EMES: Eigenschaften mobiler und eingebetteter Systeme

Drahtlose Kommunikation Teil 2

Dr. Siegmar Sommer, Dr. Peter Tröger

Wintersemester 2009/2010

Überblick

- Anwendungen
- Grundlagen
- Beschränkungen natürlicher und künstlicher Art
- Beispiele
  - IrDA
  - WLAN
  - Bluetooth
  - ZigBee
  - GSM
  - UMTS

Beispiele für drahtlose Kommunikation, Teil 2

- IrDA
- WLAN
- Bluetooth
- ZigBee

Gemeinsamkeiten:

- Räumlich sehr beschränkte Kommunikation
- Keine öffentliche Infrastruktur wird benutzt

Heute: Bluetooth und ZigBee

Teil A: Bluetooth

Motivation

- Ersatz von kabelgebundener Peripherie durch drahtlose Systeme
  Beseitigung des „Kabelsalates“
- Einfache Kommunikation über geringe Distanzen
- Uneingeschränkte Mobilität
  Szenarien:
  - Verbindung von Peripherie-Geräten
  - Adhoc-Networking
  - Verbindung verschiedener Netze

Entwicklungs-Ziele

- Implementation mit Single-Chip-Lösungen
- Benutzung global verfügbarer Frequenzen
- Übertragung von Sprache
- Übertragung von Daten
- Hoher Datendurchsatz
- Hohe Datensicherheit
- Eliminierung der Probleme von IrDA:
  - Interoperabilität
  - Netzwerkfähigkeit
  - Kommunikation ohne Sichtverbindung
- Kostengünstige Implementation auf Ebene von Hard- und Software
- Unterstützung der Anpassung existierender Anwendungen (Spezifikation einer seriellen Schnittstelle im Protokollstack)

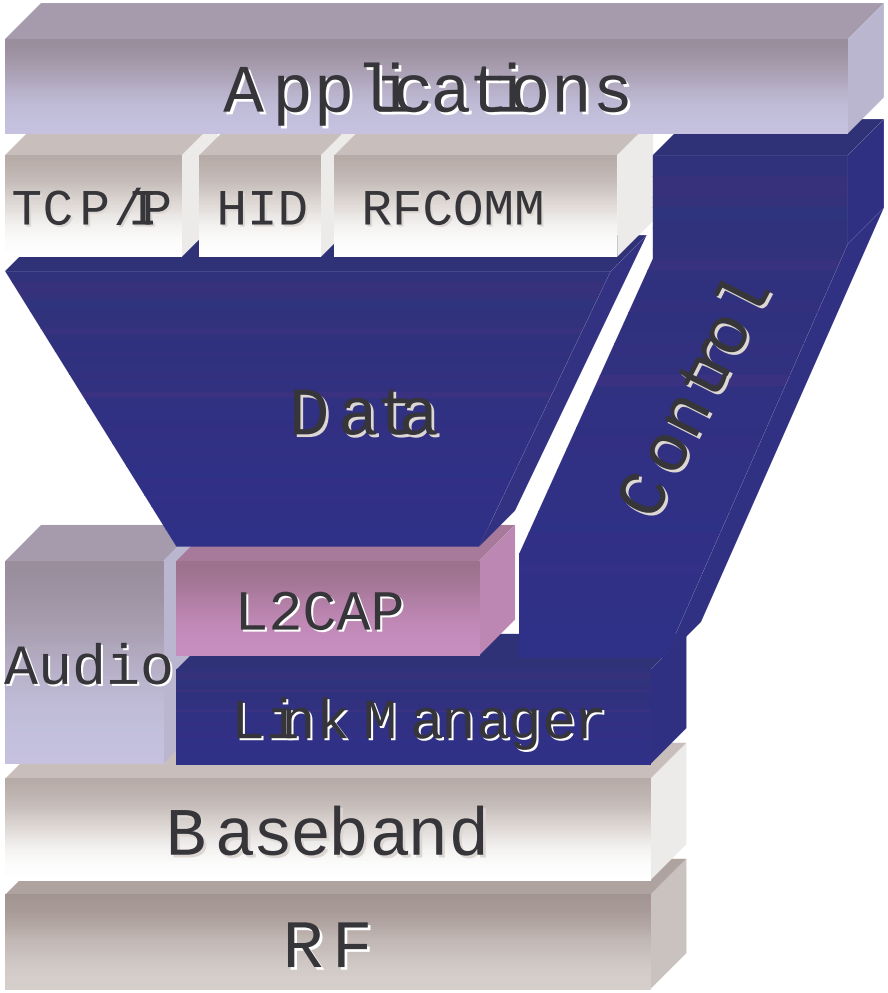
Entwicklungsgeschichte

- 1998:
  Ericsson startet Initiative zur Entwicklung einer drahtlosen Funktechnik für den Nahbereich
- 1999:
  Gründung einer SIG (special interest group) mit 3Com, Ericsson, IBM, Intel, Lucent, Microsoft, Motorola, Nokia und Toshiba
- 7/1999, 12/1999:
  Versionen 1.0A und 1.0B des Standards erscheinen
- 2000:
  2000 Mitglieder, erste Serienprodukte erscheinen
- 2/2001: Version 1.1 des Standards
- 11/2003: Version 1.2 des Standards
- 11/2004: Version 2.0 des Standards
- 8/2007: Version 2.1 des Standards

Bluetooth: Der Name

Der Name „Bluetooth“ wurde vom vom dänischen König Harald (genannt: Blauzahn) übernommen, der Teile Skandinaviens christianisierte und in seinem Königreich vereinte.

Bluetooth: Protokollstack I



Bluetooth: Protokollstack II

- Deckt alle OSI-Schichten ab
- Folgt dabei aber in der Einteilung nicht vollständig dem OSI-Modell
- Beschreibt
  - Hardware
  - Anwendungen
- Standardisiert als IEEE 802.15.1
- Hier: Bluetooth 1.1 (IEEE 802.15.1-2002)

Bluetooth: Protokollstack III

Logische Unterteilung des Protokollstacks:

- Transportprotokolle (Linkmanagement und tiefer)
  - Aufbau und Betrieb von physikalischen und logischen Verbindungen
- Middleware-Protokolle
  - Service Discovery (SDP)
  - Emulation der seriellen Schnittstelle (RFCCOMM)
  - Darauf aufbauende Protokolle (z.B. IP)
- Anwendungsebene
  - Anwendungen, die Bluetooth gekapselt benutzen
  - Anwendungen, die Bluetooth „native“ benutzen

Bluetooth: Funk I

- Frequenzband 2.4-2.5 GHz
  - ISM-Band
  - fast überall verfügbar

    Anpassung an abweichende Reglungen durch angepaßtes Frequency-Hopping
- 79 Kanäle mit Trägerabstand 1 MHz
- FHSS (frequency hopping spread spectrum)
  - 1600 Hops pro Sekunde
  - Zeitschlitze von 625 μs
- Bitrate: 1MBit/s
- Modulationsverfahren G-FSK (gaussian frequency shift keying)
  - 1 repräsentiert durch positive Frequenzabweichung
  - 0 repräsentiert durch negative Frequenzabweichung

Bluetooth: Funk II

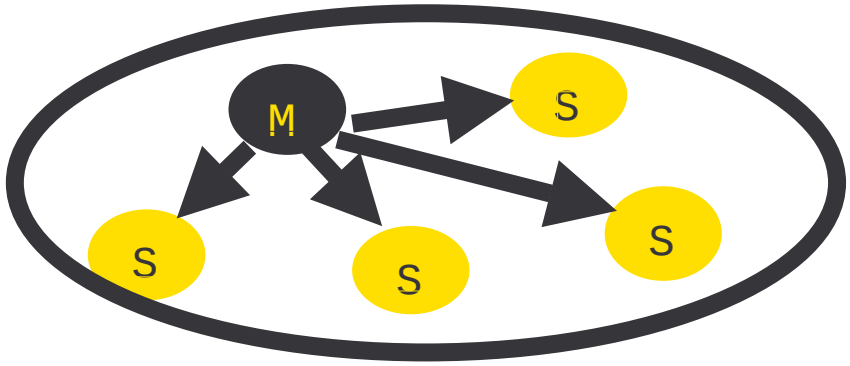
- Sendeleistung 0 dBm bis 20 dBm:
  - Klasse 1: 1 mW . . . 100 mW
  - Klasse 2: 0.25 mW . . . 1 mW . . . 2.5 mW
  - Klasse 3: 1 mW
- Je nach Klasse Power Control optional oder obligatorisch
  - Anpassung der Sendeleistung an tatsächliche Erfordernisse
  - Reduktion der Störstrahlung
  - Energieeinsparung bei mobilen Geräten

Bluetooth: Netzwerktopologien I

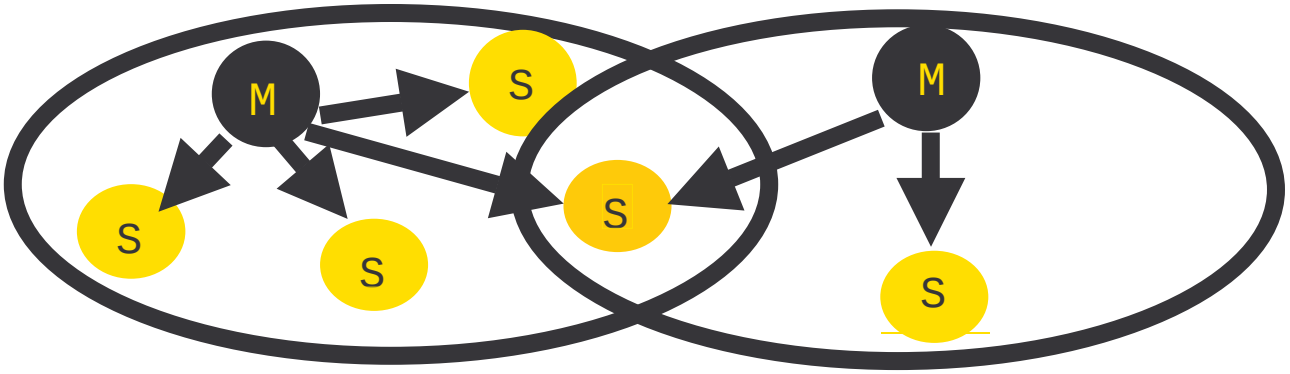
- Punkt zu Punkt
- Punkt zu Multipunkt
- Piconet
  - 7 aktive Teilnehmer (und ein Master)
  - 255 passive Teilnehmer (und ein Master)
- Scatternet
  - Verknüpfung mehrerer Piconets
  - Weiterleitung, Routing
  - Master kann Slave in anderem Piconet sein

Bluetooth: Netzwerktopologien II

- Piconet

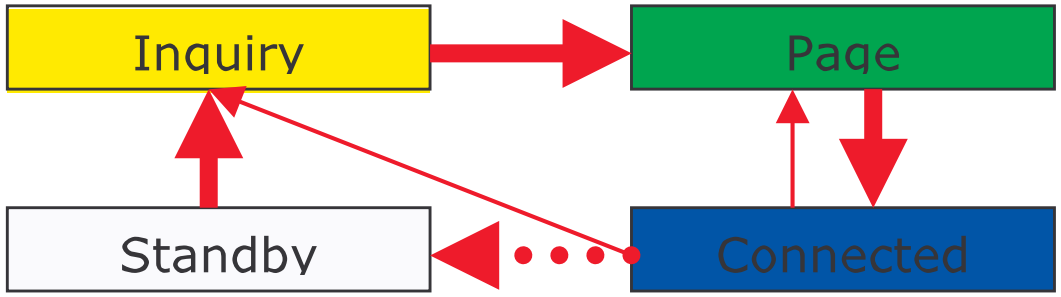


- Scatternet



Bluetooth: Verbindungsaufbau bei P2P I

- Auf Transportebene Kommunikation als Master/Slave
- Jedes Gerät kann Master oder Slave sein
- Modi:



- Standby Mode
  - Keine Kommunikation
  - Einsparung von Energie

Bluetooth: Verbindungsaufbau bei P2P II

- Inquiry Mode
  - Master sendet auf einer definierten Frequenz-Sequenz Signale im 3.12μs Muster
  - Wartet auf Rueckmeldung
  - Slave scannt gleiche Frequenzfolge im 1.28μs Muster
  - Durch unterschiedliche Hoppingfrequenzen findet Treffen mit hoher Wahrscheinlichkeit in kurzer Zeit statt
  - Slave sendet Informationen über seine Systemtaktung
  - Synchronisation des Channelhops
  - Wechsel nach Page-Mode

Bluetooth: Verbindungsaufbau bei P2P III

- Page Mode
  - Errechnung einer Sprungsequenz in Abhängigkeit von der eindeutigen Gerätenummer des Masters
  - Wechsel nach Connected Mode
- Connected Mode
  - Synchrones Frequency-Hopping nach vereinbartem Muster
  - Master kommuniziert mit Slave über Polling

Bluetooth: Verbindungsaufbau in Piconets

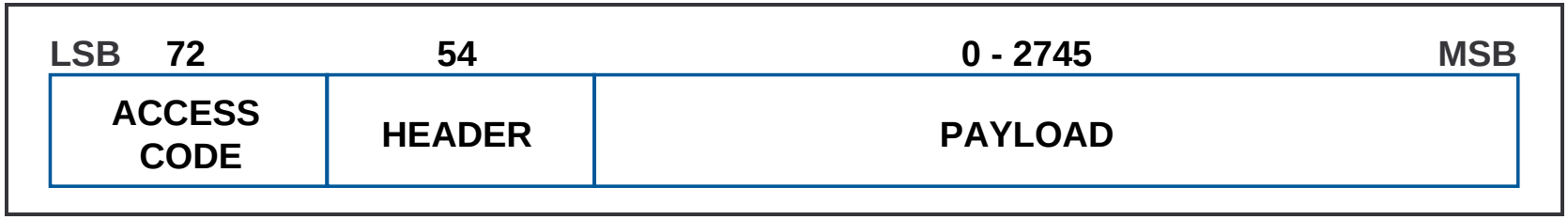
- Kommunikation durch Polling läßt dem Master freie Timeslots
- Parallele Kommunikation mit weiteren Slaves
- Zyklisches Polling von bis zu 7 Slaves
- Bis zu 255 „geparkte“ Slaves
  - Verbindung wird nur bei Bedarf aktiviert
- Kommunikation untereinander im Piconet nur über den Master
- Scatternet
  - Zyklischer Netzwechsel eines Knotens
  - Brückenfunktion zwischen zwei Piconets

Bluetooth: Physical Link Layer

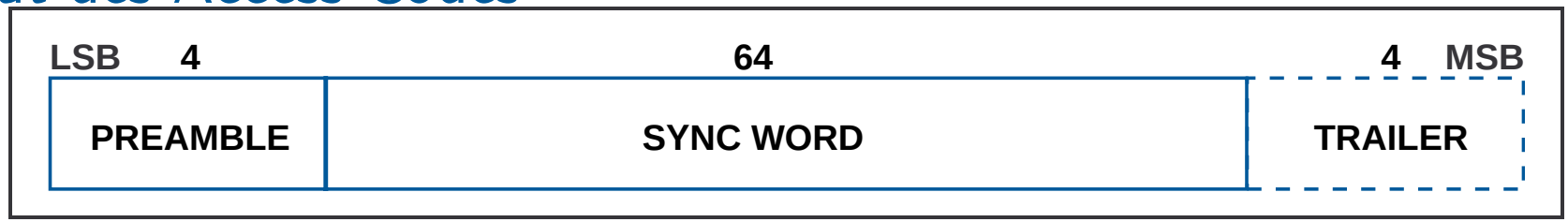
- Sprachverbindung
  SCO (synchronous connection oriented)
  - synchron
  - Datenrate: 64 KBit/s
  - leitungsvermittelt
  - Reservierung von Übertragungsslots in festen Intervallen
- Datenübertragung
  ACL (asynchronous connection less)
  - asynchron
  - Datenraten:
    * 432 KBit/s symmetrisch
    * 751/57 KBit/s asymmetrisch
  - paketvermittelt

Bluetooth: Paketformate

Paketformat:



Format des Access-Codes



- Access-Code Typen:
  - Channel Access Code (CAC)
  - Device Access Code (DAC)
  - Inquiry Access Code (IAC)

Bluetooth: Middleware-Ebene I

L2CAP: Logical Link Control and Adaption Protocol

- Segmentierung und Desegmentierung von Paketen höherer Schichten
- Multiplexing von Protokollen und Datenströmen
- Logische Kanäle zwischen L2CAP-Endpunkten
- Abstraktion der Master/Slave-Kommunikation
- Bietet Peer-to-Peer-Kommunikation

Bluetooth: Middleware-Ebene II

Beispiel: RFCOMM

- Soll Portierung existierender Anwendungen durch Emulation eines seriellen Ports erleichtern
- Basiert auf ETSI TS 01.00 Standard für serielle Kommunikation
- Erstes Protokoll, das implementiert wurde
- Bietet Signalkompatibilität zu RS232
- Multiplexing von bis zu 60 seriellen Ports

Bluetooth: Anwendungsebene

- Standard definiert Anwendungsprofile
- Standard definiert keine Schnittstellen
- Profile geben vor, wie Bluetooth-Protokollstack benutzt wird
- Stellt Interoperabilität sicher

Bluetooth: Dienste I

- Beim Verbindungsaufbau werden verwendete Dienste vereinbart
- Dienste werden über Profile definiert
- Beispiel: Generic Access Profile
  - Service Discovery Profile
  - TCS-BIN based Profiles
    - Cordless Phone Profile
    - Intercom Profile
  - Serial Port Profile
    - Dial-Up Networking
    - Fax Profile
    - Headset Profile
    - LAN Access Profile
    - Generic Object Exchange Profile
      - File Transfer Profile, Synchronization Profile

Bluetooth: Dienste II

Beispiel: Service Discovery Protocol (SDP)

- Ermöglicht das dynamische Erkennen von Diensten
- Informationen über Dienste
- Eindeutige Bezeichner (UUID) für Dienste
  - Informationen über die Klasse des Dienstes
  - Spezifische Attribute
- Möglichkeiten:
  - Service Browsing: Suche nach Diensten einer Klasse und anschliessende Auswahl
  - Direkte Nachfrage nach einem bestimmten Dienst

Bluetooth: Sicherheit

- Sicherheitsfunktionen im Link-Layer
  - Identifikation von Benutzern über 128 Bit PIN (personal identification number)
  - Verschlüsselung
- Challenge/Response-Verfahren zur Identifikation
- Verschlüsselung mit Session-Keys
  - Public/Private Key
  - konfigurierbare Schlüssellänge (bis 128 Bit)
- Flexible Verfahren
  - Ermöglichen Adaption an nationale Einschränkungen
- Speicherung von Schlüsselpaaren häufig benutzter Gerätepaarungen

Bluetooth: Weiterentwicklungen

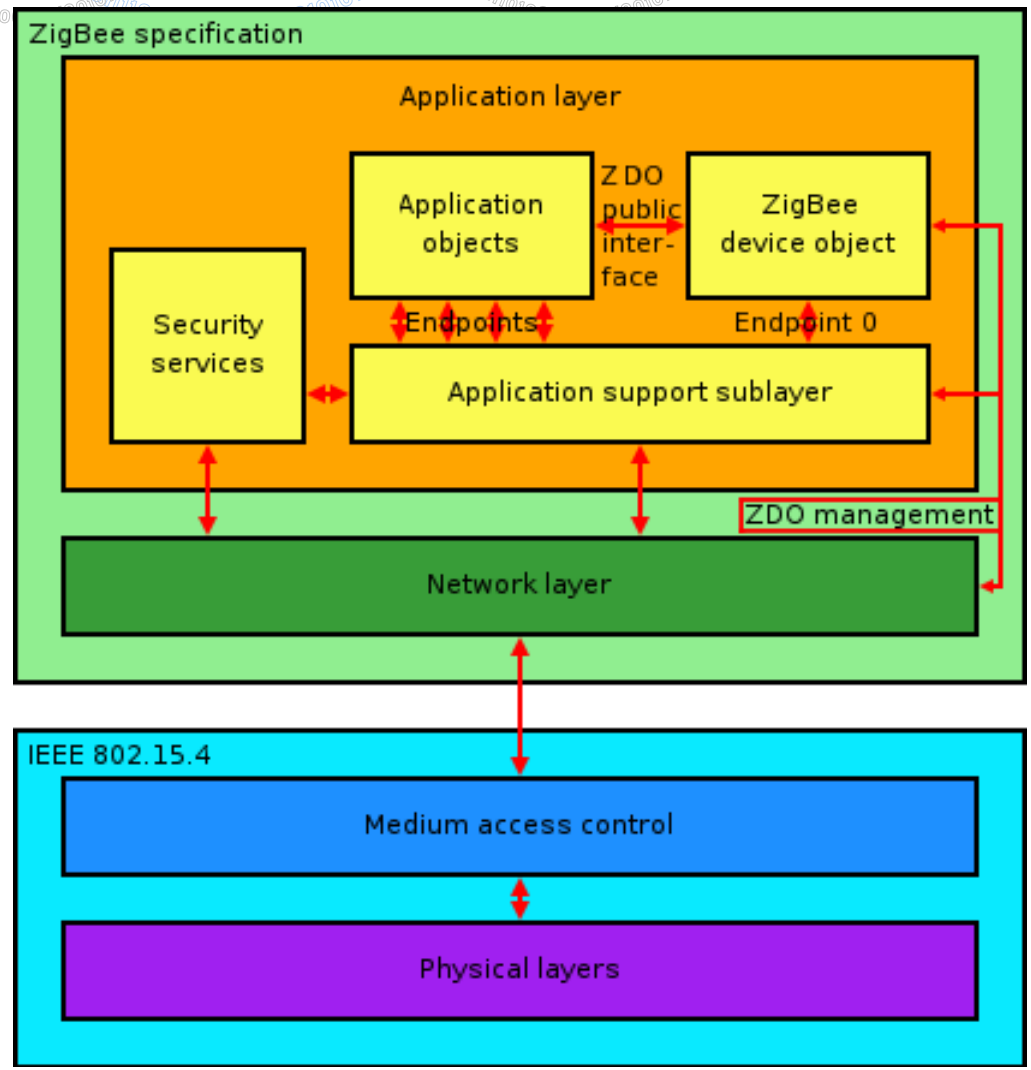
- Bluetooth 1.2
  - Schnellerer Verbindungsaufbau
  - Adaptives Frequenzhopping (Interferenzvermeidung)
  - Höhere praktisch erreichbare Übertragungsraten
- Bluetooth 2.0
  - Höhere Bitrate (bis 2,1 MBit/s)
  - Geringerer Energieverbrauch
- Bluetooth 2.1
  - Bessere Filterung beim Inquiry
  - Stärkere Verschlüsselung
  - Einfaches und sicheres Pairing
  - Automatischer (sicherer) Verbindungsaufbau im extremen Nahbereich

Teil B: ZigBee

ZigBee: Überblick

- PAN (personal area network) mit
  - niedrigem Energieverbrauch
  - niedrigen Kosten
- Vorgesehen als Baustein für “allgegenwärtige Netze”
- Verwaltet von der ZigBee Alliance
- Beschreibt höhere Protokollebenen auf Basis der physikalischen Ebene und der Medienzugangssteuerung von IEEE 802.15.4
- Ergänzt IEEE 802.15.4 um
  - Netzwerkschicht
  - Anwendungsebene
- Name abgeleitet von zickzackförmigen Tanz der Honigbienen zur Weitergabe von Informationen

Protokollstack



Quelle: Wikimedia Commons

Physikalische Schicht

- Medium Funk:
  - 868-868.8 MHz: Europa, genutzt als ein Kommunikationskanal, 2006 auf drei erweitert
  - 902-928 MHz: Nordamerika, zehn Kanäle, erweitert auf dreißig
  - 2400-2483.5 MHz: weltweit (ISM-Band), bis zu 16 Kanäle
- Version von 2003: Direct Sequence Spread Spectrum (DSSS)
  - 20 und 40 KBit/s im Band um 900 MHz
  - 250 KBit/s im ISM-Band
- Version von 2006: Vier neue Modulationsmethoden mit 100/250 KBit/s im Band um 900 MHz

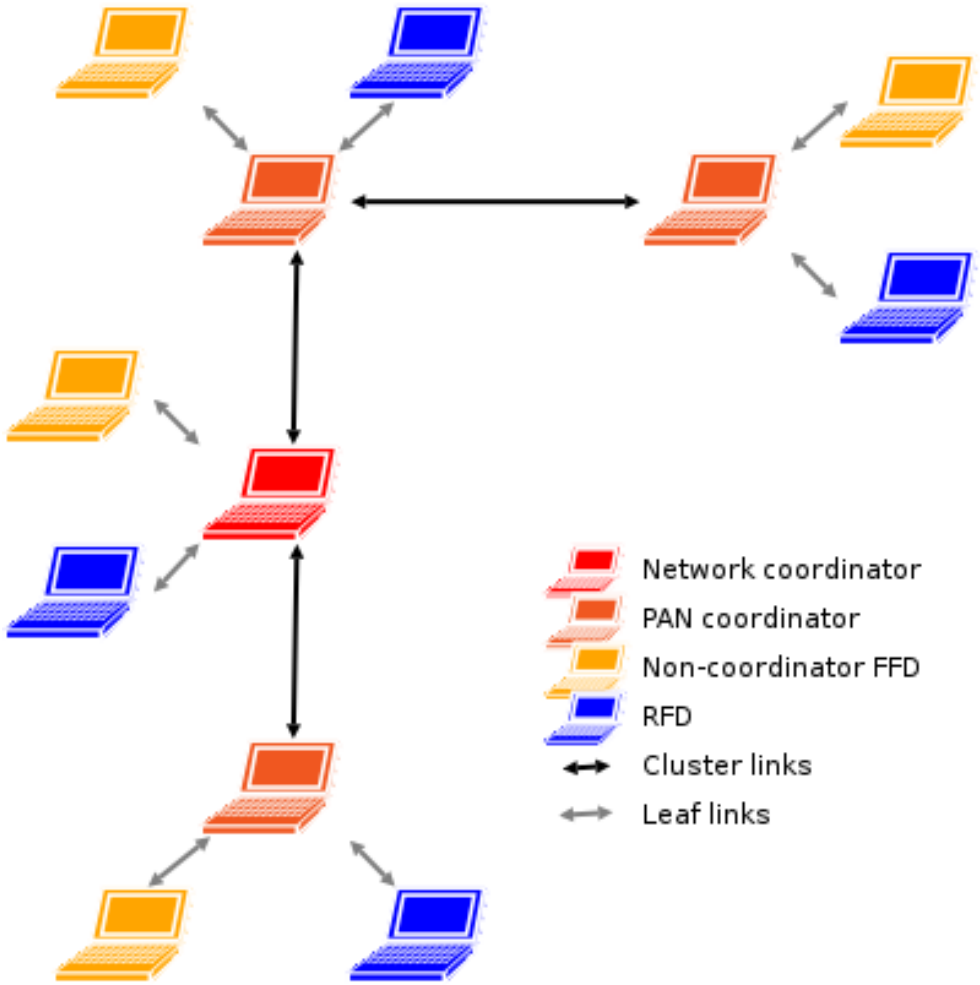
Mediumzugangssteuerung (MAC)

- Erlaubt die Übertragung von MAC-Frames über physikalische Kanäle
- Verwaltung von Knoten entsprechend des Netzwerkmodells
- Zugriffssteuerung:
  - Koordinierter Betrieb
    - Superframes des Koordinators regeln Zugriff
    - Vergabe von garantierten Zeitschlitzen für zeitkritische Anwendungen
    - Kommunikation nur über Koordinator
  - Punkt-zu-Punkt-Betrieb
    - CSMA/CA und Synchronisationsmechanismen
    - Kommunikation zwischen beliebigen Geräten möglich

Netzwerkmodell (1)

- Zwei Knotentypen:
  - Full Function Device (FFD)
    - kann als PAN-Koordinator arbeiten
    - kann mit jedem anderen Knoten kommunizieren
    - kann Nachrichten weiterleiten (wenn Koordinator)
  - Reduced Function Device (RFD)
    - sehr einfache Geräte
    - kann nur mit FFDs kommunizieren
    - kann nicht als PAN-Koordinator verwendet werden
- Mindestens ein FFD als Koordinator pro PAN
- Geräte haben 64 Bit Identifier
- Innerhalb eines PAN können 16 Bit Identifier genutzt werden
- Topologie: Stern oder Peer-to-Peer (beliebige Verbindungen, Aufbau eines Mesh-Netzes, Adhoc-Kommunikation)

Netzwerkmodell (2)



Quelle: Wikimedia Commons

Netzwerkschicht

- IEEE 802.15.4 behandelt Netzwerkschicht nicht, darum auch kein Routing im Standard
- Teil der ZigBee-Spezifikation
- Behandelt:
  - Routing anhand der vorliegenden Topologie
  - Konfiguration von Geräten
  - Aufbau neuer Netzwerke durch Erkennung neuer Geräte und Router
  - Ermöglicht direkte Kommunikation und MAC-Synchronisation

Anwendungsschicht

- ZigBee Device Object (ZDO)
  - Verwaltet MAC-Rolle eines Gerätes
  - Erkennung von angebotenen Diensten anderer Geräte
  - Baut Verbindungen zu anderen Geräten auf und antwortet auf eingehende Verbindungsanfragen
- Application Support Sublayer (APS)
  - Bietet Schnittstelle für Dienste
  - Verwaltet Tabellen mit Diensten zur Suche nach Geräten mit bestimmten Diensten
  - Routing von Nachrichten
- Adressierung: IEEE 802.15.4 Adresse + endpoint identifier (0-255, wobei 1-240 Anwendungsobjekte sind)

Kommunikation und Anwendungen

- Netzwerk besteht aus kommunizierenden Anwendungsobjekten (bis zu 240 pro Gerät)
- Benutzbare Dienste:
  - Key/Value pair service: Konfiguration (komprimiertes XML)
  - Message service: Transport beliebiger Nutzdaten über APS-Frames
- Profile definieren Kommunikationskonventionen
- Geräteauffindung über 802.15.4-Adressen oder Broadcast von "Petitionen"
- Gezielte Suche nach Diensten ist möglich
- Kommunikation direkt, über den Koordinator oder über Multicasts an Gruppen

Sicherheit

- Basiert auf Sicherheitsframework von IEEE 802.15.4
- Verschlüsselung der Kommunikation mit 128 Bit Schlüsseln
- Schlüssel sind dem Netzwerk oder einem Link zugewiesen
- Infrastruktur für Schlüsselmanagement auf Basis eines Trustcenters (ausgewähltes Gerät pro Netzwerk)
- Initiale Schlüssel sind entweder bekannt oder werden (unsicher) vom Trustcenter übertragen
- Weiterer Nachrichtenaustausch ist nur mit gültigem Schlüssel möglich