Humboldt-Universität Informatik

Humboldt Universit t zu Berlin
Institut f r Informatik

Wireless Personal Area Networks

Spezielle Techniken der Rechnerkommunikation

Jörg Pohle, pohle@informatik.hu-berlin.de
Daniel Apelt, apelt@informatik.hu-berlin.de

Überblick

(W)PAN

Ultraweitband

Bluetooth

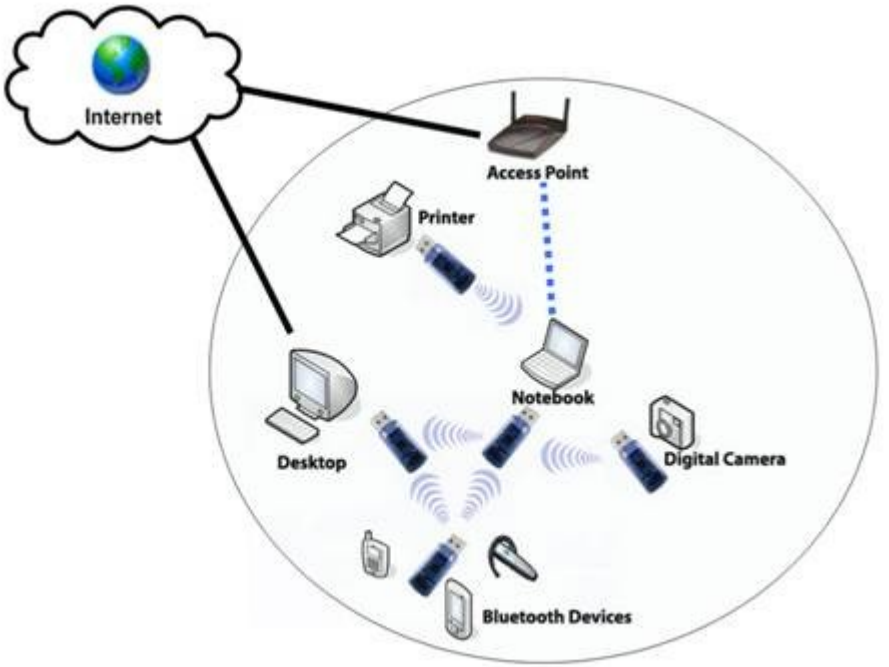
Wireless USB

ZigBee

(W)PAN

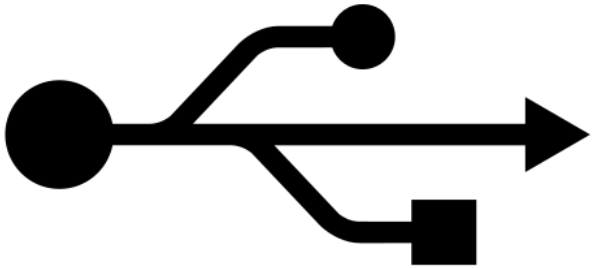
(Wireless) Personal Area Networks

– Reichweite 0,2 – 50m
– ad-hoc Netzwerke
– Anbindung Peripherie
– Vernetzung



http://anmc.postech.ac.kr

(W)PAN

USB 

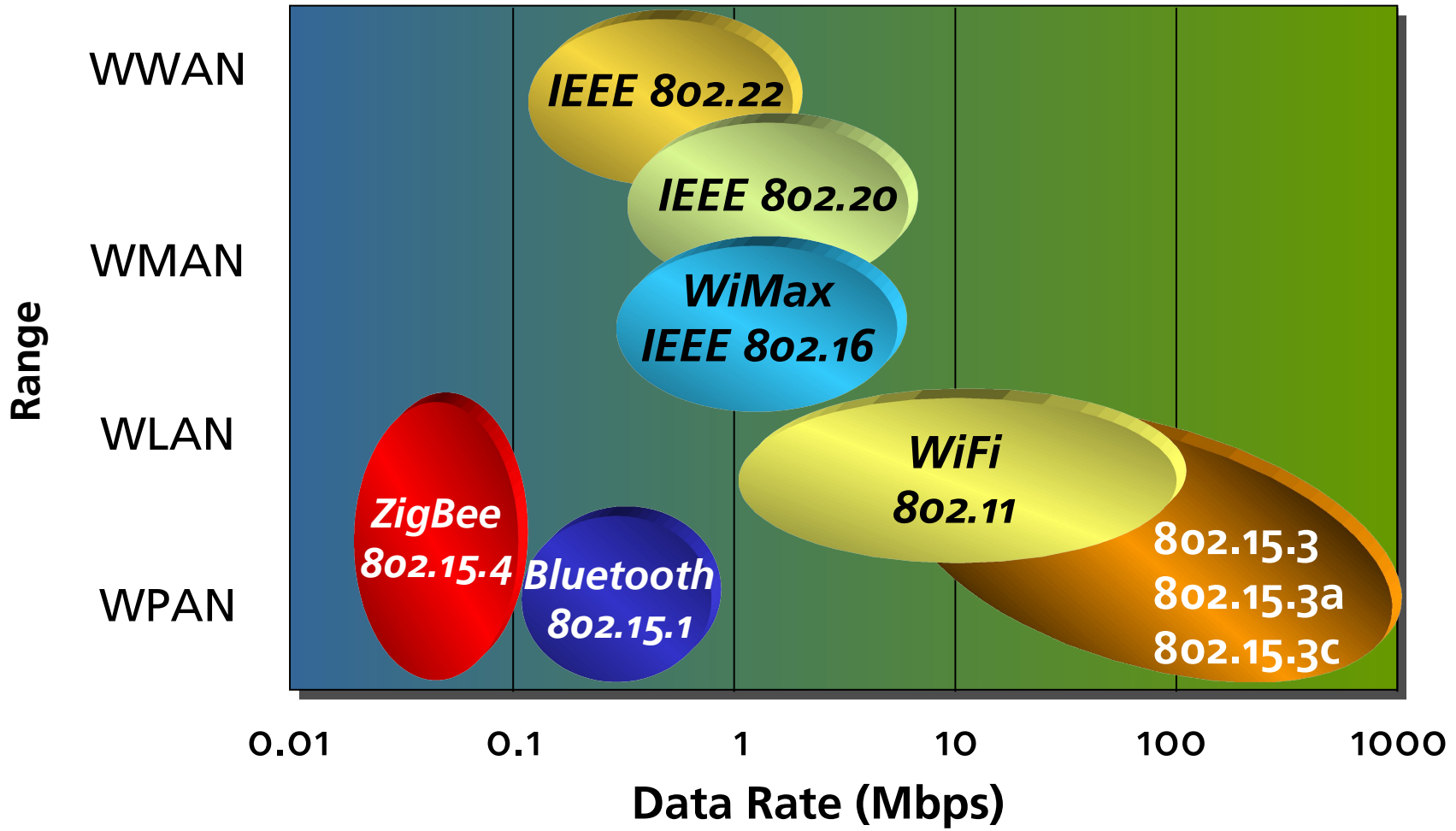
Wireless USB

Bluetooth

Firewire

ZigBee

Wireless PAN

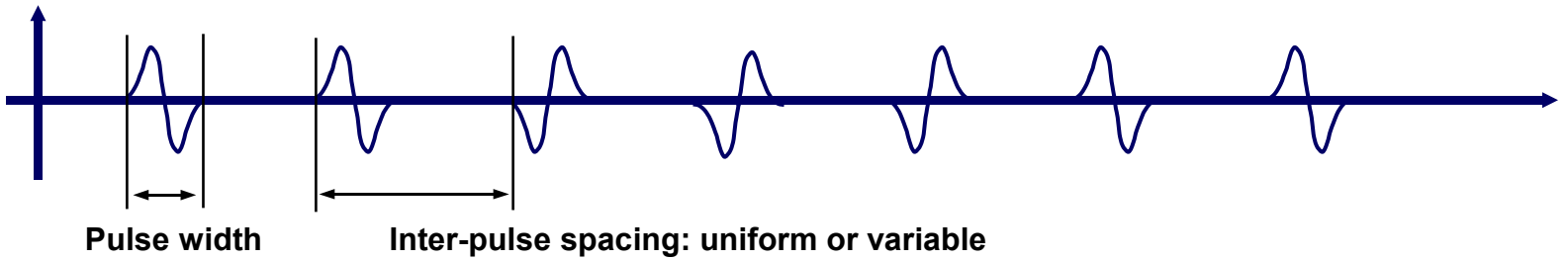


http://www.zigbee.org/en/resources/

Ultrabreitband

Ultrabreitband – Ultra-Wideband

„Als Ultra Wideband wird jede Funktechnik bezeichnet, die eine Bandbreite von mehr als ein Viertel ihrer Mittenfrequenz oder mehr als 500 MHz abdeckt.“

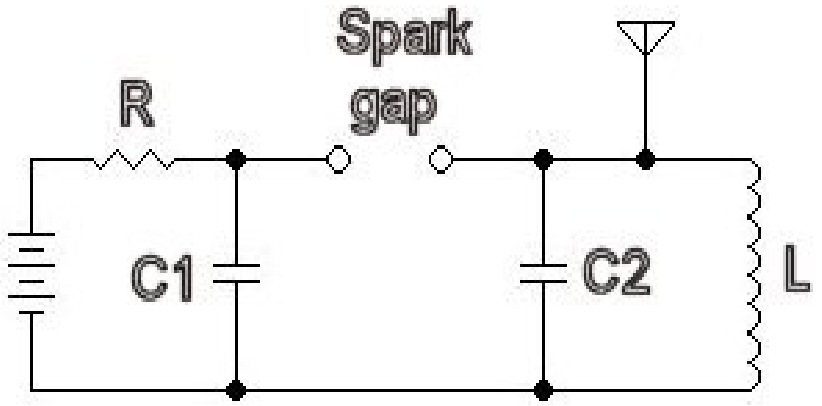


http://grouper.ieee.org/groups/802/15

Back to the roots

Funkenstrecke

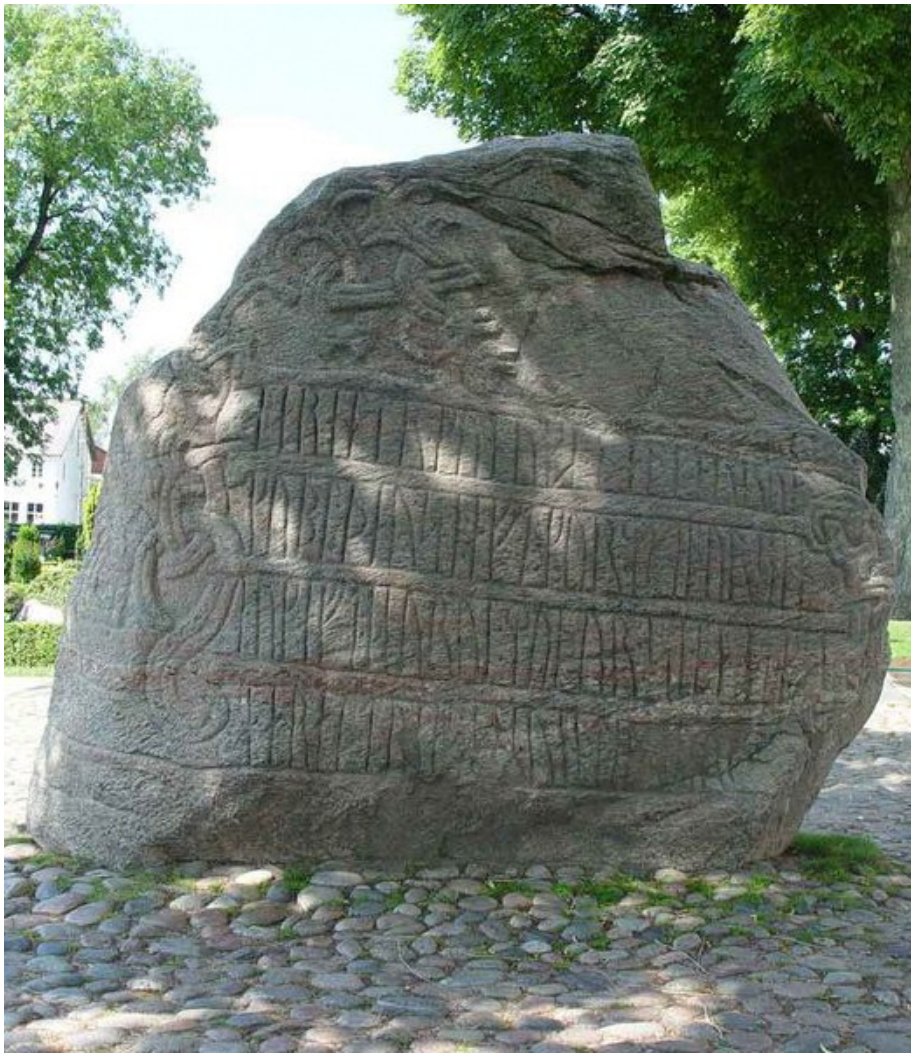
– Knallfunkensender
– Entdeckung 1886 von Heinrich Hertz
– Kommerzieller Erfolg von Marconi
– Radar



http://en.wikipedia.org/wiki/Spark-gap_transmitter

Bluetooth

- Harald I. Blauzahn Gormson (Harald Blåtand)
- 1994 Studie von Ericsson als Kabelersatz
- 1999 Bluetooth 1.0



http://de.wikipedia.org/wiki/Harald_Blauzahn

Bluetooth

Designziele

- Sprach und Datenunterstützung
- Ad-hoc-Konnektivität
- Interferenzresistenz
- weltweit nutzbar
- Sicherheit
- geringe Größe
- geringe Leistungsaufnahme

http://www.samsung.com

Bluetooth

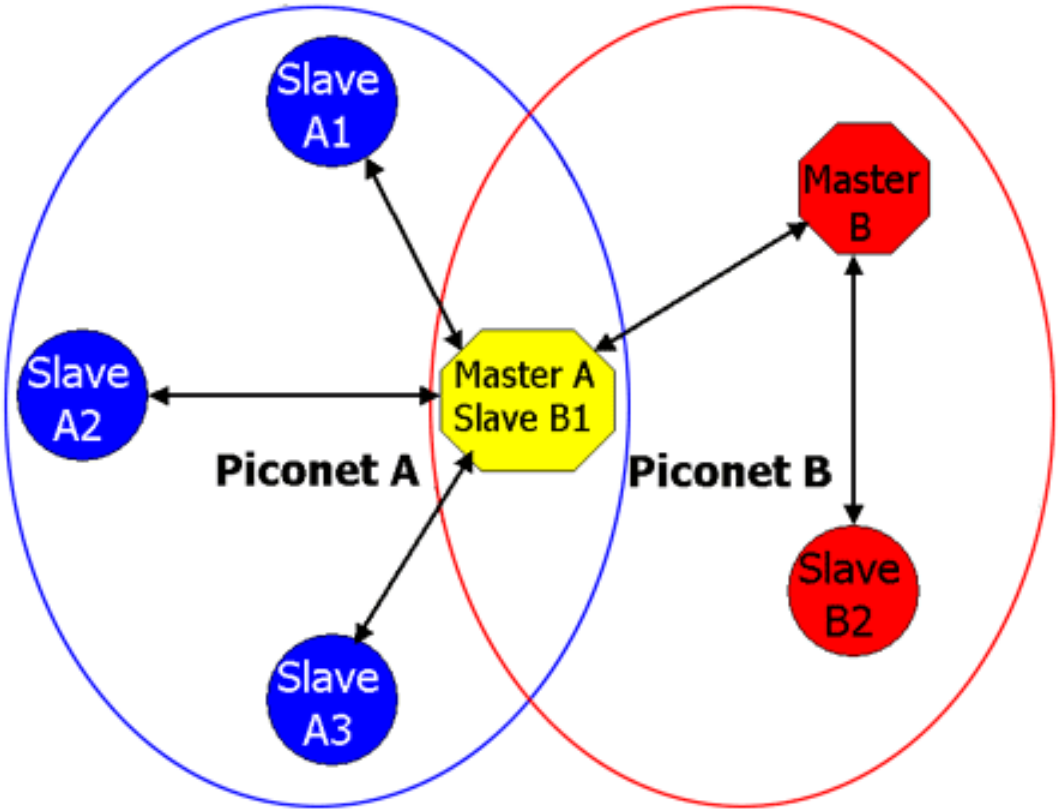
Technologie

- ISM-Band (2,402 - 2,480 Ghz)
- Kanalbreite: 1 Mhz
- Frequency hopping (79 Frequenzstufen, bis 1,6k Wechsel/s)
- FM – Gaussian Frequency Key Shifting
- TM – Time Division Duplex
- 3 Arten Fehlerkorrektur (1/3 FEC, 2/3 FEC, ARQ)

Bluetooth

Piconet vs. Scatternet

8 aktive Geräte – max. 10 Piconets



Bluetooth

Advanced

Verbindungsaufbau:

1. „inquiry“ zum finden
2. jeder kann antworten
3. Einigung über Profile & Kanäle
4. Authentifizierung (optional)

Profile: definiert angebotene Services & Befehle

Wireless USB

Auf dem Weg zu (einem) Standard

Direct Sequence Spread Spectrum

vs.

Multi-Band Orthogonal Frequency Division Multiplexing

ZigBee

Bienen und Blümchen

– laut ZigBee Alliance: Tanz der Honigbienen zur Kommunikation über Richtung und Entfernung von Futterquellen („ZigBee Principle“)

– laut Biologie: falsch!

http://mypage.bluewin.ch/a-z/yuno/Bilder/bienen.jpg

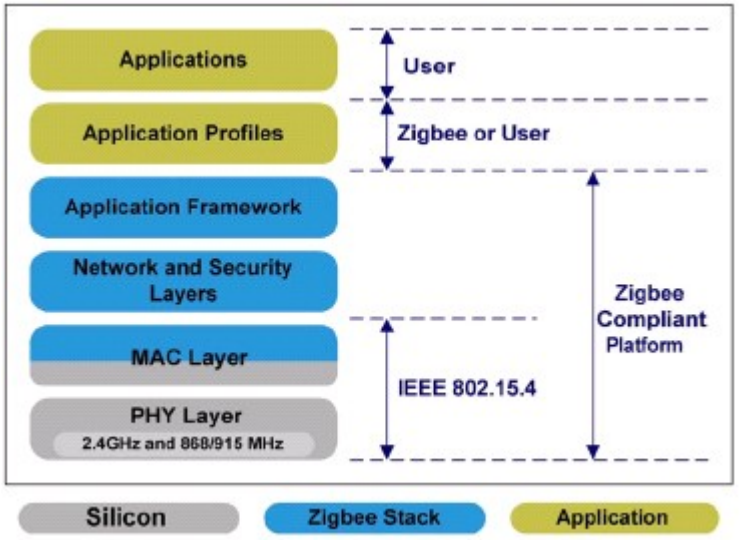
ZigBee

Anflug

1998: Beginn der Entwicklung

2003: IEEE 802.15.4 Standard (nur MAC und PHY)

2004: ZigBee-Spezifikation ratifiziert



http://www.eetimes.com/showArticle.jhtml?articleID=173600329

ZigBee

Designziele

– extrem niedriger Energieverbrauch

– einfacher und billiger als Bluetooth-Hardware

– selbstorganisierende Ad-Hoc-Netzwerke

– stabile und sichere Verbindungen

– geringe Reaktionszeiten

– hohe Bandbreite war kein Designziel

ZigBee

Technologie

- Frequenzbereich: 2,4 GHz (ISM)
- Kanäle: 16 mit je 5 MHz
- Sendeleistung: 1..10 mW
- Reichweite: max. 100 m
- Bandbreite: 20..250 kbit/s
- Direct-Sequence Spread Spectrum
- Carrier Sense Multiple Access / Collision Avoidance

ZigBee

Devices

– Reduced Function Device (RFD)

– Full Function Device (FFD)

Rollen

– ZigBee End Device (ZED): RFD oder FFD

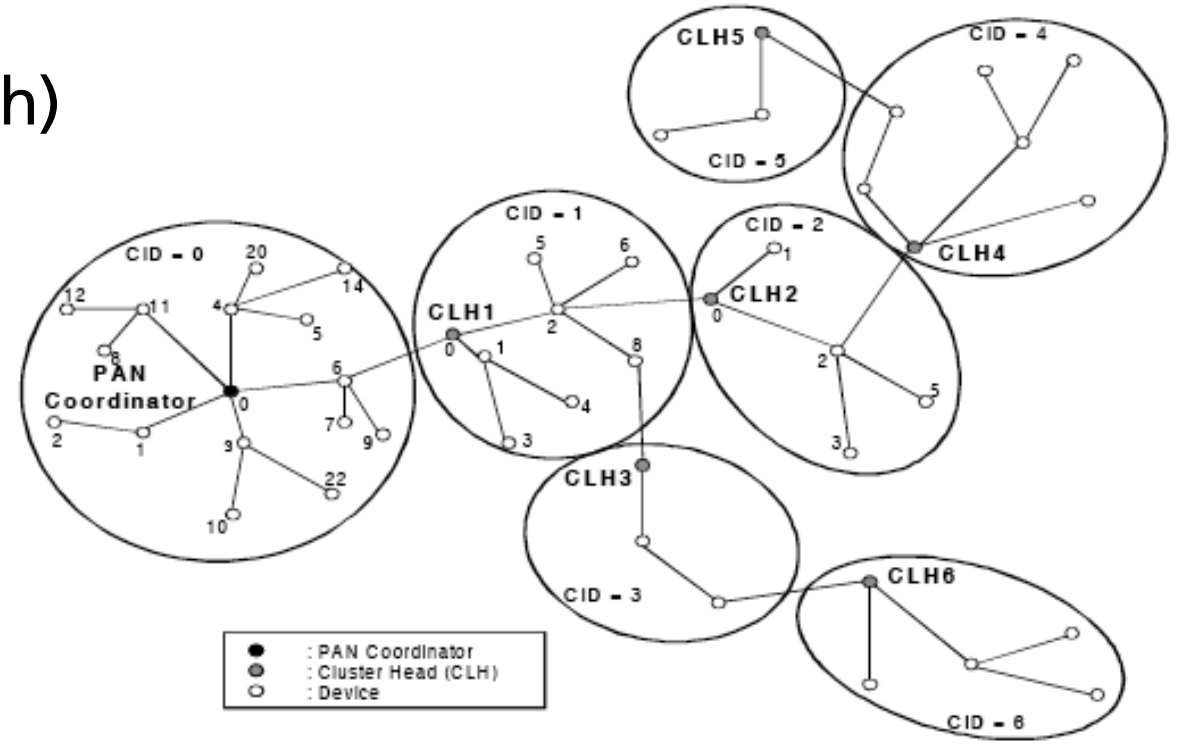
– ZigBee Router (ZR): FFD

– ZigBee Coordinator (ZC): FFD

ZigBee

Topologien

- Stern-Topologie
- P2P-Topologie (Mesh)
- Cluster Tree



http://www.nflora.dk/studie/wp-content/uploads/presentation.ppt

ZigBee

Adressierung

Adressierung eines Dienstes über Node und Endpoint (~ Port)

- lange Adresse: 64 Bit (8 Byte)
- kurze Adresse: 16 Bit (2 Byte)
- Dienst und Endpoint sind nicht fest verknüpft
- max. 255 Endpoints: 0 – Management, 241 – 254 RFU, 255 Broadcast

ZigBee

Protokolle

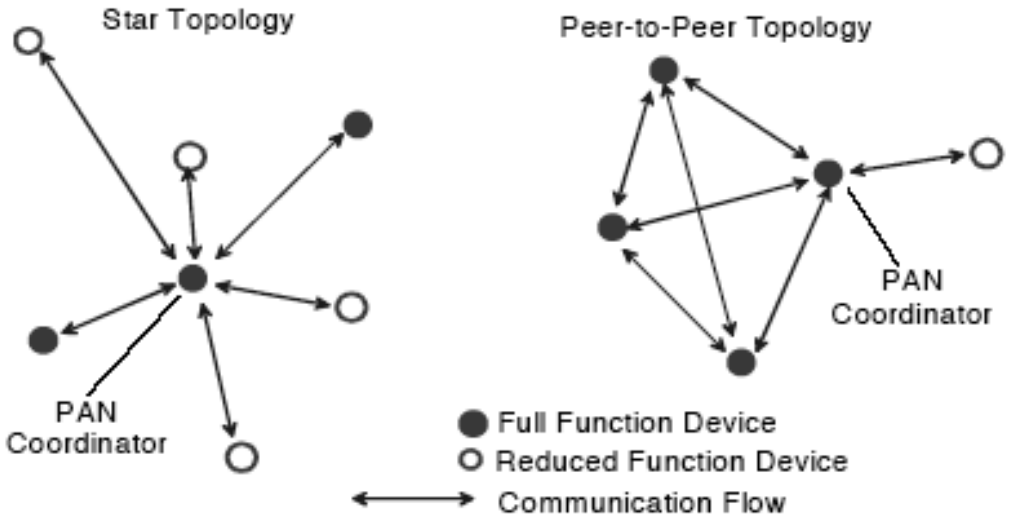
Zwei Übertragungsprotokolle: mit und ohne Beacon

- mit Beacon: komplexer Zeitschlitz („Superframe“) mit
    1. Beacon
    2. Contention Access Period (Daten mit CSMA/CA)
    3. Contention Free Period (Daten mit TDMA)
    4. Inactive Period (Coordinator hat zweiten Superframe)
- ohne Beacon: CSMA/CA

ZigBee

Personal Area Network

- Aufbau eines PAN
- Beitritt zu einem PAN
- Verwaiste Geräte
- PAN-Konflikte
- PAN Information Database (PIB)



http://www.nflora.dk/studie/wp-content/uploads/presentation.ppt

ZigBee

Sicherheit (laut Eigenwerbung)

- Access Control Lists
- Packet Freshness Timer
- 128-bit Verschlüsselung basierend auf AES

ZigBee

Kein Licht? – Denial of Service

– ein FFD lauscht nach der PAN-ID

– löst durch Senden mit dieser PAN-ID Konflikte aus

– theoretische Schwachstelle

Zeit abgelaufen? – Y2K-Problem

– Standard-Datentypen für Zeitangaben

– absolute Zeitangaben: sekundengenau für 2000 – 2187

– Zeitdauer: ms-genau für max. 49 Tage

Zusammenfassung

- WPAN wird immer wichtiger
- UWB: schnell, aber vielleicht Überlastung
- Bluetooth für Multimedia-Anwendungen
- Wireless USB wahrscheinlich zu spät
- ZigBee für kleine Geräte und kurze Entfernungen
- ZigBee mit Sicherheitsproblemen

Literatur

[de|en].wikipedia.org

www.zigbee.org

Jan Flora: 802.15.4 - An introduction

Khanh Tuan Le: ZigBee SoCs provide cost-effective solutions

Rui Silva, Serafim Nunes: Security Issues on ZigBee

Vielen Dank für Eure Aufmerksamkeit