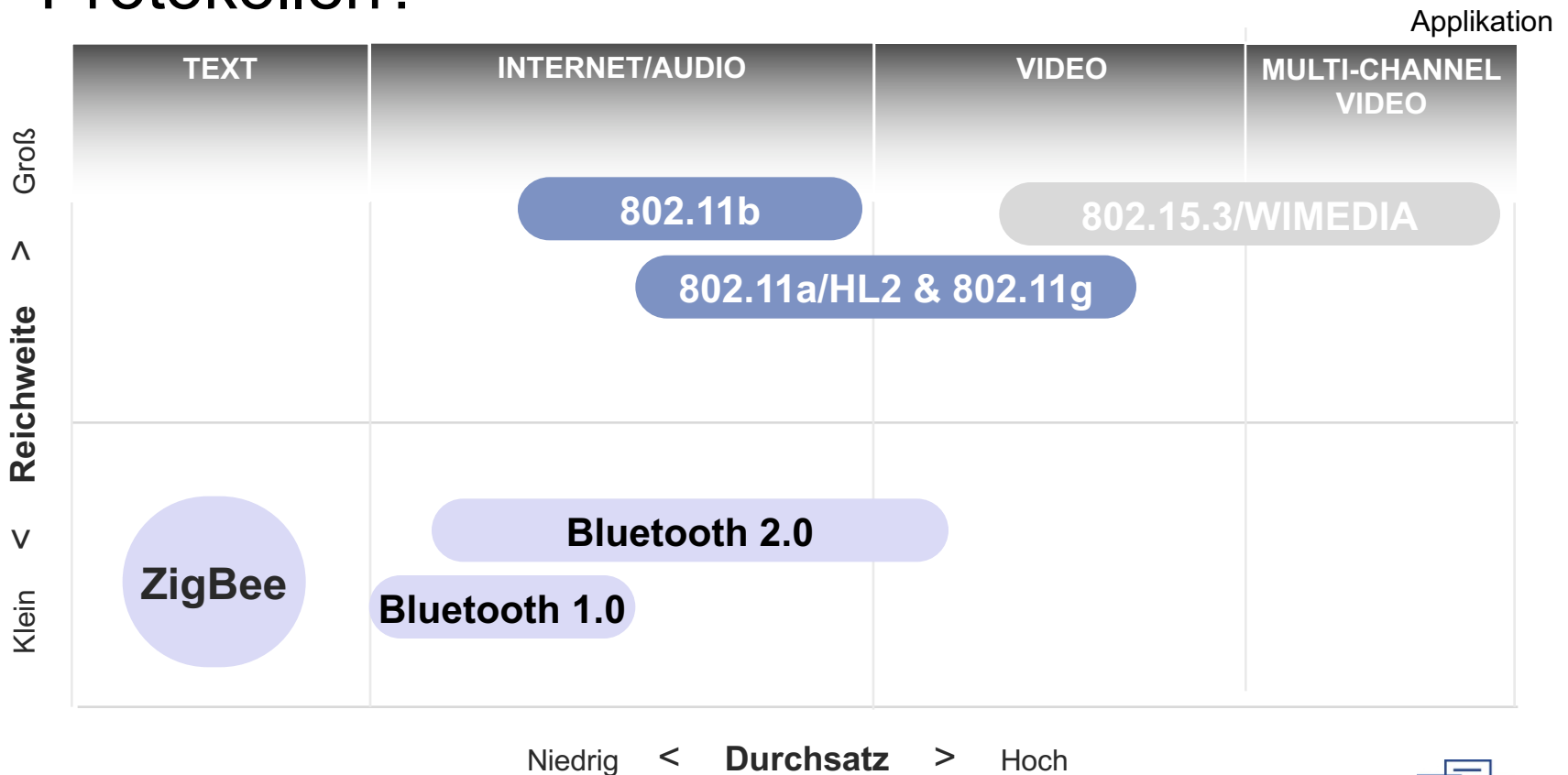
Kurzüberblick 802.15.4



- Kleine Paketgröße (< 128 Byte)
- Geringer Durchsatz (250 kBit/s)
- Geringer Energieverbrauch
- Reichweite bis 70 Meter
- 3 Frequenzbänder, nur eines weltweit verfügbar
 - 2,4 GHz, 16 Kanäle
- Verschiedene Netztypen möglich:
 - P2P/Mesh: Jeder kann mit jedem kommunizieren
 - Stern: Kommunikation nur über zentrales Gerät
- 2 Gerätearten
 - **Vollfunktionstüchtige Geräte** (Full Function Devices, FFD)
 - **Eingeschränkte Geräte** (Reduced Function Devices, RFD), nur in Stern-Netzen
- Ausführlicher behandelt in DSAN-Vorlesung

ZigBee vs. Bluetooth vs. ...

■ Wie „passt“ ZigBee zu anderen Wireless-Protokollen?



ZigBee vs. Bluetooth

	Bluetooth	ZigBee/802.15.4
Modulationstechnik	Frequency Hopping Spread Spectrum (FHSS)	Direct Sequence Spread Spectrum (DSSS)
Durchsatz	768 kbit/s	250 kbit/s
Reichweite	1, 10 oder 100m	Bis 70m
Verbindungsaufbau	≈3 s	30 ms
Sendeleistung	1mW-100mW	10mW-1000mW
Geräte pro „Master“	7	64000

Obwohl 802.15.4 teilweise mehr Strom zum Senden verbraucht, ist es auf Grund „cleverer“ Energiesparmodi (längere Schlafzeiten, keine Notwendigkeit ständig Frequenzen zu synchronisieren usw.) insgesamt stromsparender als Bluetooth.

■ Wireless Personal Area Networks

- Vernetzung von (kleinen) Geräten im direkten Umfeld, Vision „Ubiquitäre Netze“
- Begrenzte Reichweite, Energie, etc.
- Autonome Netze

■ Verschiedene Technologien

- (Infrarot, proprietärer Funk)
- Bluetooth
 - Frequenzsprung (Sequenz und Phase)
 - Piconetz – Master, Slave
 - Scatternetz – Verbund mehrerer Piconetze
 - Inquiry, Paging
- ZigBee
 - Stern-/Mesh-Netze
 - Koordinator
 - Unterschiedliche Kommunikationstypen

- 6.1 Nennen Sie Unterschiede zwischen WLANs und WPANs!
- 6.2 Beschreiben Sie die Struktur eines Pico-/Scatternetzes!
- 6.3 Welche Arten von Brücken zwischen verschiedenen Pico-Netzen gibt es in einem Scatternetz?
- 6.4 Wie funktioniert das Frequenzspringen in Bluetooth?
- 6.5 Was ist der Unterschied zwischen Paging und Inquiry?
Beschreiben Sie die Prozeduren!
- 6.6 Welche LMP-Betriebsmodi gibt es?

Referenzen und weiterführende Literatur

- [6.1] J. Roth, Mobile Computing, dpunkt-Verlag, 2005
- [6.2] <http://bluez.sourceforge.net/>
- [6.3] B. A. Miller, C. Bisdikian, Bluetooth Revealed, Prentice Hall, 2002
- [6.4] What You Should Know About the ZigBee Alliance
<http://www.zigbee.org>,
- [6.5] <http://www.elektroniknet.de>
- [6.6] http://www.lisha.ufsc.br/~guto/teaching/ish/ine5346-2003-1/work/bluetooth/hci_commands.html
- [6.7] Vorlesung „Ubiquitäre Systeme“,
<http://www.teco.edu/lehre/#vorlesung>
- [6.8] J. Schiller, Mobilkommunikation, Pearson Studium, 2003
- [6.9] NC State University, The Honey Bee Dance Language,
<http://www.cals.ncsu.edu/entomology/apiculture/PDF%20files/1.11.pdf>
- [6.10] S. Farahani, ZigBee Wireless Networks and Transceivers, Newnes, 2008
- [6.11] <http://shapp.at/MN8>