Mobilkommunikation

V. Drahtlose persönliche Netze

Kapitel 8

Bluetooth

Kapitelübersicht

I. Einleitung
1. Einführung und Grundlagen

II. Drahtlose Telekommunikationssysteme
2. GSM
3. UMTS

III. Drahtlose lokale Netze
4. IEEE 802.11 / WiFi
5. Mobile Ad Hoc Netze

IV. Drahtlose innerstätische Netze
6. IEEE 802.11s
7. IEEE 802.16 / WiMax

V. Drahtlose persönliche Netze
8. Bluetooth
9. IEEE 802.1.54 / ZigBee

VI. Positionsbestimmung
10. Positionsbestimmung

VII. Mobiles Internet
11. Mobile Vermittlungsschicht
12. Mobile Transportschicht

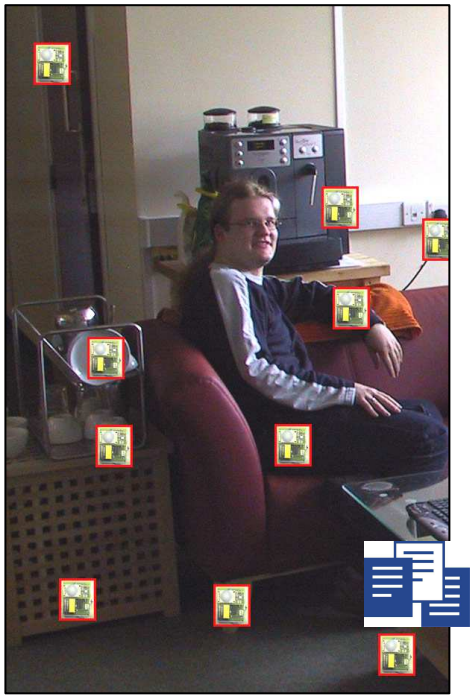
8.1 Motivation WPANs
8.2 Bluetooth Übersicht
8.3 Anwendungsbeispiele
8.4 Übertragung/Netzarchitektur
8.5 Protokollstack
8.6 Verbindungsverwaltung
8.7 Dienstfindung
8.8 Bluetooth Versionen

8.1 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



[V.7]

Charakteristika von WPANs

- 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
- Drahtlose Kommunikation
  - i.A. über Funk (oder Infrarot)
- 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)
  - RFIDs
  - Laser, z.B. „Smart Dust“ (Berkeley)
- Standardisierte Technologien
  - Infrarot
    - Proprietär, ParcTab (Xerox PARC)
    - IRDA, z.B. iCricket (MIT)
  - Funk (IEEE Arbeitsgruppe 802.15)
    - Bluetooth
    - ZigBee

8.2 Bluetooth

- 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

[V.3]

… zur Namensgebung

- Nach Harald dem I., Wikingerkönig von Dänemark, 911-970, genannt Harald Blatand (=„Blauzahn“)
  - Gerüchten zu folge litt er an einer chronischen Krankheit, die seine Zähne blau färbte …
  - Christianisierte Dänemark
  - Vereinigte große Teile Skandinaviens
    - Dänemark, Schweden, Norwegen

- Bluetooth vereinigt Kommunikation verschiedener Kleingeräte
  - Mobiltelefone, PDAs, Sensoren etc.
- Bluetooth-Logo
  - Enthält die Runen „H“ und „B“

8.3 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

Anwendungsbeispiele

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

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

8.4 Übertragung/Netzarchitektur

- Verwendung des lizenzfreien ISM-Bands (2,4 GHz)
  - Aufteilung in 79 Kanäle (nur 23 in Frankreich, Spanien und Japan)
  - Teilt sich Medium mit u.A. WLAN oder Mikrowellen
    - Frequenzsprungverfahren (später mehr) jedoch sehr robust
- Datenrate
  - 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)

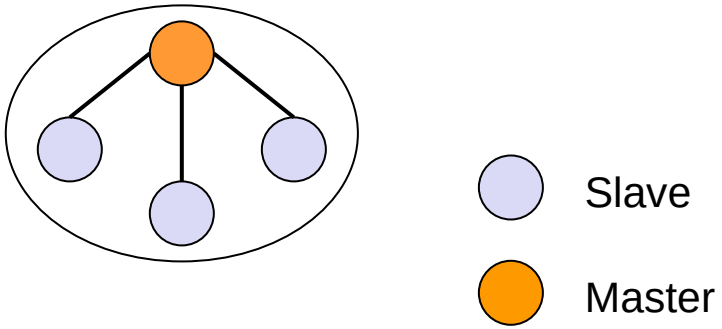
- Zusammenfassung

Eigenschaft	Wert
Reichweite	Klasse 1: 100m, Klasse 2: 10 m, Klasse 3: 10 cm
Ausgangsleistung	Klasse 1: 100mW, Klasse 2: 2,5mW, Klasse 3: 1mW
Frequenzen	2400-2483,5 MHz
Datenraten	brutto max. 1 Mbits/s, netto max. 723 kbit/s

Netzarchitektur - Pikonetz

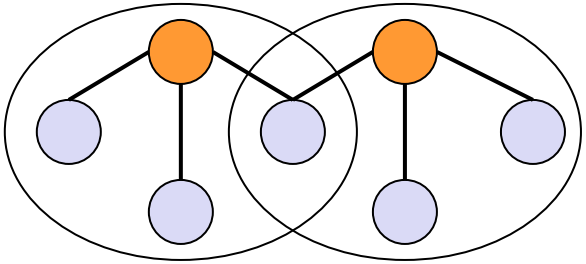
- Grundform: Pikonetz
  - 1 Master
    - verteilt Senderecht an die Slaves
  - 1 bis 7 Slaves
    - können nur über den Master miteinander kommunizieren
    - Keine direkte Kommunikation zwischen Slaves möglich
  - Jedes Gerät kann Master oder Slave sein
    - Gerät, das ein Pikonetz aufbaut wird zunächst automatisch zum Master
    - Master kann während des Betriebs wechseln

Skizze eines Pikonetzes

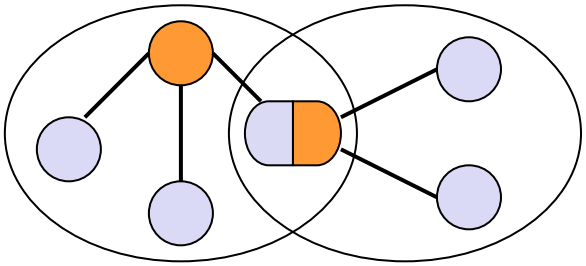


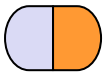
Netzarchitektur - Scatternetz

- Für größere Netze: Scatternetz
  - Überlappung mehrerer Pikonetze
    - Genau 1 Master pro Pikonetz !
  - 1 Knoten kann
    - in mehreren Pikonetzen Slave sein



    - aber nur in einem Pikonetz als Master fungieren

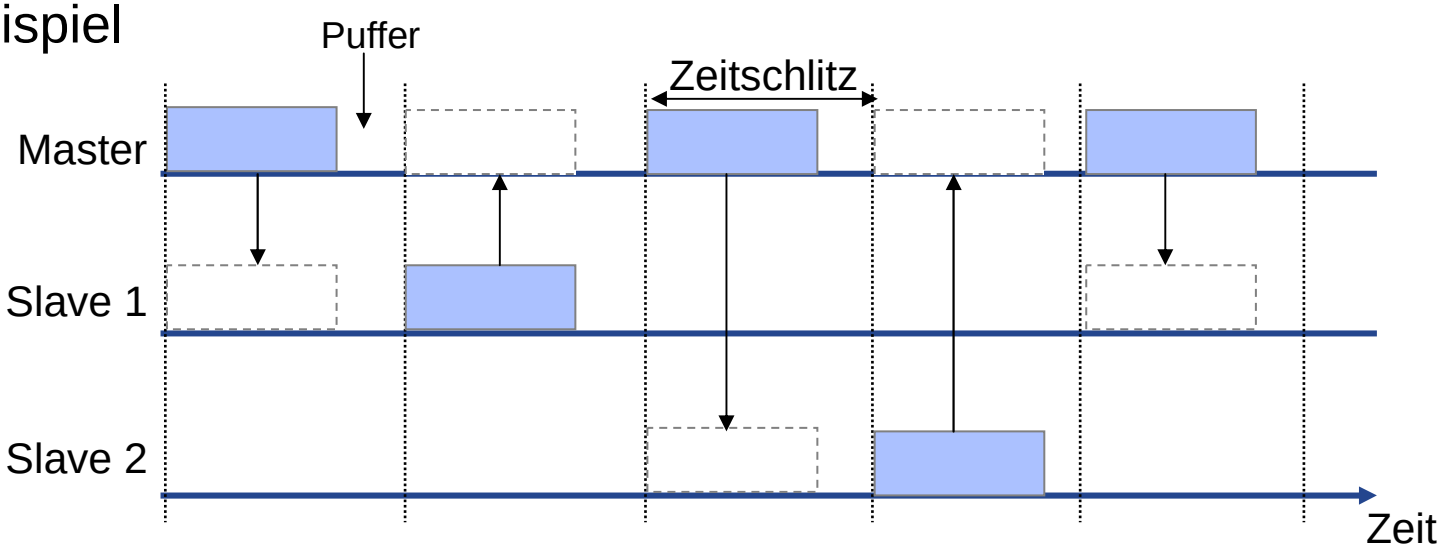




Slave in einem Pikonetz und Master in einem anderen

Master steuert Übertragung

- Time Division Duplex (TDD)
  - Übertragung ist in Zeitschlitze gegliedert
    - Dateneinheiten beanspruchen typischerweise einen Zeitschlitz
    - Es existieren auch Dateneinheiten die 3 oder 5 Zeitschlitze benötigen
  - Zeitschlitze werden wechselweise von Master und Slave genutzt
    - Master nutzt ungerade Zeitschlitze, Slaves nutzen gerade Zeitschlitze
    - 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



Frequenzspringen

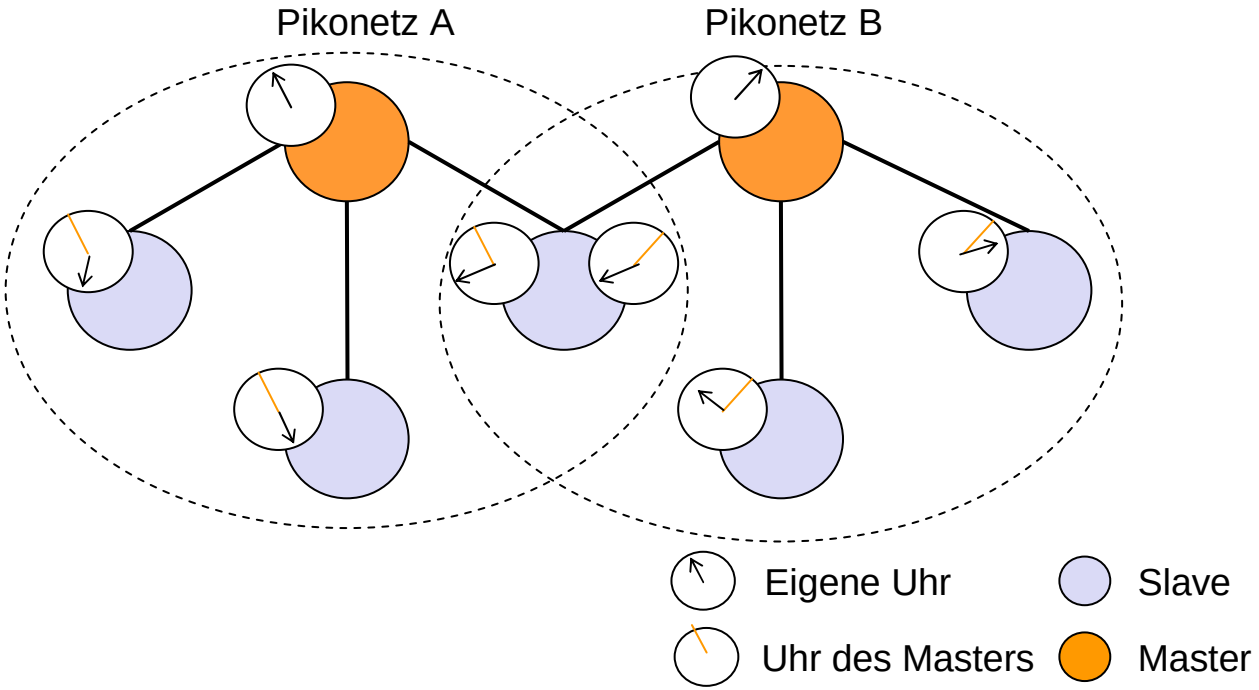
- Ziel
  - Robuste Kommunikation zwischen Bluetooth-Geräten
- Verwendung von Frequenzspringen
  - Frequenzwechsel erfolgen zwischen Zeitschlitzen bzw. zwischen Dateneinheiten
    - Bei Dateneinheiten, die länger als ein Zeitschlitz sind, wird die Frequenz beibehalten. Ansonsten wechselt die Frequenz nach jeder Dateneinheit.
    - Dabei wird ursprüngliches Schema beibehalten
      - Bei einer Dateneinheit von 3 Zeitschlitzen 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 s = 625 µs
- 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 und gleiche Phase der Sequenz
  - Sequenz (Sprung-Sequenz oder „Hopping-Sequenz“) ist eine Pseudo-Zufallszahlenfolge
  - Sequenz selbst vom Master vorgegeben
    - Berechnet aus seiner Geräteadresse
  - Aktuelle „Phase“ der Hopping-Sequenz bestimmt durch die Uhr des Masters
    - Damit kennen Master und Slave die aktuelle Frequenz
  - Die Hopping-Sequenzen in verschiedenen Pikonetzen unterscheiden sich
    - … Master kann also nicht in zwei oder mehr Pikonetzen agieren sondern ist auf eines beschränkt!

Synchronisation in Scatternetzen

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



- Problem unterschiedliche Sprungfrequenzen: Ein Slave kann immer nur in einem Pikonetz aktiv sein.
  - Abmelden im alten Netz (=“Parken”)
  - Anmelden im aktiven Netz

[V.8]

Inquiry-Prozedur

- Aufgabe: Finden von anderen Geräten
- Probleme
  - Geräte, die nicht Mitglied im Pikonetz sind, können nicht dem dortigen Frequenzspringen folgen.
  - Sie kennen auch nicht die aktuelle Phase der Sprungsequenz
- Vorgehensweise
  - Generieren einer speziellen Inquiry-Sprungsequenz
    - Besteht aus 32 Frequenzen (bzw. 16 davon für Spanien …)
      - Sind allen Geräten auch ohne Mitgliedschaft in einem Pikonetz bekannt
    - Sequenz dieser Frequenzen wird durch jeweilige Geräteadresse bestimmt
      - Alle Geräte hören auf diesen Frequenzen mit ihrer speziellen Sequenz

Inquiry-Prozedur

- Suchende und hörende Geräte nutzen unterschiedliche Häufigkeiten des Springens – sie „treffen“ sich nach einer gewissen Zeit
  - Suchendes Gerät wählt alle 312,5 µs eine neue Frequenz
  - Hörende Geräte wählen alle 1,28 s eine neue Frequenz
- Inquiry-Dateneinheiten enthalten einen allen Geräten bekannten Inquiry Access Code
- Hörende Geräte antworten unter anderem mit ihrer Geräteadresse, ihrer Uhr und ihrer Geräteklasse
  - Dadurch gelingt späteres Paging schneller

… immer sichtbar?

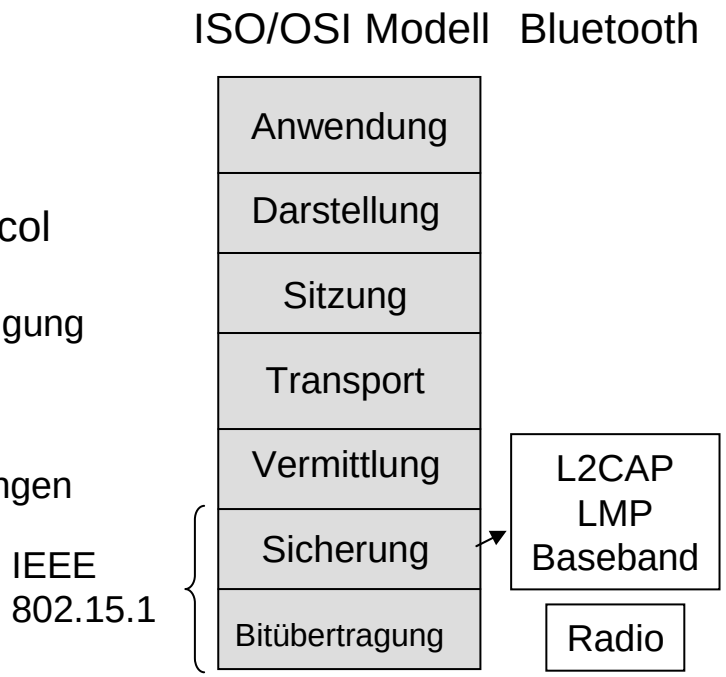
- Beobachtung
  - Die Inquiry-Prozedur erfordert, dass das Bluetooth-Gerät sichtbar ist … wollen wir das immer?
    - Privatsphäre
    - Angriffe auf Fehlerhafte Bluetooh-Implementierungen, z.B. BlueSnarf, Chaos, BlueBug, …
      - Auslesen von Adressbüchern
      - Initiieren von Telefongesprächen
      - …?
- … don´t panic
  - Anwender kann das Verhalten seines Bluetooth-Gerätes beeinflussen
  - Bluetooth-Geräte ermöglichen Unsichtbarkeit
    - Keine Antwort auf Inquiries
    - Verbindungsaufbau über Page dennoch möglich
    - Keine Sicherheitsgarantie! Geräteadresse kann man erraten…

Paging-Prozedur

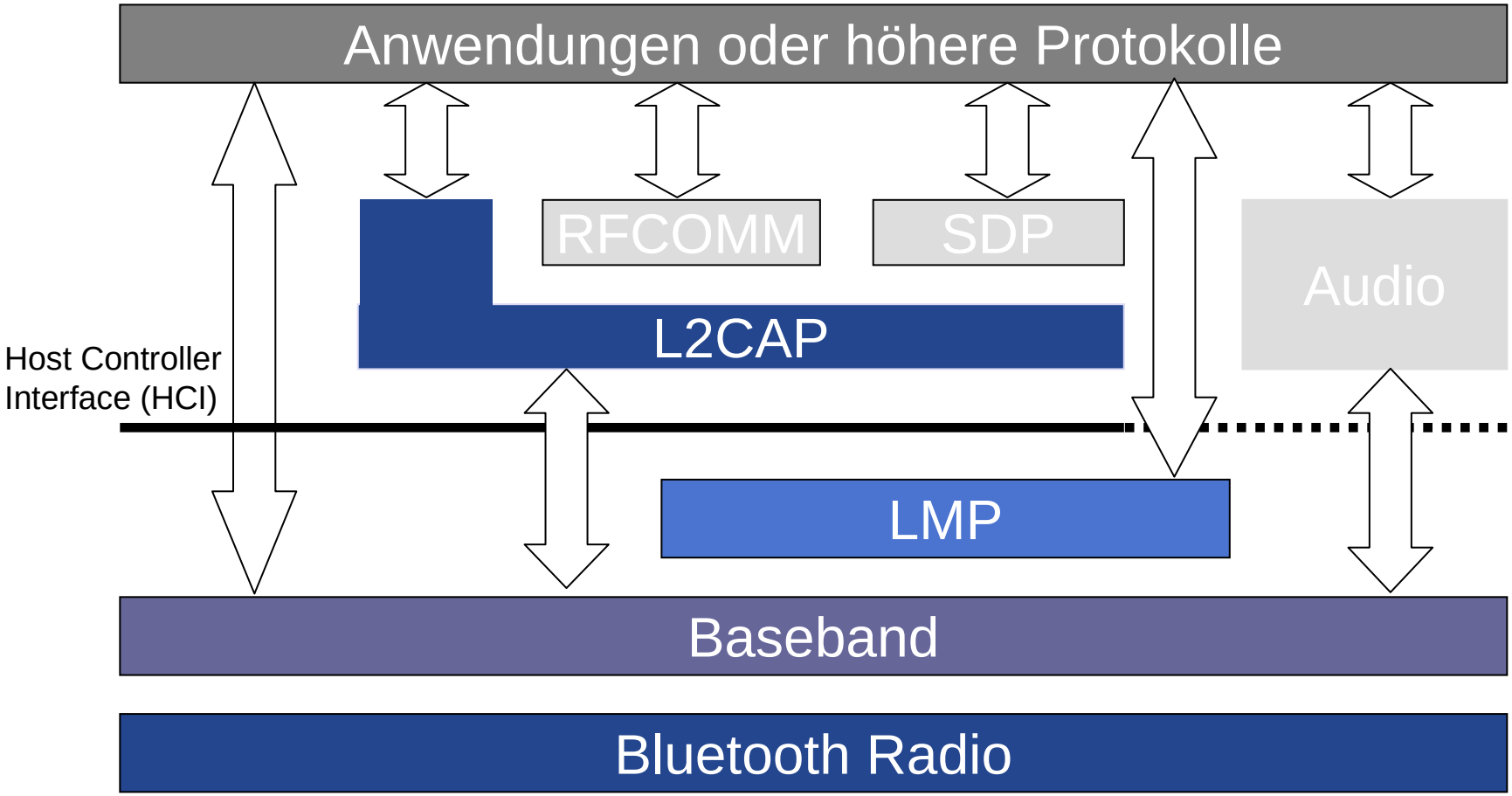
- Aufgabe
  - Ein Gerät soll in ein Pikonetz eingeladen werden
- Voraussetzung
  - Geräteadresse des einzuladenden Geräts ist bekannt
    - Hierfür sorgt die Inquiry-Prozedur
    - Bekannte Uhrzeit beschleunigt Paging-Prozedur
- Ablauf
  - Einladendes Gerät berechnet Sprungsequenz aus der Geräteadresse 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 eine Phase „danach“ oder „davor“ gesucht
  - Beide Geräte nutzen unterschiedliche Wechselgeschwindigkeiten für die Sprungsequenz
    - Einladendes Gerät wählt alle 312,5 µs eine neue Frequenz
    - Eingeladenes Gerät wählt alle 1,28 s eine neue Frequenz
  - Das Gerät, dass die Paging Prozedur ausführt wir Master der Verbindung

8.5 Protokollstack

- Für Bluetooth ist bereits eine Vielzahl von Protokollen spezifiziert. Hierzu gehören
  - 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)
      - Regelt Verschlüsselung für einen Link
      - Gleicht Uhren ab
      - Tauscht Master-Slave
      - Stellt Sendeleistung ein
    - Logical Link Control and Adaption Protocol (L2CAP)
      - Stellt pro Link mehrere Kanäle zur Verfügung
      - Regelt Dienstgüte
  - Profilspezifikationen
    - Protokolle und Funktionen zur Anpassungen an Anwendungen



Protokollstack im Überblick

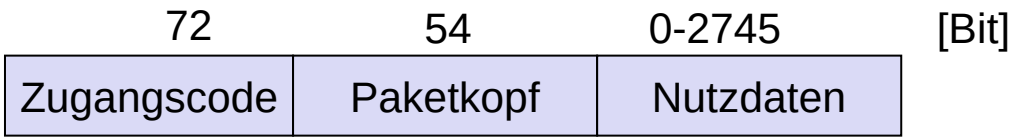


Aufgaben der Schichten

- Bluetooth Radio und Basisband
  - Stellen Zugriff von höheren Protokollschichten auf das Funk-Medium bereit
- LMP (Link Manager Protocol)
  - Verwaltung von Verbindungen
- L2CAP (Logical Link Control and Adaption Protocol)
  - Bereitstellung mehrerer logischer Kanäle
  - Segmentierung großer Daten
- 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 Daten, bei Datenaustausch
  - Zugangscode
    - Identifiziert Pikonetz
    - Ist abgeleitet von der Gerätekennung des Masters
    - Besteht aus
      - Präambel zur Synchronisierung
      - Synchronisationsfeld, das Zweck 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 Pikonetz 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

3	4	1	1	1	8	[Bit]
MAC-Adresse	Typ	Flow	ARQN	SEQN	HEC	

  - Senden mit 1/3 Vorwärtsfehlerkorrektur (FEC)
    - Jedes Bit wird dreimal gesendet
      - 3 x 18 Bit = 54 Bit

8.6 Verbindungsverwaltung

- Aufgabe 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 Zeitschlitze („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 Zeitschlitze ist ein Zeitschlitz reserviert
    - *HV2*: FEC mit 2/3 Coderate, alle 4 Zeitschlitze ist ein Zeitschlitz reserviert
    - *HV3*: ohne FEC, alle 6 Zeitschlitze 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 Zeitschlitze, die eine Dateneinheit einnehmen darf (bis zu 5)
    - Es findet kein Frequenzwechsel zwischen diesen Zeitschlitzen statt

LMP – Link Management Protocol

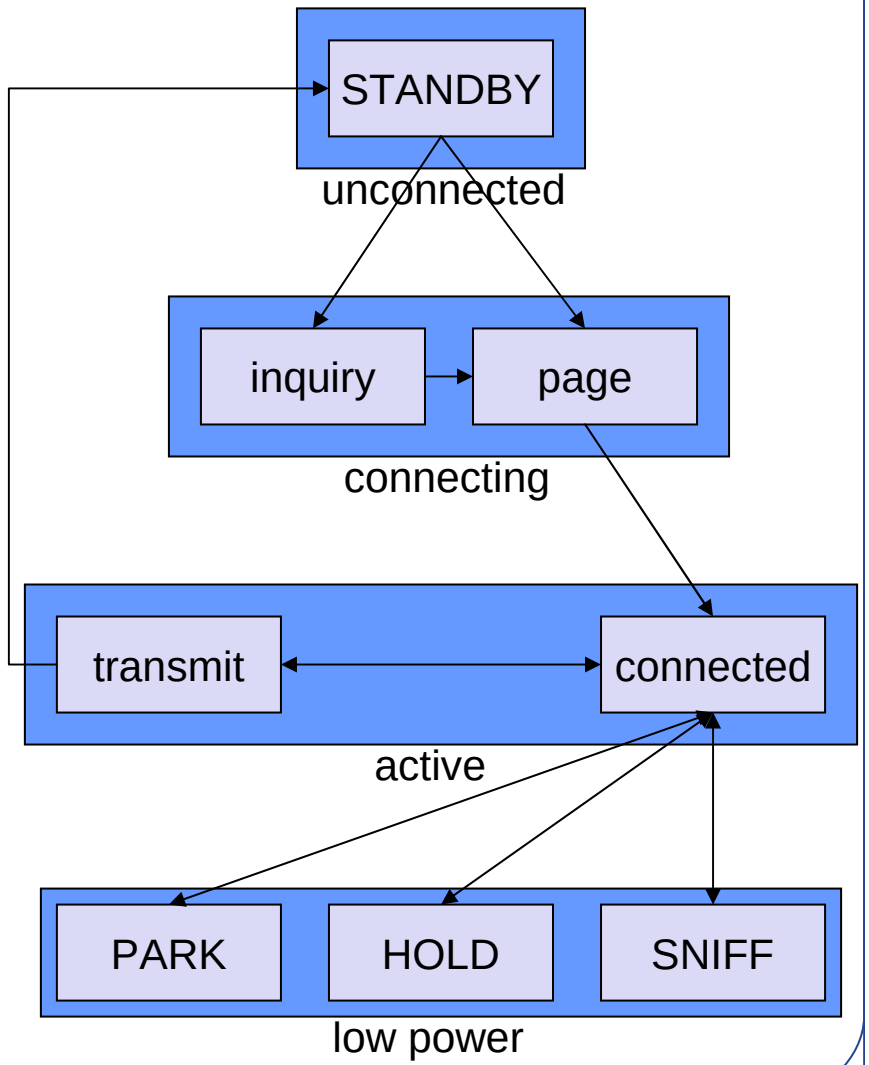
- Authentifikation und Verschlüsselung
  - Authentifikation des Kommunikationspartners („Pairing“), da Daten von dritter Seite über die Luftschnittstelle gesendet werden können
    - Basierend auf Challenge-Response-Verfahren
    - Aus „Shared Secret“ (PIN) wird gemeinsamer Schlüssel berechnet
    - Challenge ist 16-Byte-Zufallszahl
  - Verschlüsselung der Daten, da diese bei der Übertragung abgehört werden können (optional)
    - Symmetrische Verschlüsselung über SAFER+
    - 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

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 Pikonetzes (behält Active Member Address)
- HOLD
  - Gerät schläft einmalig für „hold time“
  - Gerät bleibt aktiver Teil des Pikonetzes (behält Active Member Address)
- PARK
  - Gerät kein aktiver Teil des Pikonetzes mehr (erhält Parked Member Address)
  - Erhaltung der Synchronisation durch Beacons, die in großen Abständen vom Master gesendet werden



L2CAP

- L2CAP: Logical Link Control and Adaption Layer Protocol
- Funktionen
  - Zerlegen großer Dateneinheiten in mehrere kleine Teile für den Transport (Segmentation and Reassembly – SAR)
    - Basisbandübertragung wird variabel ausgehandelt
    - Max. L2CAP-Dateneinheit (MTU) wird ausgehandelt (bis 64 kByte)
    - Nur Teile *einer* Dateneinheit werden hintereinander über die Verbindung versendet, d.h. es werden keine Dateneinheiten unterschiedlicher Anwendungen gemultiplext
  - 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 jeweilige 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)
  - Zwei unterschiedliche Kanalarten
    - Verbindungsorientierte Kanäle: Kanal zwischen zwei Geräten
    - Verbindungslose Kanäle: Ein Sender, mehrere Empfänger (Multicast)
  - Häufige Verwendung zweier Geräte als Dienstgeber bzw. Dienstnehmer
    - Identifikation von Diensten erfolgt über L2CAP-PSM-Nummern (Protocol and Service Multiplexer), PSM sind analog zu Ports bei TCP
    - Nummern werden beim Verbindungsaufbau übertragen
    - Zuordnung Profil – PSM erfolgt über SDP
    - Well-Known PSMs (z.B.: PSM1 für SDP und PSM3 für RFCOMM)

CID	Beschreibung
0x0000	Null
0x0001	Signalisierung
0x0002	Empfang von Multicast-Nachrichten
0x0003-0x003F	reserviert
0x0040-0xFFFF	frei verfügbar

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

8.7 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)
  - Derzeit Grundlage der meisten Produkte
  - 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
- 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
- Zukunft: Ultra-Wide-Band?

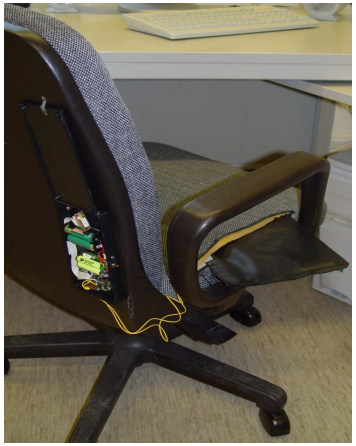
Anwendungen am Institut

Multifunktionale Sensorknoten

BlueEgg
Mini-Ausgabe eines Sensorknoten

- Mikrocontroller, Batterie, Bluetooth
- Bewegungssensoren
- Steckbare Erweiterungen: weitere Sensoren, LEDs, Lautsprecher

Alltagsgegenstände als Sensorknoten



BlueChair

BlueCup

Erkennen Kontext und können diesen kommunizieren

- Drucksensor
- Bewegungssensoren

- Bewegungssensoren
- Temperatursensor
- Füllstandsensor

Mobilkommunikation

V. Drahtlose persönliche Netze

Kapitel 9

IEEE 802.15.4 / ZigBee

Kapitelübersicht

I. Einleitung
1. Einführung und Grundlagen

II. Drahtlose Telekommunikationssysteme
2. GSM
3. UMTS

III. Drahtlose lokale Netze
4. IEEE 802.11 / WiFi
5. Mobile Ad Hoc Netze

IV. Drahtlose innerstätische Netze
6. IEEE 802.11s
7. IEEE 802.16 / WiMax

V. Drahtlose persönliche Netze
8. Bluetooth
9. IEEE 802.1.54 / ZigBee

VI. Positionsbestimmung
10. Positionsbestimmung

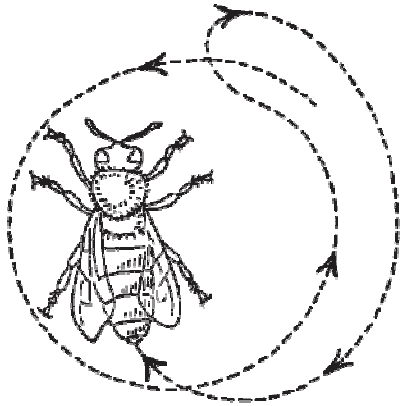
VII. Mobiles Internet
11. Mobile Vermittlungsschicht
12. Mobile Transportschicht

9.1 ZigBee Übersicht
9.2 IEEE 802.15.4 Grundlagen
9.3 Dateneinheiten
9.4 IEEE 802.15 Arbeitsgruppen
9.5 Zusammenfassung WPAN

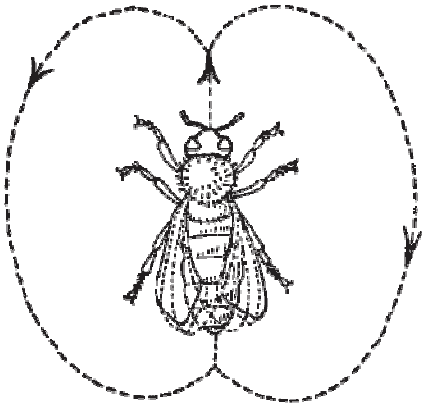
Übungen
Referenzen

Bienentanz

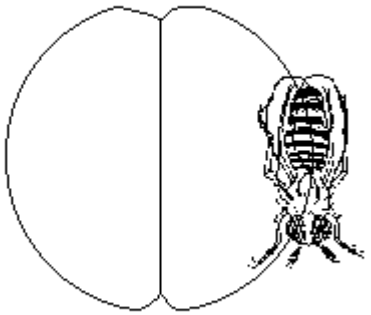
- Name „ZigBee“ stammt aus der Bienensprache
- Bienen teilen Standort neuer Futterquelle dem Stock mit – durch *Zick-Zack-Tanzen*
- Rundtanz – Futter in Entfernung 50m-150m
- Schwänzeltanz – Distanz >150m
- Länge des Tanzes Hinweis auf exakte Entfernung
  - z.B. 2,5s Schwänzeln entsprechen etwa 2,6km
  - 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



[V.9]

5.3 ZigBee

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."

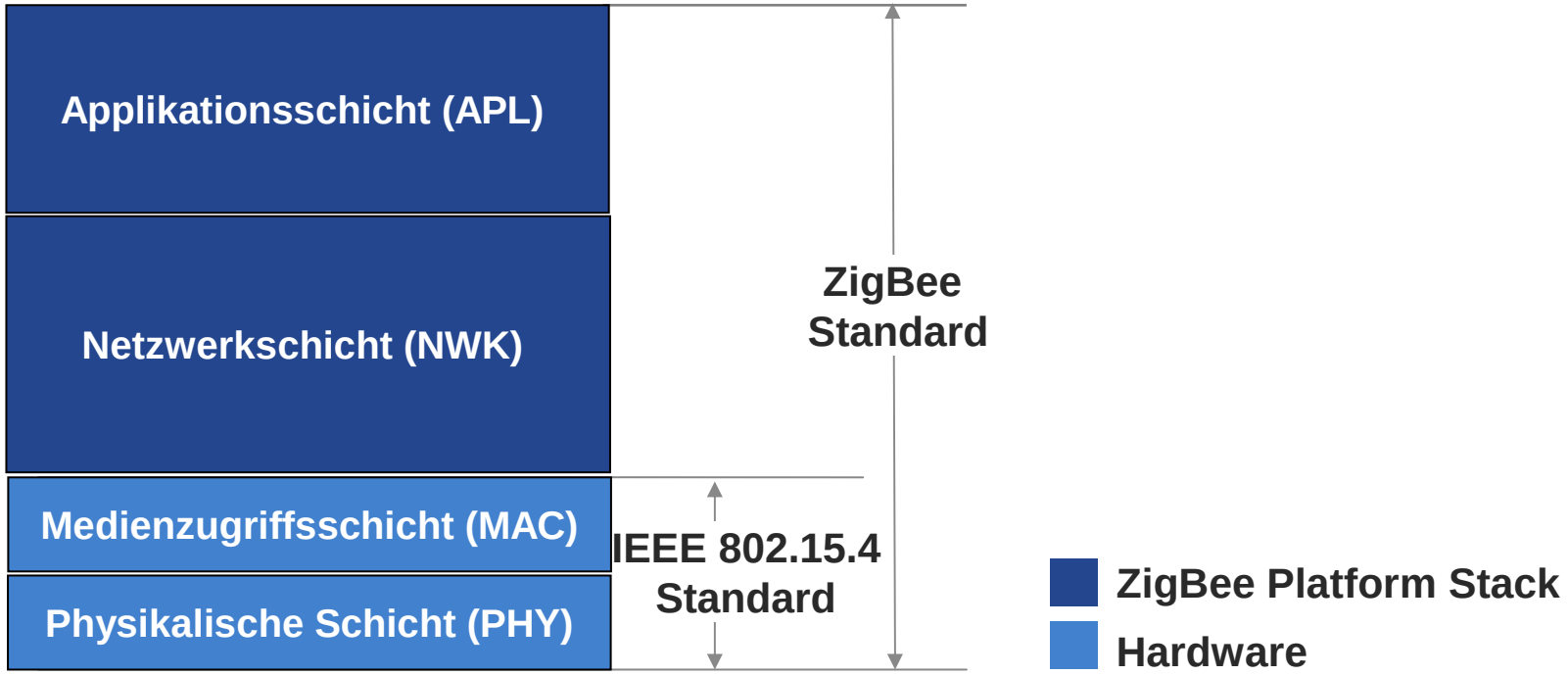
- Die ZigBee Alliance ist ein Firmenkonsortium, zu dem neben den Gründern Honeywell, Motorola, Mitsubishi Electric, Philips und Invensys inzwischen über 120 Partner gehören.
- Gegründet 2002
- Ziel ist Entwicklung eines neuen WPANs mit dem Fokus auf
  - Geringe Komplexität, geringe Kosten, geringer Durchsatz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

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 zentralen Knoten
- 2 Gerätearten
  - Vollfunktionstüchtige Geräte (Full Function Devices, FFD)
  - Eingeschränkte Geräte (Reduced Function Devices, RFD), nur in Stern-Netzen
- Ausführlicher behandelt in DSAN-Vorlesung

ZigBee-Allianz

- Spezifiziert
  - physikalische Übertragung und Sicherung (in IEEE 802.15.4)
  - höhere Schichten wie z.B. Darstellung oder Transportschicht



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

Die ZigBee Netzwerkschicht

- Aufgaben der ZigBee Netzwerkschicht:
  - Zuweisung von Netzwerkadressen durch Coordinator (ein bestimmtes FFD im ZigBee PAN)
  - Aufbau und Erhalt von Routen zwischen Geräten
  - Routing von Paketen zu Zielgeräten durch Router und Coordinatoren (beides FFD)
  - Beitritt zu und Austritt aus einem ZigBee-Netzwerk
  - Entdeckung von direkten Nachbarn
  - Anwendung von Sicherheitsmaßnahmen auf Netzwerkebene

Kommunikationsmuster und Topologien

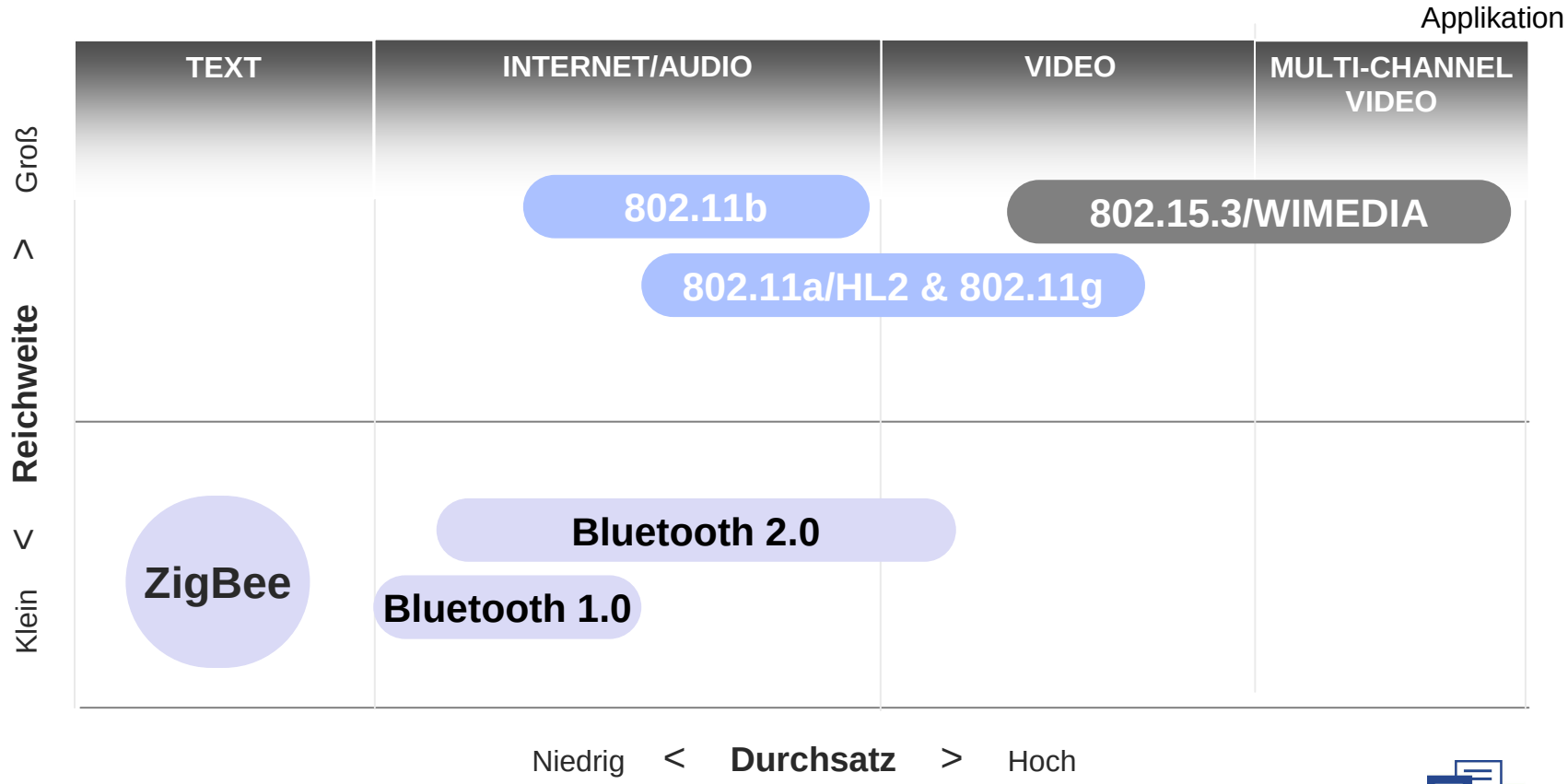
- Von ZigBee vorgesehene Kommunikationsmuster:
  - Unicast
  - Broadcast
  - Multicast
- Mögliche Topologien
  - Mesh: Jeder Knoten kann versuchen mit jedem anderen Kontakt aufzunehmen – entweder direkt oder über Router
  - Hierarchische Baumtopologie: Unter den Knoten herrschen hierarchische Verwandschaftsverhältnisse. Das Routing basiert auf einem Baumgraphen.

Die 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 vs. Bluetooth

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



[V.4]

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
Knoten pro „Master“	7	64000

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

9.5 Zusammenfassung WPAN

- 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)
    - Pikonetz – Master, Slave
    - Inquiry, Page
  - ZigBee
    - Stern-/Mesh-Netze
    - Koordinator
    - Unterschiedliche Kommunikationstypen

V. Übungen

1. Nennen Sie Unterschiede zwischen WLANs und WPANs!
2. Welche Aufgabe hat RFCOMM?
3. Welche Dienste stellt Bluetooth zur Verfügung?
4. Wofür stehen ACL und SCO – und worin unterscheiden sie sich?
5. Welche Probleme können beim Aufbau eines Scatternetzes entstehen?
6. Was ist der Unterschied zwischen Page und Inquiry?
7. Welche Aufgabe hat der Koordinator?

Referenzen und weiterführende Literatur

- [V.1] J. Roth, Mobile Computing, dpunkt-Verlag, 2005
- [V.2] http://bluez.sourceforge.net/
- [V.3] B. A. Miller, C. Bisdikian, Bluetooth Revealed, Prentice Hall, 2002
- [V.4] What You Should Know About the ZigBee Alliance http://www.zigbee.org,
- [V.5] http://www.elektroniknet.de
- [V.6] http://www.lisha.ufsc.br/~guto/teaching/ish/ine5346-2003-1/work/bluetooth/hci_commands.html
- [V.7] Vorlesung „Ubiquitäre Systeme“, http://www.teco.edu/lehre/#vorlesung
- [V.8] J. Schiller, Mobilkommunikation, Pearson Studium, 2003
- [V.9] NC State University, The Honey Bee Dance Language, http://www.cals.ncsu.edu/entomology/apiculture/PDF%20files/1.11.pdf
- [V.10] S. Farahani, ZigBee Wireless Networks and Transceivers, Newnes, 2008