Bluetooth

Hauptseminar
Dienste & Infrastrukturen mobiler Systeme

Sandra Hagen & Christian Wöck

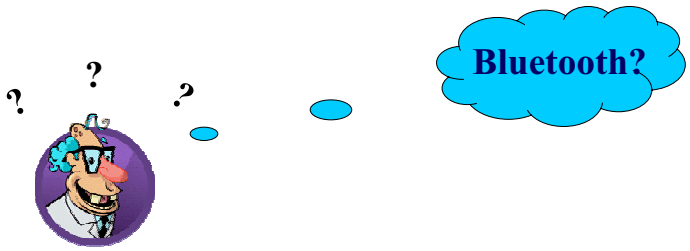
Überblick

Bluetooth

Was ist Bluetooth?

Bluetooth

- Lizenzfreier Funkstandard für drahtlose Sprach- und Datenkommunikation über kurze Strecken
- SIG (Special Interest Group) Mai 1998 von Nokia, Ericsson, Intel, IBM, Toshiba gegründet
- Namensgeber: Harald Blatand (engl. Bluetooth) Wikinger-König, der Norwegen und Dänemark vereinte



Anwendungsbereiche

Bluetooth

- **Kabelersatz für Drucker, Tastatur, Maus, Fax, Scanner.....**
- **Datensynchronisation zwischen PDA und Mobiltelefon oder PC**
- **Headsets ermöglichen handfreies Telefonieren**
- **PC als Bluetooth-Zentrale mittels USB-Adapter**
- **Fernsteuerung von Haushaltsgeräten (TV, Kühlschrank,....)**
- **Übertragung der Stuhlgang-Messwerte intelligenter Toiletten auf den PDA des Benutzers (Japan)**

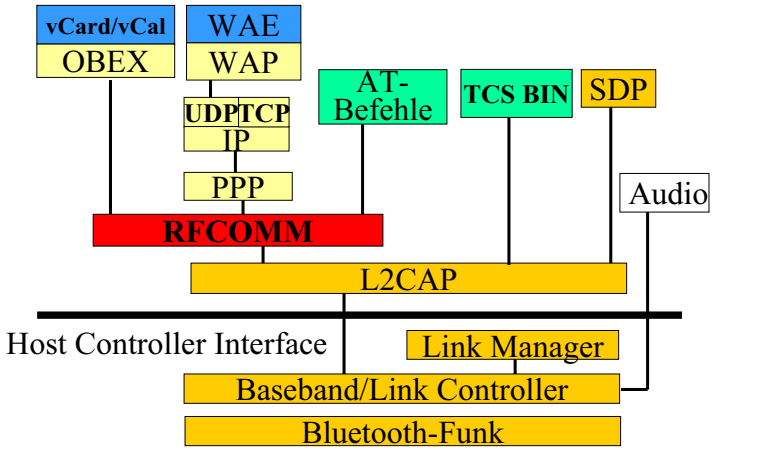
Anwendungsszenario

Bluetooth

1.Einleitung

Protokollarchitektur

Bluetooth



Kernprotokolle

Kabelersatzprotokoll

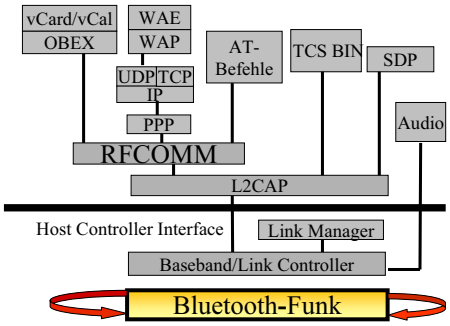
Telefonieprotokolle

Adaptierte Protokolle

Bluetooth-Funk

Bluetooth

- Physikalische Schnittstelle
- 2,4 GHz ISM-Band, lizenzfrei
- Modulation GFSK
- Übertragungsrate max. 1 Mbit/s
- Funkreichweite abhängig von der Sendeleistungsklasse:
  - 100 mW → 100 m (Klasse 1)
  - 2,5 mW → 20 m (Klasse 2)
  - 1 mW → 10 m (Klasse 3)

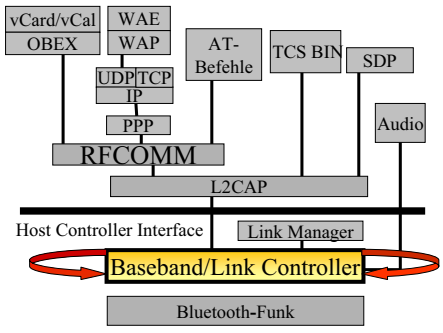


Physikalische Schnittstelle

Baseband / Link Controller

Bluetooth

- ✓ Datentransfer
- ✓ Adressierung
- ✓ Festlegung der Sprungsequenz
- ✓ Fehlerkorrektur
- ✓ Steuerung der physikalischen Funkverbindung
- ✓ Authentifizierung und Verschlüsselung



Physikalische Ebene des Stacks

Frequency Hopping

Bluetooth

Geschichtlicher Hintergrund

- **Hedy Lamarr (Schauspielerin)**
- **Erfinderin des Frequenzsprung-verfahrens während des zweiten Weltkrieges**
- **Wie verhindert man feindliche Störungen des Steuerungssignals von Torpedos?**

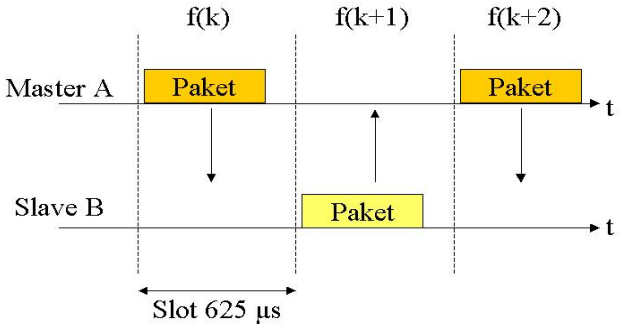
Hedy Lamarr

- **Idee: Signal über mehrere zufällig ausgewählte Frequenzen zu verteilen**

Frequency Hopping

Bluetooth

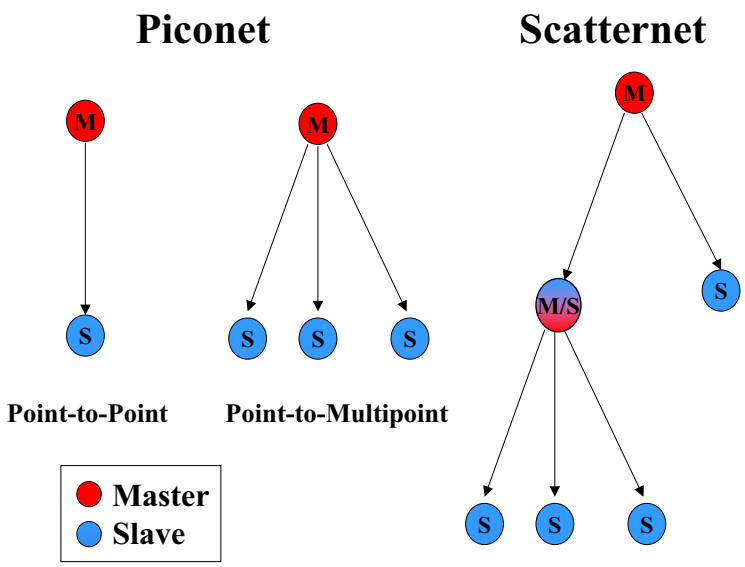
FH / TDD Schema



- **FHSS / TDD**
- **Zeitschlitzgröße 625 µs**
- **Aufteilung in 79 Kanäle (23 in Frankreich) mit jeweils 1MHz Breite**
- **1600 hops/s**

Netzwerktopologien

Bluetooth



Physikalische Verbindungen

Bluetooth

SCO: Synchronous Connection-Oriented Link

- Synchron, verbindungsorientiert, leitungsvermittelnd
- Punkt-zu-Punkt-Verbindung
- Bis zu 3 SCO-Links gleichzeitig (Master → Slave)
- Sprache
- Slotreservierung
- Paketgröße bis zu 64 kbit/s

Physikalische Verbindungen

Bluetooth

ACL: Asynchronous Connection-Less Link

- asynchron, verbindungslos, paketorientiert
- Punkt-zu-Mehrpunkt-Verbindung
- bis zu 7 ACL-Links pro Piconet (Master ⟹ Slave)
- Daten
- Keine Slotreservierung
- Datenrate der ACL-Pakete

Physikalische Verbindungen

Bluetooth

Typ	Symmetrisch	Asymmetrisch	
DM1	108,8 kbit/s	108,8 kbit/s	108,8 kbit/s
DH1	172,8 kbit/s	172,8 kbit/s	172,8 kbit/s
DM3	256 kbit/s	387,2 kbit/s	54,4 kbit/s
DH3	384 kbit/s	585,6 kbit/s	86,4 kbit/s
DM5	286,7 kbit/s	477,8 kbit/s	36,3 kbit/s
DH5	432,6 kbit/s	723,2 kbit/s	57,6 kbit/s

- Maximaler Datendurchsatz
  - 432,6 kbit/s Symmetrisch
  - 723,2 kbit/s ⟺ 57,6 kbit/s Asymmetrisch

Paket-Struktur

Bluetooth

Standard-Paket-Format

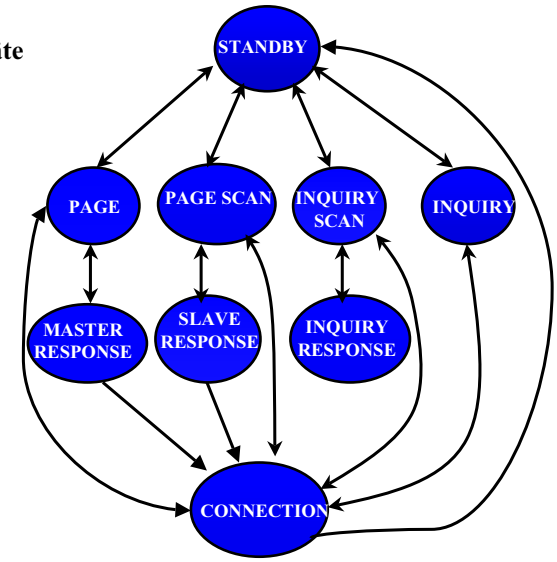
Access Code 72 Bit	Header 54 Bit	Payload 0-2745 Bit

- **Access Code** - Synchronisation und Identifikation
- **Header** - enthält Link-Steuerinformationen
  - 1/3 FEC (Forward Error Correction) ⇒ 54 Bit (eigentliche Größe von 18 Bit)
- **Payload** - enthält SCO-Sprachpakete oder ACL-Datenpakete

Link Controller

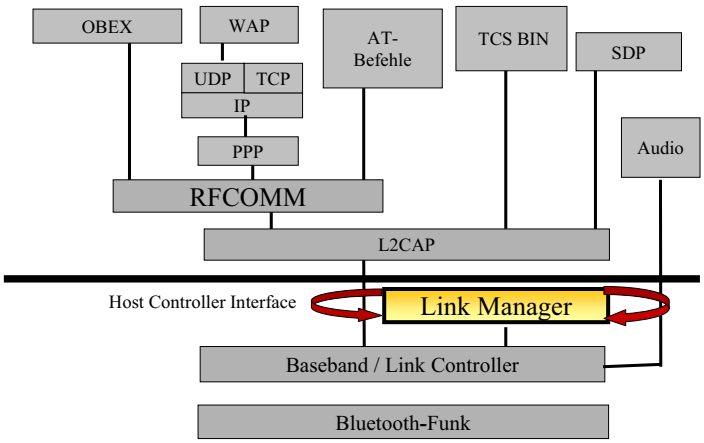
Bluetooth

- **Erkennung neuer Geräte**
- **Koordination des Verbindungsaufbaus**
- **Hauptzustände**
  - Standby
  - Connection
- **7 Subzustände für den Verbindungsaufbau zu einem neuen Slave**



Link Manager

Bluetooth



Link Manager

Bluetooth

- ✓ Auf- und Abbau von Verbindungen
- ✓ Wechsel der Master/Slave Rolle
- ✓ Sicherheit
- ✓ Energiesparzustände
  - Park - passiv (bis zu 255 Slaves), Synchronisation bleibt erhalten
  - Hold - keine Datenübertragung, Kommunikation erst nach Ablauf einer Zeitspanne möglich
  - Sniff - hört in regelmäßigen Zeitabständen das Netz ab

Link Manager

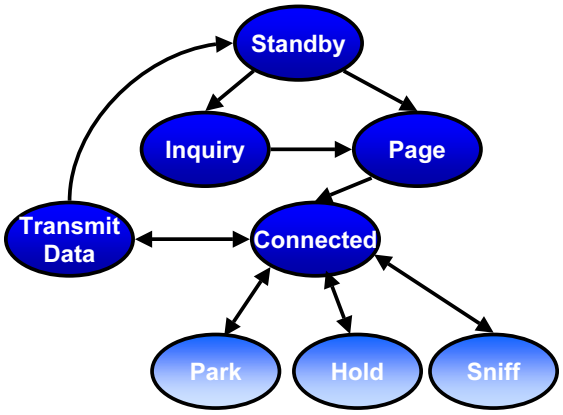
Bluetooth

Unconnected

Connecting

Active

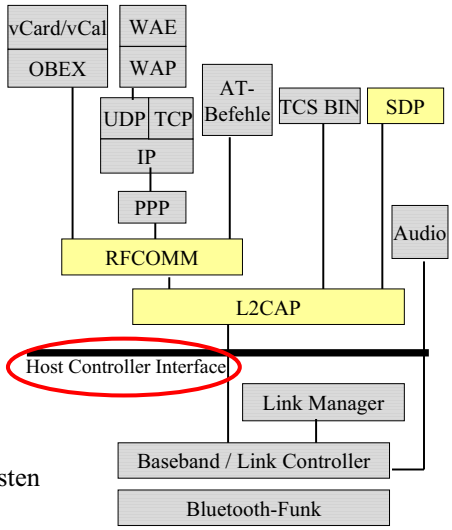
Low Power



HCI und die oberen Protokolle

Bluetooth

- **Host Controller Interface**
  - Befehlsschnittstelle zwischen Bluetooth-Modul und Host
- **L2CAP**
  - Verbindung oberer Schichten mit dem Baseband
  - Segmentierung/Reassemblierung
- **RFCOMM**
  - Emulation des seriellen RS232-Anschlusses über L2CAP
- **SDP**
  - Auffinden von verfügbaren Diensten



Die oberen Protokolle

Bluetooth

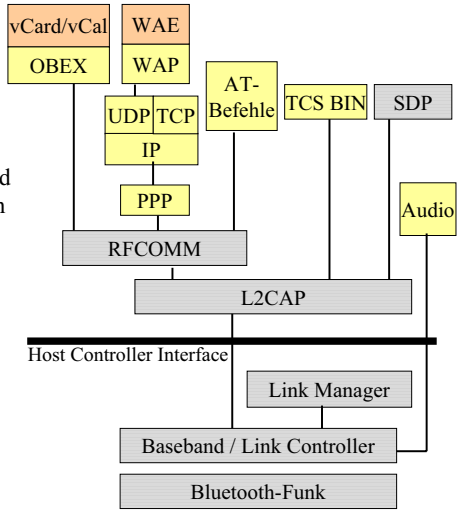
Adaptierte Protokolle

- **OBEX**
  - Austausch & Darstellung von Datenobjekten (vCard, vCal)
- **WAP**
  - Spezifikation zum Senden und Empfangen von Internet-Inhalten
- **TCP/UDP/IP/PPP**

- **Audio**

Telefonieprotokolle

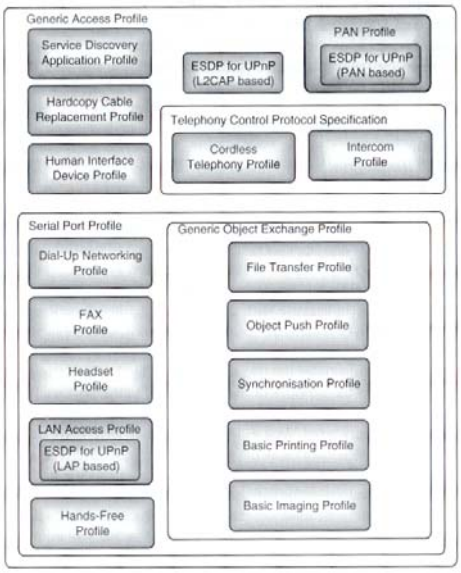
- **TCS BIN**
- **AT-Befehle**



Bluetooth-Profile – Allgemein

Bluetooth

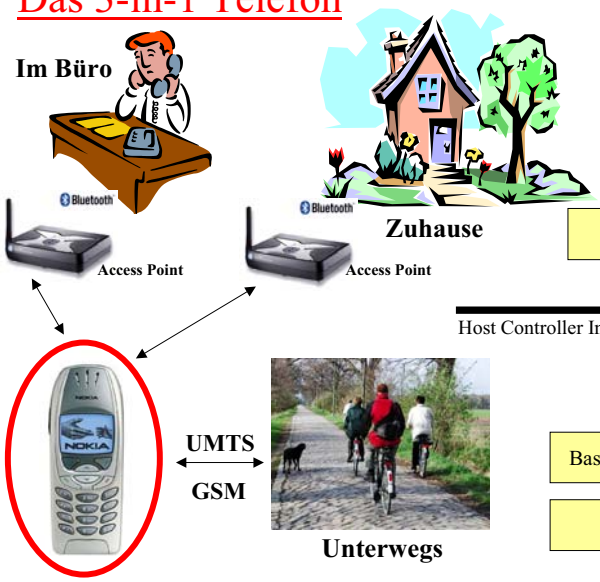
- Profile definieren erforderliche Protokolle und Eigenschaften
- Profile gewährleisten die reibungslose Interopera-bilität von Geräten verschiedener Hersteller
- Vorschläge, wie Einsatz-modelle implementiert werden können
- Alle Profile bauen auf dem Generic Access Profile auf

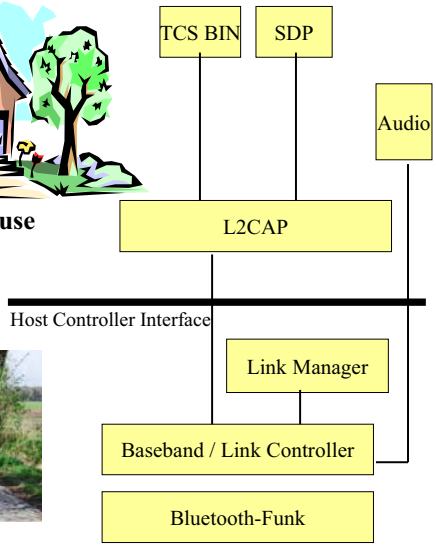


Bluetooth-Profile – Einsatzmodelle

Bluetooth

Das 3-in-1 Telefon





Bluetooth-Geräte & Unterstützte Profile

Bluetooth

Nokia Handy 3650	Nokia Digitalstift SU-1B	Nokia Headset HDW-2
		
Serial Port Profil **Hands-Free Profil** **DUN Profil**	**Serial Port Profil** **Object Push Profil** **DUN Profil**	**Serial Port Profil** **Hands-Free Profil** **Headset Profil**

Sicherheit-Überblick

Bluetooth

- Sicherheitsmodi
- Schlüsselmanagement
- Sicherheitsmechanismen
  - Authentifizierung
  - Verschlüsselung
- Sicherheitsmängel

Sicherheitsmodi

Bluetooth

- **Modus 1**
  - Keine Sicherheitsmechanismen
- **Modus 2**
  - Sicherheitsmechanismen erst nach dem Verbindungsaufbau
- **Modus 3**
  - Generell Authentifizierung vor dem Verbindungsaufbau
  - Verschlüsselung optional

Schlüsselmanagement

Bluetooth

Verbindungsschlüssel:

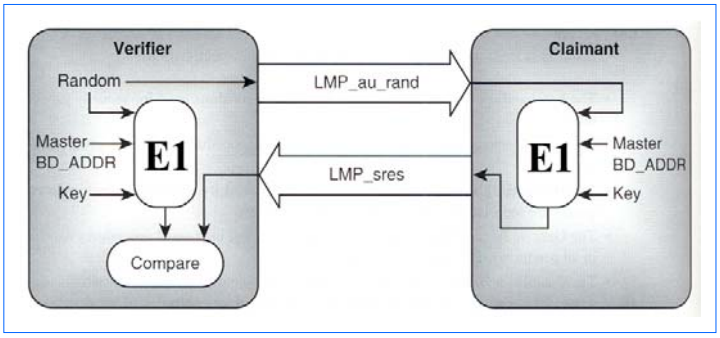
- Basis aller Sicherheitsmaßnahmen
- 128 Bit große Zufallszahl
- 4 verschiedene Arten
  - Kombinationsschlüssel
  - Initialisierungsschlüssel
  - Geräteschlüssel
  - Masterschlüssel

Sicherheitsmechanismen

Bluetooth

Authentifizierung

- Verhinderung unerwünschter Zugriffe
- Grundsätzlich einseitige Authentifizierung

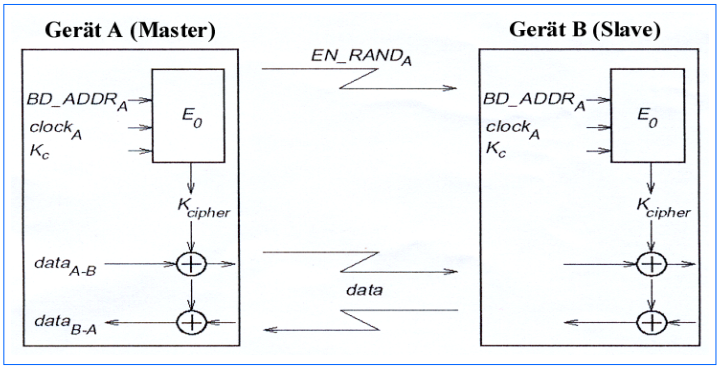


Sicherheitsmechanismen

Bluetooth

Verschlüsselung

- Abgeschlossene Authentifizierung notwendig
- Grundsätzlich nur Verschlüsselung des Payload



Sicherheitsmängel

Bluetooth

- **Nur Geräte-Authentifizierung**
- **Verschlüsselung nicht grundsätzlich vorgeschrieben**
- **Die PIN als unzuverlässiger Sicherheitsparameter**
- **Geräteschlüssel sind unsicher**
- **Qualität des Zufallsgenerators**
- **Unsichere Voreinstellungen**

IrDA

Bluetooth

- seit 1993 Standard für kabellosen Datenaustausch
- entwickelt von der Infrared Data Association

Vorteile	Nachteile
Bis zu 16 Mbit/s Datenübertragungsrate	Reagiert empfindlich auf Umgebungslicht
Günstige Sender und Empfänger	Nur Point-to-Point-Verbindungen möglich
Geringer Energieverbrauch	Sichtverbindung notwendig
Keine Störung anderer Geräte	Kurze Reichweite

ZigBee

Bluetooth

- **ZigBee Allianz (seit Oktober 2002)**
- **2,4 GHz ISM-Band**
- **IEEE 802.15.4**
- **Anwendungsbereiche**
  - **Security Bereich**
  - **Gebäudeautomatisierung**
  - **Telemetrie-Applikationen**

ZigBee Alliance, MICROCHIP, MATTEL, intel, PHILIPS Let's make things better, MOTOROLA intelligence everywhere, Honeywell

ZigBee

Bluetooth

- Geringe Herstellungskosten
- Minimaler Stromverbrauch
- Bis zu 254 aktive Slaves
- Sendereichweite 30 – 100 m
- Max. Datenrate 250 kbit/s

ZigBee

Bluetooth

ZigBee
und
Bluetooth → **Interferenzen**

→ **Bei Bluetooth-Übertragung: gering**

→ **ZigBee**
- Häufiger Stand-by-Betrieb
- Kürzere Arbeitszyklen

→ **Bei ZigBee-Übertragung: erneute Datenübertragung**

WLAN

Bluetooth

WLAN und Bluetooth

- **2,4 GHz-Band**
- **geringer Abstand**

→ **Interferenzen**

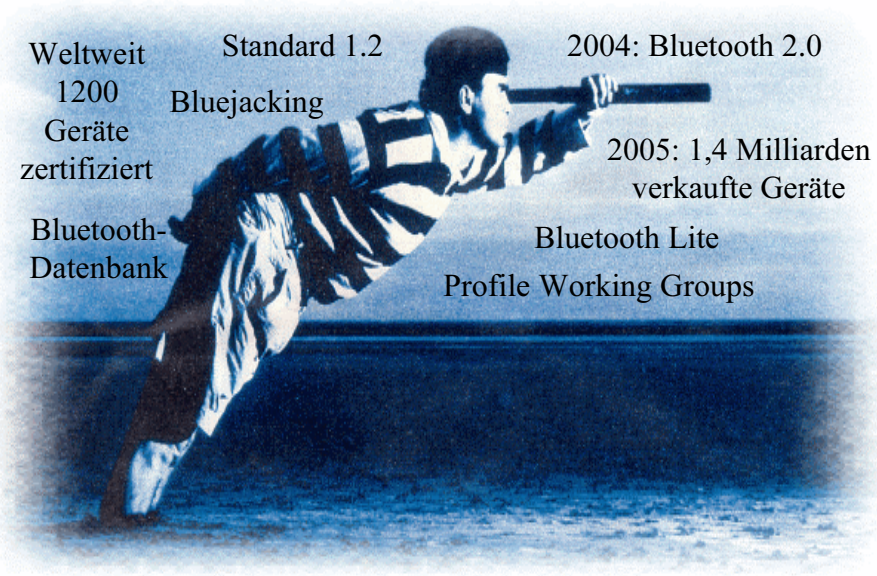
→ **Einbrüche in Übertragungsleistung bei WLAN**

- **sinkende Datenrate**
- **längere Übertragungszeit**

→ **steigende Störanfälligkeit**

Aktuelles & Ausblick

Bluetooth




Ich träum von
Bluetooth ...