Bluetooth

Sandra Hagen, Christian Wöck

Hauptseminar „Dienste & Infrastrukturen mobiler Systeme“
Wintersemester 03/04
Institut für Informatik
Ludwig Maximilians Universität München
{hagens, woeck}@informatik.uni-muenchen.de

Zusammenfassung. Überall, ob in öffentlichen Einrichtungen, Firmenbüros oder auch Zuhause sind Kabel allgegenwärtig. Dabei existieren die unterschiedlichsten Kabelverbindungen, wie z. B. Verbindungen zwischen dem Computer und Drucker, oder anderen Peripheriegeräten, die u.a. unter dem Schreibtisch einen unerwünschten Kabelsalat bilden. Der heutige Trend geht jedoch über zur drahtlosen Kommunikationstechnik, wobei die Kommunikation zwischen den mobilen Endgeräten kabellos erfolgt. Die drahtlose Bluetooth-Technologie ist genau so eine Technik, die Kabel überflüssig werden lässt und bequem die Daten per Funk zwischen den einzelnen Geräten austauscht.
Diese Ausarbeitung soll einerseits einen grundlegenden Überblick über die Bluetooth-Technologie geben und die Funktionsweise dieser drahtlosen Übertragungstechnik weitestgehend vermitteln. Andererseits sollen auch Sicherheitsmechanismen und Konzepte betrachtet und Bezug auf konkurrierende Technologien genommen, sowie ein Ausblick auf kommende Entwicklungen gegeben werden.

1 Einleitung

1.1 Für was steht Bluetooth?

Bluetooth ist ein offener, internationaler, lizenzfreier Industriestandard, welcher mittels Funk eine drahtlose Sprach- und Datenkommunikation über kurze Strecken zwischen verschiedenen Geräten ermöglicht. Er dient als Kabelersatz und unterstützt ein Ad-Hoc Netzwerk mit bis zu acht Teilnehmern.

Der Name stammt ursprünglich von dem dänischen Wikinger-König Harald Blatand (englisch Bluetooth), der im 10. Jahrhundert Dänemark und Norwegen vereinte. Die Namensgeber assoziierten damit die Vereinigung von Peripheriegeräten. Ein Zusammenwachsen der Telekommunikations- und Computerbranche sollte dadurch angestrebt werden.

Durch die Interessengemeinschaft von fünf Unternehmen aus der Telekommunikations- und Computerbranche wurde im Mai 1998 die SIG (Special Interest Group) gegründet. Zu den Gründungsfirmen gehören Nokia, Ericsson, Intel, IBM und Toshiba. Ziel war es, einen preiswerten und energiesparenden Standard zu entwickeln, mit dem man Daten mittels Kurzstreckenfunk zwischen verschiedenen Geräten, wie PC und

anderen mobilen Endgeräten austauschen und übertragen kann. Es sollte eine neue Form der Kommunikation den Markt revolutionieren.

Bluetooth ist eine Technologie, mit der eine Übertragung von Sprache und Daten über kurze Strecken möglich ist und dabei die Kommunikation zwischen den mobilen Endgeräten kabellos erfolgt. Die Bluetooth-Spezifikation ist eine offene Technologie und bedeutet, dass andere Firmen Bluetooth lizenzfrei nutzen können, jedoch die Gründungsfirmen sich bei Spezifikationsänderungen ein Veto Recht vorbehalten.

Bluetooth zeichnet sich durch seine besonderen Eigenschaften wie Sicherheit, Flexibilität, Robustheit und geringem Energieverbrauch aus. Da Bluetooth dezentral arbeitet, können alle Geräte, die Bluetooth-fähig sind, ohne Verwendung einer zentralen Station miteinander kommunizieren und ihre Daten austauschen.

Im folgenden werden Bereiche, in denen Bluetooth angewendet wird, sowie ein mögliches Szenario vorgestellt. In Kapitel 2 werden die technischen Grundlagen und die Funktionsweise der drahtlosen Übertragungstechnik, als auch Netzwerkstrukturen und Topologien, anhand der Bluetooth-Protokollarchitektur, genauer betrachtet.

Das Kapitel 3 befasst sich mit den Profilen, welche eine grundlegende Voraussetzung für die Entwickler sind, da sie die Bluetooth-Protokolle mit bestimmten Parametern festlegen und somit gewährleisten, dass die Geräte herstellerunabhängig miteinander kommunizieren können. Kapitel 4 gibt einen Überblick der verschiedenen Sicherheitsmechanismen und Konzepte. In Kapitel 5 wird Bezug auf vergleichende Technologien genommen und anschließend ein Ausblick auf kommende Entwicklungen gegeben. Zu guter Letzt folgt eine Schlussbetrachtung.

1.2 Anwendungsbereiche

Anfangs war Bluetooth zunächst nur als Kabelersatz für Peripherieanschlüsse gedacht, um Modems, Mäuse und Tastatur mit dem PC zu verbinden. Heute findet es in vielen Bereichen der Tele- und Datenkommunikation Einsatz und deckt eine Reihe weiterer Anwendungen ab, wie etwa die direkte Kommunikation zwischen Personal Digital Assistants und Mobiltelefonen, um Visitenkarten und Termine zu übertragen, oder zu surfen.

Das Funkmodul lässt sich in zahlreichen Geräten, wie Mobiltelefone, drahtlose Headsets, Notebooks, Digitalkameras oder Internetzugangsgeräten (ISDN-Adapter, Modems) einbauen. Im Haushalt können auch Kühlschränke, Heizungen und Alarmanlagen über Bluetooth mit einer Schalt- und Alarmzentrale verbunden werden. Die Anwendungsfelder bieten diesbezüglich ein breites Spektrum.

Was Bluetooth von anderen, bereits bestehenden Wireless-Lösungen wie IrDA unterscheidet, ist seine Fähigkeit nicht nur mit zwei Geräten, sondern mit mehreren Komponenten gleichzeitig und noch dazu ohne Sichtverbindung kommunizieren zu können.

Der Einsatz von Bluetooth ist nahezu unbegrenzt. Hier ein kleiner Auszug von Bluetooth-fähigen Anwendungen, die denkbar sind oder bereits verwendet werden. [5]

- Bluetooth-Smartphones mit eingebauter Kamera befördern Fotos per Nahfunk zum PC und sparen so teure GPRS-Gebühren
- Bluetooth verbindet Mobiltelefone mit PDAs und Freisprecheinrichtungen im Kraftfahrzeug

- Durch das Bluetooth-Headset kann der Autofahrer im Straßenverkehr schnurlos und ohne Einsatz der Hände legal 43telefonieren
- Mit einer drahtlos angeschlossenen Digitalkamera lassen sich per PC oder Mobiltelefon Bilder in Echtzeit, sowie elektronische Postkarten verschicken
- Schnelle drahtlose Konferenzschaltung mit Sprachverkehr und Datenaustausch, etwa bei geschäftlichen Besprechungen und die drahtlose Steuerung von Geräten, wie etwa von Videoprojektoren
- E-Mail im Zug oder Flugzeug am Laptop verfassen und später, nach Wiedereinschalten des Mobiltelefons, automatisch versenden
- USB-Adapter bieten die Möglichkeit den PC mit Bluetooth nachzurüsten
- Per Fernbedienung lässt sich der MP3-Player per Bluetooth aus einem Nachbarraum bedienen
- Bluetooth bietet durch die Implementierung in einen Access Point den Anschluss an ein LAN, das GSM- oder das Festnetz
- In Japan können Bluetooth-fähige Toiletten Stuhlgang-Messwerte auf den PDA des Benutzers übertragen
- Kabellose Digitallautsprechersysteme mit Bluetooth-Technik ermöglichen ein flexibles Aufstellen der Boxen

Nun soll noch anhand eines möglichen Szenarios der Einsatz von Bluetooth verdeutlicht werden.

Morgens um sieben. Max startet normalerweise den Tag mit Kaffee und einem gemütlichen Frühstück. Da er aber schon spät dran ist, drückt er, um Wegzeit in die Küche zu sparen, die Bluetooth-fähige Fernbedienung, welche die Kaffeemaschine automatisch in Gang setzt. Das Telefon klingelt, als er gerade im Bad ist. Zum Glück liegt sein Headset noch vom letzten Telefonat griffbereit neben dem Waschbecken. Es ist sein Chef, der noch bestimmte Daten für die heutige Präsentation ausgedruckt haben will. Das hat ihm gerade noch gefehlt. Jetzt hat er schon nicht mal mehr Zeit für ein Frühstück und soll noch was ausdrucken. Er will Zeit sparen und sendet die Daten an sein PDA, um sie dann im Büro auszudrucken. Dafür muss er aber ganz schön ins Gaspedal treten. Am Büro angekommen, zwängt er sich in die einzig vorhandene Parklücke, die natürlich zu klein ist. Dabei rammt er noch einen Pfosten, der zu niedrig war, um ihn im Rückspiegel zu entdecken. Wütend steigt er aus dem Auto und denkt sich „Na toll, heute passt einfach alles! Jetzt finde ich wenigstens gleich Verwendung für die neue Digitalkamera, die schon seit einer Woche unbeachtet auf der Rückbank liegt.“ Mit der Kamera hält er den Schaden fest und überträgt das Bild an sein Mobiltelefon, welches es gleich per Mail an seine Autoversicherung sendet. Da die Präsentation schon angefangen hat, findet er keine Zeit mehr die Daten auszudrucken. Zum Glück ist das Notebook von seinem Chef Bluetooth-fähig. Er sendet die Daten an das Notebook, bevor er den Präsentationsraum betritt, und platzt dann vor lauter Hektik mit: “Danke, Bluetooth!..ähh, Sorry Chef!“ herein. Sein Chef ist erst verdutzt, dann aber doch sichtlich erfreut über die fortschrittliche Denkweise seines Mitarbeiters und fährt voller Begeisterung die Präsentation mit den jetzt vorhandenen Daten fort.

2 Die Bluetooth-Protokollarchitektur

Im folgenden werden die Funktionsweisen der einzelnen Protokolle der Bluetooth-Protokollarchitektur betrachtet. Dabei ist anzumerken, dass bereits vorhandene Protokolle wiederverwendet und für Bluetooth-spezifische Anwendungen entsprechend neu entwickelt wurden. In Abbildung 1 ist die Bluetooth-Protokollarchitektur abgebildet. Zunächst ein Überblick.

Die unterste Schicht ist die Funk-Schicht, die für die eigentliche Übertragung der Daten via Funk zuständig ist. Darauf setzen das Baseband und der Link Controller auf, die wesentliche Funktionen zur Kommunikationsabwicklung und des Verbindungsaufbaus bereithalten.

Das Link Manager Protocol (LMP) kontrolliert und konfiguriert die Verbindungen zu anderen Bluetooth-Geräten. Das Host Controller Interface ist die Schnittstelle zwischen den oberen und den unteren Schichten und ermöglicht so die Kommunikation zwischen einem Bluetooth Host und einem Bluetooth Modul.

Das Logical Link Control and Adaptation Protocol (L2CAP) unterstützt das Multiplexing der höheren Ebenen, die Paketsegmentierung und Reassemblierung sowie QoS (Quality of Service). Das Service Discovery Protocol (SDP) dient zum Auffinden von verfügbaren Diensten und dem Abfragen der Eigenschaften dieser Dienste. Es folgt eine detaillierte Beschreibung der Bluetooth-Protokollarchitektur. [24], [25]

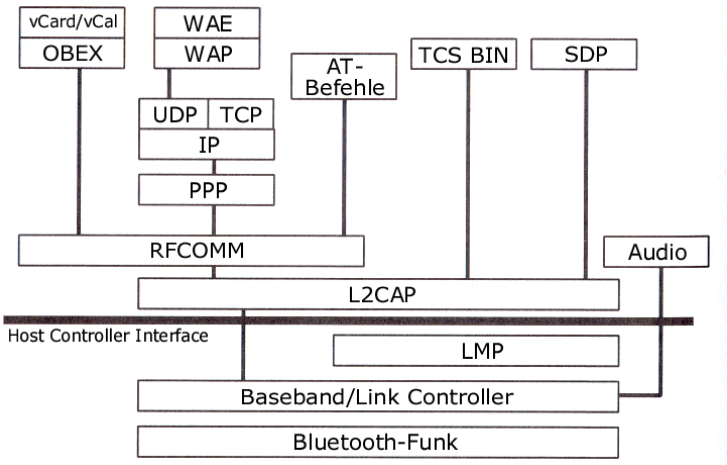


Abbildung 1: Die Bluetooth-Protokollarchitektur

2.1 Funk

Der Bluetooth-Funk ist die physikalische Schnittstelle und unterste Schicht in der Protokollarchitektur. Er definiert die Eigenschaften und Anforderungen für die Bluetooth-Transceiver-Geräte und für den Übertragungsweg bzw. der Funkstrecke. Bluetooth arbeitet im weltweit verfügbaren lizenzfreien 2,4 GHz ISM-Band (**I**ndustrial, **S**cientific and **M**edical), welches auch für Geräte aus Industrie, Wissenschaft und

Medizin zur Verfügung steht. Einige der Parameter sind in Tabelle 1 aufgelistet. [21], [29]

Topology	**Up to 7 simultaneous links in a logical star**
Modulation	GFSK
Peak data rate	1 Mbps
RF bandwidth	220 kHz (-3 dB), 1 MHz (-20 dB)
RF band	2.4 GHz, ISM band
RF carriers	23/79
Carrier spacing	1 MHz
Transmit power	0.1 W
Piconet access	FH-TDD-TDMA
Frequency hop rate	1600 hops/s
Scatternet access	FH-CDMA

Tabelle 1: Bluetooth Funk- und Baseband-Parameter

Um gegen Störungen gegenüber anderen Geräten unempfindlich zu sein, verwendet Bluetooth eine Spreiz-Spektrum-Technologie, das Frequency Hopping Spread Spectrum in Kombination mit Time Division Duplex. Das Band wird dabei in 79 Kanäle (bzw. 23 in Frankreich) mit jeweils 1 MHz Breite aufgeteilt und die Frequenz 1600-mal pro Sekunde gewechselt.

Für die Modulation wird das GFSK (Gaussian Frequency Shift Keying) eingesetzt, da sich die Hardware im Vergleich zu komplexeren Modulationsverfahren sehr leicht und preiswert herstellen lässt. [13]

Die Funkreichweite hängt von der Übertragungsleistung der Bluetooth-Geräte ab und wird dazu in drei Sendeleistungsklassen unterteilt:

Klasse 1 100 mW bis zu maximal 100 m Reichweite
Klasse 2 2,5 mW bis zu ca. 20 m Reichweite
Klasse 3 1 mW bis zu ca. 10 m Reichweite

2.2 Baseband und Link Controller

Das Baseband bezieht sich auf die physikalische Schicht der Bluetooth-Protokollarchitektur. Es ist für die Übertragung von Daten über die Funk-Schicht zuständig und realisiert dazu den physikalischen Übertragungskanal. Dieser wird verwendet um physische Links zwischen den Bluetooth-Geräten in einem Piconet aufzubauen. Der Link Controller kontrolliert und konfiguriert dabei die Verbindungen zu den anderen Bluetooth-Geräten und kann neu hinzukommende Geräte, die sich in Reichweite befinden, entdecken.

2.2.1 Piconet und Scatternet

Bluetooth unterscheidet zwischen **Master** und **Slave,** wobei aus Sicht der Netzwerktopologie der Master derjenige ist, der eine Verbindung initiiert. Er bestimmt die Frequenzsprungfolge der Übertragung, die Phasen der Hop-Frequenz (abhängig von der internen Clock des Masters) und ist für die Synchronisation der verschiedenen Slaves zuständig. Somit kann er u. a. Kollisionen zwischen mehreren Slaves vermeiden, da alle Slaves, die mit dem gleichen Master kommunizieren, die gleiche Frequenzsprungfolge und Phase verwenden.

Es können sowohl Point-to-Point- als auch Point-to-Multipoint-Verbindungen aufgebaut werden. Ein Netz bestehend aus einem Master und maximal sieben aktiven Slaves wird als **Piconet** bezeichnet. Die Kommunikation erfolgt ausschließlich über den Master, eine direkte Kommunikation zwischen zwei Slaves ist nicht möglich. Da sich die Teilnehmer im Netz permanent ändern können, ist das Piconet auf Grund der Bewegungsfreiheit der Geräte ein dynamisches Netz.

Bei Bluetooth ist keine Infrastruktur notwendig, um eine Kommunikation zwischen den einzelnen Geräten zu ermöglichen und ein Netzwerk zu bilden, deswegen bezeichnet man dieses auch als ein sog. Ad-hoc Netzwerk.

Wird ein neuer Slave in ein Piconet aufgenommen, so wechselt dieser in einen aktiven Zustand und bekommt vom Master eine 3-bit lange Active Member Address (AM_ADDR) zugewiesen. Diese identifiziert den Slave eindeutig und bestimmt die maximale Anzahl von acht aktiven Geräten innerhalb des Piconet.

Um mit mehr als sieben Slaves kommunizieren zu können, werden zwei oder mehrere Piconets zu einem **Scatternet** zusammengefügt. In diesem Fall ist ein Blutooth-Gerät in einem Piconet der Slave und im anderen der Master.

In der folgenden Abbildung 2 ist eine Point-to-Point-Verbindung, eine Point-to-Multipoint-Verbindung und eine mögliche Bildung eines Scatternets abgebildet. [6], [10], [16], [29], [31]

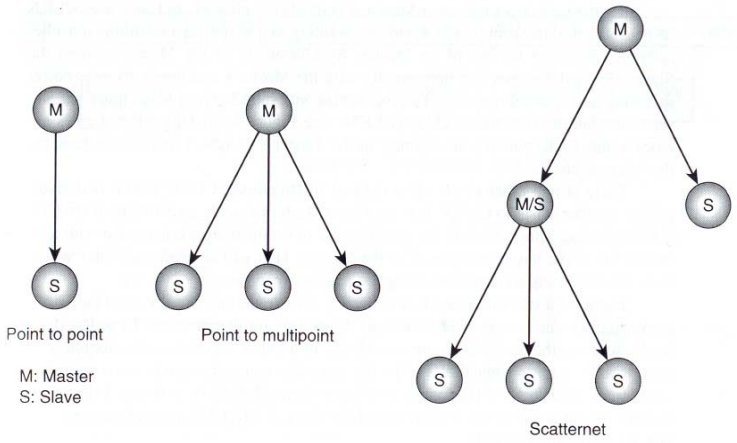


Abbildung 2: Piconet und Scatternet

2.2.2 Frequency Hopping

Ursprünglich wurde das Frequency Hopping von der Schauspielerin Hedy Lamarr während des 2. Weltkrieges erfunden. In der damaligen Militärtechnik gab es Überlegungen, Torpedos über Funk zu steuern. Technisch ließ sich die Fernsteuerung zwar mittels Funk lösen, doch das Steuerungssignal der Torpedos konnte leicht vom Feind entdeckt und gestört werden. Der Freqeuncy Hopping Mechanismus sollte das Steuerungssignal der Torpedos über mehrere Frequenzen verteilen, um so vor Störungen des Feindes sicher zu sein. [20], [24], [27]

Wie bereits erwähnt, arbeitet Bluetooth im 2.4 GHz ISM-Band. Da dieses Band frei zugänglich ist und somit auch von Mikrowellenherden und WLAN verwendet wird, helfen sog. Spreizspektrum Technologien Störungen zu vermeiden.

Bluetooth verwendet das Frequenzsprungverfahren in Verbindung mit Time Division Duplex. Das benutzte Frequenzband wird in 79 physikalische Kanäle unterteilt. Die Größe der Zeitschlitze beträgt 625 µs und damit ergibt sich ein Frequenzhäufigkeitswechsel von 1600 hops/s, wobei die Hoppingsequenz pseudozufällig ist. Wenn ein Paket „gestört“ wird, wird es zu einem späteren Zeitpunkt noch mal auf einer anderen Frequenz gesendet.

TDD bedeutet bei Bluetooth, dass Up- und Downlink auf demselben Frequenzbereich zu verschiedenen Zeitpunkten gesendet wird. Der Master sendet in geraden Zeitschlitzen und der Slave in ungeraden. Das Zeitschlitzverfahren ist in Abbildung 3 dargestellt. [1], [13], [16], [29]

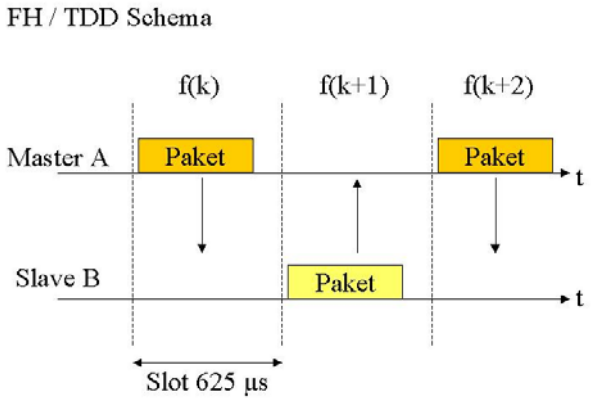


Abbildung 3: Time Division Duplex

2.2.3 Physikalische Verbindungen

Die Bluetooth-Spezifikation hat zwei Arten von physikalischen Verbindungen für die Übertragung von Sprache und Daten definiert:

SCO Synchronous Connection-Oriented Link
ACL Asynchronous Connection-Less Link

Beim Einsatz von einer synchronen verbindungsorientierten und leitungsvermittelten Übertragung spricht man von einer SCO-Verbindung. Diese ist eine symmetrische Punkt-zu-Punkt-Verbindung zwischen einem Master und genau einem Slave in einem Piconet. Dabei kann der Master bis zu drei SCO-Links gleichzeitig unterstützen. Slaves unterstützen zwei SCO-Links gleichzeitig zu verschiedenen Mastern.

Diese Verbindungsart wird verwendet, wenn eine geringe Verzögerung und ein hoher QoS verlangt ist. Deswegen wird sie bei der Übertragung von Sprache, welche entweder mit Continuously Variable Slope Delta (CVSD) oder mit Pulse Code Modulation (PCM) möglich ist, eingesetzt. Über jede dieser SCO-Verbindungen können Pakete mit maximal 64 kbit/s übertragen werden.

SCO-Paketen wird eine feste Bandbreite durch den Master garantiert, d.h. es werden Slots für die zu übertragenden Pakete reserviert. Durch die synchrone Übertragung wird weniger Overhead produziert, da keine Header-Informationen benötigt werden. Beide Kommunikationspartner wissen außerdem genau, wann das nächste Paket kommt. Nachteilig ist jedoch die Verschwendung von Funkressourcen, weil bei der kompletten Übertragung die Slots konstant zugewiesen sind und kein wiederholtes Senden der Pakete erfolgt. Sie werden nur einmalig übertragen, weil die sonst entstehende Verzögerung die Sprachqualität herabsetzen würde. Slots, die nicht für einen SCO-Link reserviert sind, kann der Master für ACL-Verbindungen nutzen.

Die ACL-Verbindung ist eine asynchrone, verbindungslose und paketorientierte Verbindung und kommuniziert über eine Punkt-zu-Multipunkt-Verbindung zwischen dem Master und allen aktiven Slaves in einem Piconet. Dabei stehen also bis zu 7 Kanäle pro Piconet zur Verfügung. Zwischen einem Slave und Master kann jeweils nur eine ACL-Verbindung bestehen. Slaves können bei diesem Verbindungstyp nur Daten senden, wenn der Master dies anordnet. Es ist keine Reservierung der Slots für die Übertragung notwendig. Diese asynchronen verbindungslosen Verbindungen werden hauptsächlich für Datenübertragung genutzt. Verlorengegangene Pakete werden wiederholt versendet.

Die Daten werden mit maximal 432,6 kbit/s (symmetrisch) in beide Richtungen oder mit 723,2 kbit/s (57,6 kbit/s im Rückkanal, asymmetrisch) in eine Richtung übertragen. In Tabelle 2 sind alle möglichen Datenraten, die über eine ACL-Verbindung gesendet werden, aufgelistet. [1], [3], [7], [29]

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

Tabelle 2: Datenraten der ACL-Pakete

2.2.4 Link Controller

Der Link Controller dient zur Ausführung von höherliegenden Operationen wie Inquiry und Paging und koordiniert die Erkennung eines neuen Gerätes und dessen Verbindungsaufbau.

Bluetooth-Geräte befinden sich zu jedem Zeitpunkt in einem bestimmten Zustand. Die Hauptzustände sind Standby und Connection. Die sieben Sub-Zustände werden verwendet, um Slaves einem Piconet hinzuzufügen und Verbindungen aufzubauen. Dazu zählen **Inquiry, Inquiry Scan, Page, Page Scan, Master Response, Slave Response** und **Inquiry Response**. [4], [29], [30]

Im folgenden werden die einzelnen Zustände beschrieben. Eine graphische Darstellung der einzelnen Zustände und deren Übergänge wird in Abbildung 4 dargestellt.

- **Standby**

In diesem Zustand ist das Gerät inaktiv und kann auch nicht von den anderen Geräten entdeckt werden. Dieser Zustand wird verwendet, um einen Low-Power-Zustand zu ermöglichen. Nur wenn nach Page- oder Inquiry-Nachrichten gescannt wird, kann der Standby-Zustand verlassen werden.

- **Inquiry**

Die Inquiry-Prozedur kann feststellen, ob sich andere Bluetooth-Geräte innerhalb der Reichweite befinden. Nach einem Inqiry liegen alle Geräteadressen und Zeittakte der gefundenen und kommunikationsbereiten Geräte vor.

- **Inquiry Scan**

Dieser Zustand stellt ein Teil des Inquiry-Zustandes dar. Damit ein Gerät auch ein Inquiry entdecken kann, wird in diesen Zustand gewechselt.

- **Inquiry Response**

Ein Gerät, welches ein Inquiry ausgeführt hat, erhält ein Inquiry Reponse zurück.

- **Page**

Wurden die in Reichweite befindlichen Bluetooth-Geräte bereits erfasst, so wird versucht, zu einem bestimmten Bluetooth-Gerät durch Paging eine Verbindung aufzubauen. Dabei überträgt der Master auch den Device Access Code (DAC) vom Slave.

- **Page Scan**

Das Gerät lauscht, ob ein Page mit seinem eigenen Device Access Code gesendet wird.

- **Master Response**

Der Master empfängt eine Antwort vom Slave und kann nun in den Connection- Zustand übergehen oder in den Page-Zustand zurückkehren, um nach weiteren Slaves zu pagen.

- **Slave Response**

Slave antwortet hierbei auf ein Page vom Master. Wenn der Verbindungsaufbau erfolgreich war, wird in den Zustand Connection übergegangen. Ansonsten kehrt er in den Page Scan-Zustand zurück.

- **Connection**

Nachdem eine Verbindung beiderseits aufgebaut wurde, kann in den Zustand Connection gewechselt werden.

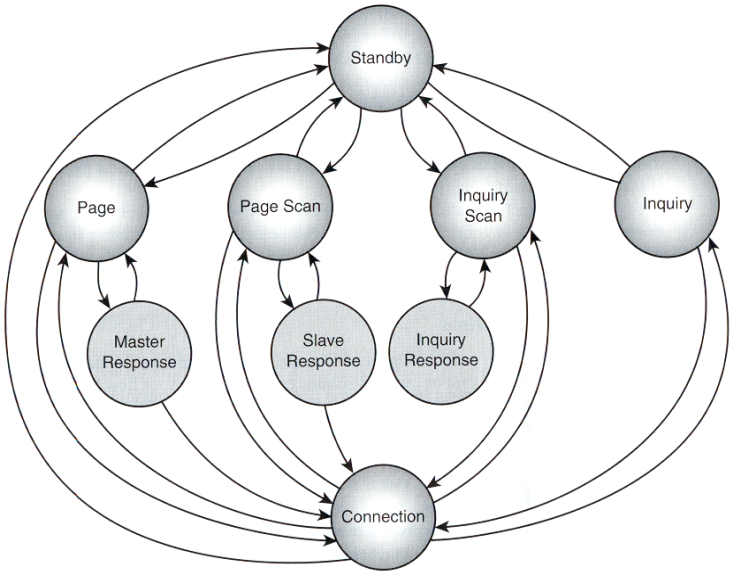


Abbildung 4: Link Controller Zustandsdiagramm

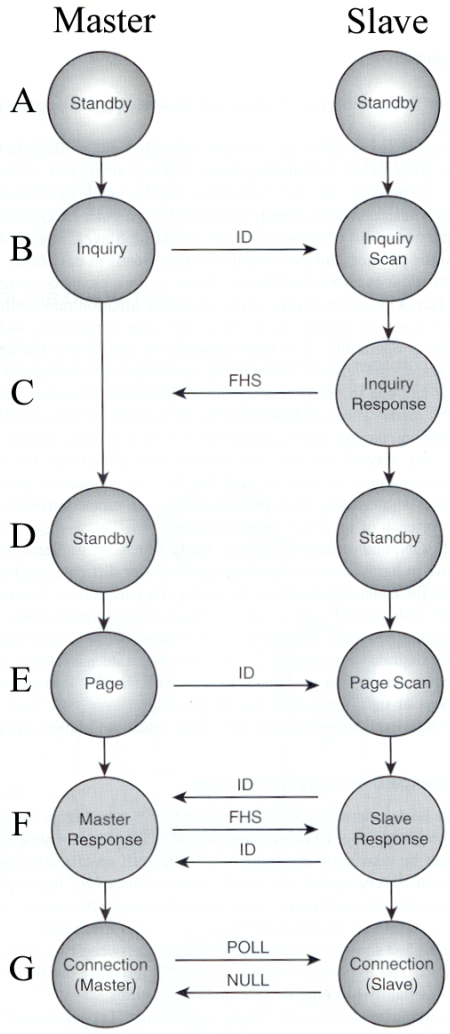
2.2.5 Verbindungsaufbau durch Inquiry und Paging

Der Verbindungsaufbau kann von jedem Endgerät initiiert werden, welches dann automatisch der Master wird. In Abbildung 5 ist der Verbindungsaufbau zwischen zwei Bluetooth-Geräten dargestellt.

Bevor eine Verbindung aufgebaut wird, befinden sich alle Geräte im Standby-Zustand **(A)**. Der Verbindungsaufbau erfolgt über die Prozeduren Inquiry und Paging. Mit Inquiry kann ein Bluetooth-Gerät feststellen, ob sich andere Geräte innerhalb der Reichweite befinden. Wenn also die Adresse und der Zeittakt der neu hinzukommenden Geräte nicht bekannt ist, wird Inquiry angewendet.

Führt ein Gerät ein Inquiry aus, so sendet es Inquiry-Pakete an alle Bluetooth-Geräte, die sich in Reichweite befinden **(B)**. Das Gerät, welches sich z.B. gerade im Inquiry Scan-Zustand befindet, kann nun, nachdem es ein Inquiry-Paket empfangen hat, in den Inquiry Response-Zustand übergehen und mit einem FHS-Paket (Frequency Hopping Synchronization) antworten **(C)**. Das Paket enthält u.a. die Geräteadresse und den Zeittakt.

Nach der Inquiry-Prozedur ist es dem Master möglich eine Kommunikationsverbindung zu den entsprechenden Geräten mit der Paging-Prozedur aufzubauen und ein Piconet zu bilden.



Die Geräte wechseln zunächst in den Zustand Standby zurück **(D)**.

Dann geht der Master in den Zustand Page, und die anderen Geräte entsprechend in den Page Scan-Zustand über **(E)**.

Der Master sendet ein ID-Paket mit dem Device Access Code des Slaves und wechselt in Master Response.

Der Slave, der ein Page mit seinem Device Access Code empfangen hat, geht in den Zustand Slave Response über und antwortet dem Master mit dem gleichen Paket **(F)**.

Nach diesem Handshake sendet der Master in einem FHS-Paket seine Geräteadresse und Zeittakt an die verbundenen Slaves.

Für die weitere Kommunikation wird der Zeittakt und die Sprungsequenz des Masters, die so genannte Channel-Hopping-Sequence verwendet.

Wenn es keine weiteren Slaves gibt, die einen Verbindungsaufbau wünschen, wird in den Zustand Connection gewechselt **(G)**.

Ansonsten führt der Master so lange ein Page durch, bis zu allen Slaves eine Verbindung besteht und geht dann erst in den Zustand Connection über.

Abbildung 5: Der Verbindungsaufbau

Um sicher zu gehen, dass die Channel-Hopping-Sequence und der Zeittakt des Masters verwendet wird, schickt der Master ein POLL-Paket (erfordert vom Empfänger eine Bestätigung) zum Slave. Der wiederum antwortet mit einem NULL-Paket, um den erfolgreichen Empfang des Paketes zu bestätigen. Die Verbindung ist nun aufgebaut und die Datenübertragung kann beginnen. [2], [3], [6], [24]

2.2.6 Paket-Struktur

Bluetooth verwendet für die Datenübertragung ein allgemeines Paket-Format, das sogenannte **Standard-Paket-Format.** Das allgemeine Format besteht aus drei Einheiten:

1. *Access Code (Zugangscode)*
2. *Header (Paketkopf)*
3. *Payload (Nutzdaten)*

Access Code und Header haben im Allgemeinen feste Größen. Der Payload bzw. die Nutzdaten können in der Größe von 0 bis 2745 Bit variieren. Wenn die Größe 0 beträgt, kann der Payload somit auch entfallen.

(1) Access Code

Der Access Code ist abhängig von der Adresse des Masters und dessen Uhr. Er dient zur Synchronisation und Identifizierung und ist auch für das Paging und Inquiry zuständig.

Ein Bluetooth-Gerät überprüft den Access Code eines jeden empfangenen Paketes. Wenn er ungültig ist, wird das komplette Paket ignoriert. Innerhalb eines Piconet haben alle gesendeten Pakete den gleichen Access Code. Die Identifikation der richtigen Pakete fällt dadurch den teilnehmenden Bluetooth-Geräten leicht.

Jedes Paket beginnt mit einem 72 Bit langen Access Code, der sich aus der Gerätekennung des Masters ableitet. Folgt kein Paket-Header, ist der Access Code nur 68 Bit lang. Im folgenden wird der Aufbau des Access Codes erläutert und in Abbildung 6 dargestellt.

PREAMBLE

Der erste Teil des Access Code besteht aus einer Sequenz von 4 alternierenden Bits, der Präambel (Preamble). Dabei ist die Bitfolge abhängig vom ersten Bit (Least Significant Bit, LSB) des Sync Word Feldes. Ist das erste eine 1, so lautet die Präambel 1010, ist es eine 0, dann lautet sie 0101. Die Präambel zeigt dem Empfänger die Ankunft eines Paketes an und dient zur Feinsynchronisierung zum Sender.

SYNC WORD

Das Sync Word wird für die Synchronisation und das Timing mit dem Empfänger verwendet und ist 64 Bit lang.

TRAILER

Der Trailer hat, wie die Präambel, den gleichen Nutzen und besteht genauso aus vier alternierenden Nullen und Einsen. Wenn das Most Significant Bit (MSB) des Synchronisationswortes eine 1 ist, folgt 0101, hingegen bei einer 0 lautet er 1010. Nur wenn nach dem Access Code ein Header folgt, wird der Trailer mit angehängt.

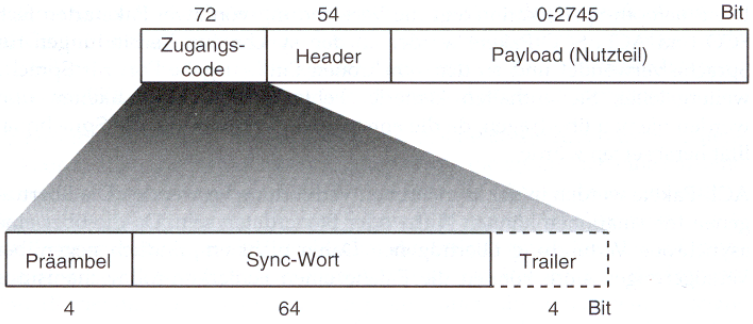


Abbildung 6: Der Access Code

- **Access Code Typen**

Der Access Code wird je nach Betriebszustand in drei Typen unterschieden:

– **CAC** (Channel Access Code): Der CAC wird zur Synchronisation und Identifikation in einem Piconet verwendet. Alle gesendeten Pakete, die sich im selben Piconet befinden, haben den gleichen CAC.

– **DAC** (Device Access Code): Dieser Code wird für spezielle Prozeduren, wie der Verbindungsaufbau mittels Paging, verwendet.

– **IAC** (Inquiry Access Code): Der IAC wird verwendet, um Bluetooth-Geräte innerhalb der Reichweite zu finden, was, wie bereits erwähnt, durch eine Inquiry Prozedur möglich ist.

(2) Header

Der Header enthält Link-Steuerinformationen wie z.B. Sequenznummer und Empfängeradresse für eine Verbindung. Da der Header mit einer 1/3 FEC (Forward Error Correction) gesichert ist, ergibt sich aus der eigentlichen Größe von 18 Bit eine Header Grösse von 54 Bit, da jedes Bit dreimal hintereinander gesendet wird.

Folgende Felder befinden sich im Header (siehe auch Abbildung 7):

– *Active Member Address AM_ADDR*

Die Active Member Address, welche aus 3 Bits besteht, bestimmt die Adresse der Teilnehmer im Piconet bzw. identifiziert die aktiven Slaves.

Die Limitierung auf 7 ($2^3 - 1 = 7$) Slaves (Master selber hat keine) wird dadurch bestimmt, dass die Adresse 000 als Broadcast-Adresse vom Master an die Slaves benutzt wird.

– *Type*

Das Type Feld, bestehend aus vier Bit, legt fest, um was für ein Paket es sich handelt. Es gibt 16 verschiedene Paketarten. Entscheidend ist hierbei, ob es sich um eine SCO-Verbindung oder ACL-Verbindung gehandelt hat.

– *Flow*
Das Flow-Bit wird zur Flusssteuerung verwendet. Wenn der Empfangspuffer voll ist, wird ein temporärer Stop initiiert, welcher ein Überlaufen des Puffers verhindert. Dabei ist das Flow-Bit eine 0. Ist es eine 1, wurde der Puffer geleert.

– *ARQN*
Das ARQN ist ein Bestätigungsbit, das nach einem erfolgreichen Datenaustausch mit Hilfe einer Prüfsumme (CRC, Cylic Redundancy Check) überprüft und auf 1 gesetzt wird. Bei einem fehlerhaften Empfang wird es auf 0 gesetzt. Wenn der Sender keine Bestätigung erhält, geht er automatisch von einem negativen Empfang aus.

– *SEQN*
Das SEQN-Bit dient zur Erkennung und Ausfilterung der doppelt gesendeten und verlorenen Pakete. Mit Hilfe eines sequentiellen Nummerierungsschema kann die Reihenfolge der eintreffenden Datenpakete bestimmt und so die Integrität überprüft werden.

– *HEC*
Jeder Header endet mit einem 8 Bit großen Header Error Check, der für die Fehlererkennung und Überprüfung des Header zuständig ist. Ist der HEC nicht gültig, wird das gesamte Paket ignoriert.

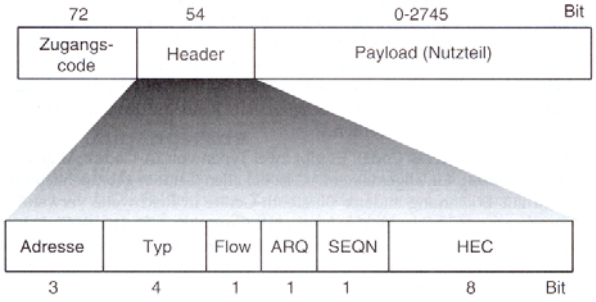


Abbildung 7: Der Header

(3) Payload

Die eigentlichen Daten werden im bis zu 2746 Bit langen Payload übertragen. Er enthält je nach Verbindungsart und Pakettyp entweder SCO-Sprachpakete- oder ACL-Datenpakete. Der ACL Payload besteht aus drei Feldern:

1. *Payload-Header* (8 Bit Header für ein Single-Slot-Paket, 16 Bit Header für ein Multi-Slot-Paket),
2. *Eigentliche Nutzdaten* (0-2721 Bit) und
3. *CRC* (16 Bit)

Der Payload bei SCO-Paketen hat eine feste Größe von 240 Bit. SCO-Pakete enthalten keinen CRC-Code. Sie sind ausschließlich Single-Slot-Pakete. Wenn ein Paket verloren geht, wird es, wie bereits erwähnt, nicht noch mal gesendet. Die Abbildung 8 zeigt den ACL Payload. [21], [29], [30]

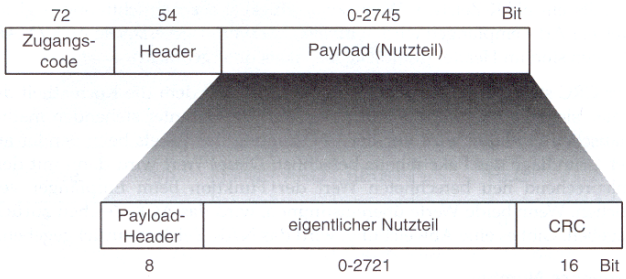


Abbildung 8: Der ACL Payload

2.3 Link Manager

Das Link Manager Protocol (LMP) setzt direkt auf dem Baseband auf. Die Kommunikation zwischen zwei Bluetooth Link Managern erfolgt über das Link Manager Protocol. Die Nachrichten, die im Datenstrom für den Link Manager bestimmt sind, werden von diesem herausgefiltert und entsprechend ausgewertet. Somit erreichen sie nicht die höheren Schichten.

Aus Sicht der höheren Schichten stellt der Link Manager Dienstleistungen zur Verfügung. Die Nachrichten, die zwischen den Link Managern ausgetauscht werden, nennt man PDUs (Protocol Data Units).

Der Link Manager ist für den Aufbau, sowie das Beenden der Verbindungen und für die Kontrolle zwischen den Bluetooth-Geräten und das Aushandeln der Baseband-Paketgrößen zuständig. Auch die Sicherheit, darunter fällt u.a. die Authentifizierung und Verschlüsselung, sowie die Generierung, der Austausch und die Überprüfung der Sicherheitsschlüssel, zählen zu seinen Aufgaben. Er ermöglicht auch den Wechsel der Master/Slave-Rollen. Die Einrichtung von SCO-Links findet ebenfalls auf dieser Ebene statt. Durch Power Control Prozeduren kann die Sendeleistung verändert und so für einen bestmöglichen Empfangspegel gesorgt werden.

Um den Leistungsverbrauch zu reduzieren, werden die sogenannten Energiesparzustände Hold, Sniff und Park verwendet, welche der Link Manager steuert. Dabei können die Geräte, die nicht senden oder empfangen, sich aber im Zustand Connected befinden, in den Low-Power-Modus wechseln (siehe auch Abbildung 9) und sich dann jeweils in einem der verschiedenen Energiesparzustände befinden. Im folgenden werden diese erläutert. [16], [21], [27]

- **Hold**

In diesem Zustand werden keine Daten übertragen, jedoch bleibt das Gerät im Piconet integriert. Nur der interne Timer des Slave läuft weiter. Es werden auch keine ACL-Pakete mehr unterstützt, SCO-Verbindungen bleiben jedoch erhalten. Der Master

kann den Hold-Zustand für einen Slave anordnen oder der Slave fordert den Master auf, ihn in den Hold-Zustand zu versetzen. Erst nach Ablauf einer vorher festgelegten Zeitspanne ist eine Kommunikation mit dem Gerät wieder möglich. Die Active Member Address bleibt bestehen.

- **Sniff**

Im Sniff-Zustand hört das Gerät nur in festgelegten Abständen das Netz ab, ob ein Paket mit seiner Adresse gesendet wird. Falls ja, antwortet es dem Master. Zur Synchronisation läuft der Timer im Slave weiter. Ein Slave hört demnach nicht kontinuierlich auf dem Kanal mit und reduziert damit seinen Energieverbrauch.

- **Park**

Innerhalb eines Piconets können die Bluetooth-Geräte auch geparkt werden. Sie sind passiv, d.h. sie nehmen nicht mehr aktiv am Piconet teil und haben auch keine der sieben Active Member Addresses (AM_ADDR) mehr, sondern eine Parked Member Address (PM_ADDR) sowie eine Access Request Address (AR_ADDR). Die PM_ADDR wird vom Master genutzt, um einen geparkten Slave wieder aufzuwecken. Die AR_ADDR wird vom geparkten Slave genutzt, um selbst ein „Entparken“ beim Master zu verlangen. Um dies aber zu ermöglichen, bleibt die Synchronisation mit dem Master erhalten. Durch die Nutzung des Park-Zustandes kann ein Piconet aus mehr als sieben Slaves bestehen. Bis zu 255 Bluetooth-Geräte können im Park-Mode mit dem Master vernetzt sein und wie bereits erwähnt bis zu sieben Slaves gleichzeitig aktiv mit dem Master kommunizieren.

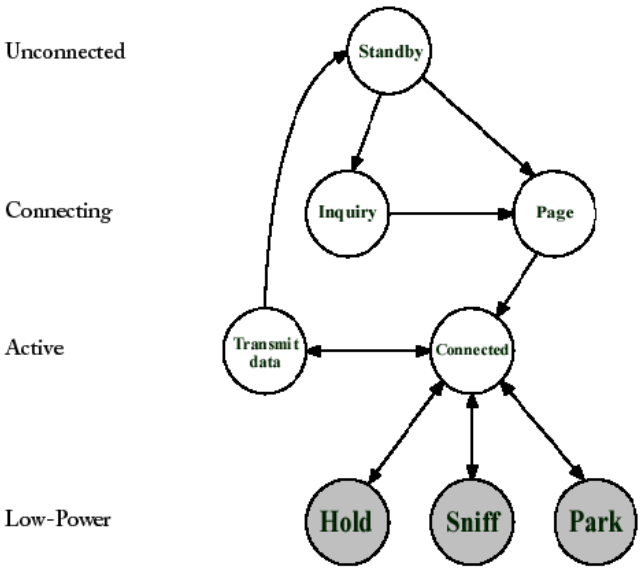


Abbildung 9: Der Kommunikationsablauf

2.4 Host Controller Interface (HCI)

Die Grenze zwischen dem Host-Controller und dem Host verläuft zwischen der LMP- und der L2CAP-Schicht. Um diese zwei Teile des Bluetooth-Protokollstacks in einer Realisierung miteinander in Verbindung zu bringen, wurde das Host Controller Interface definiert, welches eine Befehlsschnittstelle zum Baseband-Controller, Link Manager und zum Zugriff auf den Hardwarestatus und die Steuerregister darstellt. [25], [28]

2.5 Die oberen Schichten

2.5.1 L2CAP (Logical Link Control and Adaptation Protocol)

Das Logical Link Control and Adaptation Protocol verbindet die höherliegenden Schichten des Bluetooth-Protokollstacks mit dem darunter liegenden Baseband. Es empfängt dabei Daten von den höheren Schichten und sendet diese über die darunter liegenden Schichten, d.h., dass die Daten über das Host Controller Interface gesendet werden. Weiterhin besteht die Möglichkeit, dass das L2CAP die Daten direkt zum Link Manager sendet, sofern kein HCI implementiert ist. L2CAP ist zudem für das Multiplexen von Datenströmen höherer Schichten, die Verwaltung von Kommunikationsgruppen und die Segmentierung/Reassemblierung von bis zu 64 KB großen Datenpaketen verantwortlich. L2CAP bietet verbindungsorientierte und verbindungslose Datendienste an, welche beide ausschließlich über ACL-Links realisiert werden. SCO-Links werden nicht unterstützt, da sie primär für Echtzeitsprachübertragung vorgesehen sind. [1], [25], [28], [29]

2.5.2 SDP (Service Discovery Protocol)

Das Service Discovery Protocol setzt auf die Dienste der L2CAP-Schicht auf und dient dem Auffinden von verfügbaren Diensten in einem Bluetooth-Piconet und dem Abfragen der Eigenschaften dieser Dienste. Allerdings beinhaltet das SDP keine Möglichkeit, die gefundenen Dienste zu nutzen bzw. auf diese zuzugreifen. Die Diensterkennung ist innerhalb des Bluetooth-Systems ein wichtiges Element, da sie die Grundlage sämtlicher Einsatzmodelle darstellt. [25], [28]

2.5.3 RFCOMM (Radio Frequency Communications)

Viele Geräte, wie beispielsweise PDAs, Notebooks, Mobiltelefone und Drucker nutzen serielle Schnittstellen zur Kommunikation. Diese weit verbreiteten seriellen Kabel werden durch Bluetooth ersetzt. Um dies erfolgreich zu bewerkstelligen, muss der Protokollstack genau diese seriellen Verbindungen unterstützen. Nur so können bereits vorhandene Applikationen problemlos über Bluetooth arbeiten. Die unteren Protokollschichten unterstützen aber die (RS-232) seriellen Verbindungen nicht.

Aus diesem Grund ist das RFCOMM-Protokoll, welches für eine Emulation des seriellen RS232-Anschlusses über das L2CAP sorgt, im Bluetooth-Protokollstack implementiert. Das in der Spezifikation „Kabelersatzprotokoll“ genannte RFCOMM-

Protokoll basiert auf dem ETSI-Standard TS 07.10, der auch bei GSM Verwendung findet. [21], [25]

2.5.4 Audio

Bei der Betrachtung des Bluetooth-Protokollstacks erkennt man eine Audioschicht, die aber keine ist. Bluetooth Audio definiert nur die möglichen Audioformate für die Umsetzung und Komprimierung der Sprache bzw. Musik. Bekannte Formate wie MP3 oder WAVE sind dabei keine Audiodaten im Sinne von Bluetooth, denn sie werden nicht über einen synchronen Kanal übertragen. Für die Übertragung von Audio und Sprache wird entweder das logarithmische PCM- oder das CVSD-Verfahren verwendet. Die Audiodaten werden über SCO-Links übertragen, von denen gleichzeitig bis zu drei vollduplex zu einem Slave aufgebaut werden können. Wird mehr als nur ein Slave bedient, so können maximal zwei Audioverbindungen aufgebaut werden, d.h. zwei Slaves erhalten jeweils einen Audiokanal. Beim Verbindungsaufbau wird nicht über die L2CAP-Schicht gegangen, sondern die Daten werden nach dem Verbindungsaufbau direkt zwischen den Bluetooth-Geräten übertragen. Bevor jedoch eine SCO-Verbindung aufgebaut werden kann, muss zuerst eine ACL-Verbindung bestehen, da der Link Manager Steuerinformationen für diese Verbindung überträgt. [1], [24], [29]

2.5.5 TCS BIN (Telephony Control Specification Binary)

TCS BIN stellt ein bitorientiertes Protokoll dar, das die Rufsignalisierung zum Aufbau von Sprache und Daten zwischen Bluetooth-Geräten regelt. Es definiert weiterhin Verfahren für das Mobilitätsmanagement für Gruppen von Bluetooth-TCS-Geräten. TCS BIN gründet auf der von ITU-T (International Telecommunication Union) veröffentlichten Regelung Q.931 (die ITU-T-Spezifikation für die grundlegende Rufsteuerung unter ISDN).

2.5.6 AT-Befehle

Zur Realisierung der Telefonsteuerung stehen AT-Befehle zur Verfügung, basierend auf dem ETSI-Standard 07.07 für Mobiltelefone.

2.5.7 Adaptierte Protokolle

Ein Hauptanliegen bei der Entwicklung der Protokolle war eine Wiederverwendung schon bestehender Protokolle. Dadurch sind die Entwickler in der Lage, leichter und schneller schon existierende und neue Anwendungen auf Bluetooth zu adaptieren. „Ältere“ Anwendungen können auf diese Weise mit der drahtlosen Bluetooth-Technologie zusammenarbeiten und reibungslos mit neueren Anwendungen kooperieren, die speziell für Bluetooth-Geräte entwickelt wurden. Weiterhin profitiert Bluetooth von der Tatsache, dass diese Protokolle mittlerweile relativ ausgereift sind. Sie werden teilweise von Bluetooth unverändert übernommen. Bei manchen Protokollen wurde aber eine Anpassung für die speziellen Eigenschaften von Bluetooth durchgeführt.

OBEX (Object Exchange Protocol)

Das Object Exchange Protocol wurde ursprünglich unter der Bezeichnung IrOBEX von der Infrared Data Association (IrDA) entwickelt. OBEX definiert, wie Datenobjekte (z.B. vCard oder vCalendar) dargestellt und ausgetauscht werden können. Im Bluetooth-Protokollstack wird OBEX entweder über das RFCOMM-Protokoll oder über TCP/IP als Transportprotokoll realisiert. In den unteren Schichten des Bluetooth-Protokollstacks wird OBEX über die verbindungsorientierten Protokolle gefahren, weshalb auch nur die verbindungsorientierte Variante von OBEX in Bluetooth Anwendung findet. Anwendungsbeispiele wären der Object-Push von Business-Cards über OBEX, die Synchronisation eines Terminkalenders zwischen zwei Geräten oder die Übertragung von Daten.

vCard und vCalendar sind offene Spezifikationen, die ursprünglich vom Versit Consortium entwickelt und nun vom IMC (Internet Mail Consortium) verwaltet werden. vCard- und vCalendar-Spezifikation sind transport- und plattformunabhängig. vCard ist ein Format für persönliche Informationen (z.B. Telefon- und Adressdaten), wie sie auf Visitenkarten zu finden sind. vCalendar definiert ein Format für den einfachen, automatischen und konsistenten Austausch von Kalender- und Termindaten. [6], [25], [28]

WAP (Wireless Application Protocol)

WAP ist eine Spezifikation zum Senden und Empfangen von Internet-Inhalten für kleine drahtlose Geräte mit Text-Displays (wie etwa Mobiltelefone). WAP eignet sich innerhalb einer Bluetooth-Umgebung sowohl für den Informationstransport als auch für Hidden Computing bestens.

Hinsichtlich des Informationstransports erkennt ein WAP-Client mit der drahtlosen Bluetooth-Technologie die Anwesenheit eines WAP-Servers über das Diensterkennungsprotokoll SDP. Sobald der Dienst erkannt worden ist, wird die Adresse des WAP-Servers ermittelt. Wenn der Client die Adresse erhält, baut er eine Verbindung zum Server auf und greift über das Pull/Push-Verfahren auf die ihm angebotenen Informationen oder Dienste zu.

Mit Hidden Computing ist die Fähigkeit gemeint, von einem mobilen Peer-Gerät aus auf die Funktionen eines Computers zugreifen und diese steuern zu können. Eine Hidden Computing-Anwendung kann ein Flughafen-Schalter oder ein Einkaufszentrum sein, an dem das mobile Gerät nach Informationen suchen, Tickets bestellen oder Waren einkaufen kann.

WAP-Anwendungen werden in der WAE-Umgebung (Wireless Application Environment) entwickelt, die dem Modell für den Transport von Webinhalten weitestgehend folgt, jedoch zusätzlich noch Gateway-Funktionen bietet. [6], [25]

Bei TCP (Transmission Control Protocol), UDP (User Datagram Protocol) und IP (Internet Protocol) und PPP (Point-to-Point-Protocol) handelt es sich um bekannte Internet-Protokolle, die für die Kommunikation im Internet eingesetzt werden. Aus diesem Grund wird hier nicht weiter darauf eingegangen.

3 Die Bluetooth-Profile

Die Bluetooth-SIG hat verschiedene Einsatzmodelle ermittelt, von denen jedes mit einem entsprechenden Profil verknüpft ist. Diese Profile definieren die Protokolle und Eigenschaften, die die bestimmten Einsatzmodelle unterstützen. Grundsätzlich werden nicht alle Protokolle des Bluetooth-Protokollstacks von einem Gerät benötigt, sondern nur die Protokolle, die die benötigte Funktionalität bereitstellen. Wenn eine Eigenschaft implementiert ist, muss sie auf die im entsprechenden Profil spezifizierte Weise implementiert werden, so dass sichergestellt ist, dass sie – unabhängig vom Hersteller – bei allen Geräten auf dieselbe Weise arbeitet. Von Geräten verschiedener Hersteller, die derselben Bluetooth-SIG-Profilspezifikation entsprechen, kann man also eine reibungslose Zusammenarbeit erwarten, wenn diese für diesen spezifischen Dienst und Einsatzweck genutzt werden.

Die Struktur der Profile und deren Abhängigkeiten sind in Abbildung 10 dargestellt. Ein Profil ist von anderen Profilen abhängig, wenn es Teile davon verwendet.

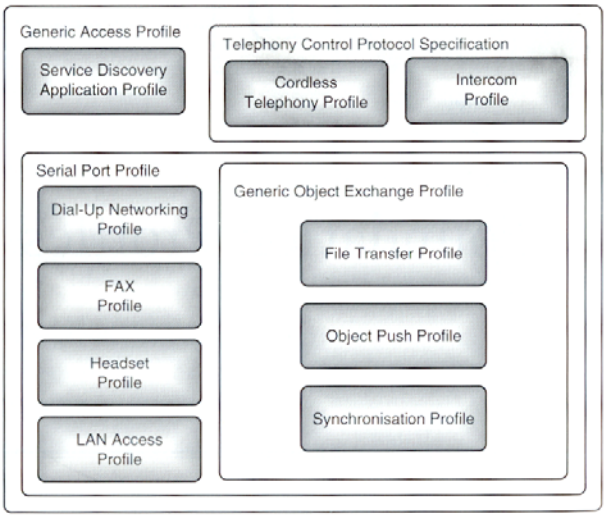


Abbildung 10: Bluetooth-Profile

Zunächst werden die allgemeinen Profile erörtert. Anschließend werden jene Profile vorgestellt, die enger mit den spezifischen Einsatzmodellen in Beziehung stehen. [1], [6], [21], [24], [25], [26]

3.1 Allgemeine Profile

Es gibt vier allgemeine Profile, die in den verschiedenen Einsatzmodellen häufig verwendet werden: das Generic Access Profile, das Serial Port Profile, das Service Discovery Application Profile und das Generic Object Exchange Profile.

Generic Access Profile (GAP)

Das GAP definiert die allgemeinen Prozeduren zur Erkennung der verschiedenen Geräteeinheiten (identities), deren Namen und der grundlegenden Eigenschaften der anderen Bluetooth-Geräte, die erkennbar sind bzw. sich im sogenannten „discoverable mode“ befinden. Wenn sich Geräte in diesem Modus befinden, können sie Verbindung zum Netz aufnehmen und die Dienstanforderungen anderer Geräte empfangen. Außerdem definiert das GAP Prozeduren für das Verbindungsmanagement (link management), die für deren Verbindung untereinander zuständig sind. Der Hauptzweck dieses Profils besteht daher im Einsatz der unteren Schichten des Bluetooth-Protokollstacks (Link Controller und LMP). Darüber hinaus beschreibt das GAP verbindlich das Verhalten von Geräten, die sich im Standby- und Connecting-Status befinden. Dies sorgt wiederum dafür, dass zwischen Bluetooth-Geräten immer Verbindungen aufgebaut und Kanäle eingerichtet werden können. Wenn die Geräte gleichzeitig mehreren Profilen entsprechen, beschreibt das GAP auch die für diesen Fall zuständigen Mechanismen. Im GAP ist zudem der Ablauf der verschiedenen Sicherheitsmaßnahmen festgelegt. Hier werden die höheren Schichten L2CAP, RFCOMM und OBEX einbezogen.

Auch wenn Bluetooth-Geräte keinem anderen Bluetooth-Profil entsprechen, müssen sie zumindest dem GAP entsprechen. Dadurch wird – unabhängig von der Art der Geräte und der von ihnen unterstützten Anwendungen – für die grundlegende Zusammenarbeit und Koexistenz aller Bluetooth-Geräte gesorgt.

Serial Port Profile (SPP)

Soll die Bluetooth-Technologie Kabelverbindungen ersetzen, kommt für diesen verbindungsorientierten Kanal das SPP zum Einsatz. Dieses Profil baut auf dem GAP auf und legt fest, wie sich Bluetooth-Geräte so einrichten lassen, dass sie mit Hilfe von RFCOMM serielle Kabelverbindungen nachbilden können. Wie bereits in Kapitel 2 beschrieben, ist RFCOMM ein einfaches Transportprotokoll, das serielle RS-232-Schnittstellen zwischen zwei Endstellen emuliert. „Erblast“-Anwendungen (legacy applications) können jedoch die Bluetooth-Prozeduren zur Einrichtung einer emulierten seriellen Kabelverbindung nicht kennen. Daher wird auf beiden Seiten der Verbindung die Unterstützung einer Hilfsanwendung benötigt, die die erforderlichen Bluetooth-Befehle kennt.

Das SPP unterstützt maximale Datenraten von 128 kbit/s. Auch wenn die Bluetooth-Spezifikation nur eine einzelne emulierte Verbindung zwischen zwei Geräten über die serielle Schnittstelle in einer Zwei-Punkte-Konfiguration beschreibt, verhindern keinerlei Vorkehrungen eine mehrfache Ausführung des SPP. Daher können auch gleichzeitig mehrere Verbindungen auf einzelnen Geräten unterstützt werden.

Bei einer einfachen Gerätekonfiguration mit seriellen Schnittstellen, bei der beispielsweise zwei Notebooks über ein emuliertes serielles Kabel verbunden werden, ergreift ein Gerät die Initiative, um Verbindung zum anderen Gerät aufzunehmen. Dieses Gerät nennt man Initiator, während man das Zielgerät der Verbindung Akzeptor nennt. Wenn der Initiator mit der Verbindungeinrichtung beginnt, werden Prozeduren zur Diensterkennung ausgeführt, die der Einrichtung der emulierten seriellen Kabelverbindung dienen. SPP legt übrigens keine festen Master/Slave-Rollen fest, da es davon ausgeht, dass beide Geräte gleichberechtigt sind. Die Unterstützung von Sicherheitsmerkmalen ist optional. Bluetooth-Geräte müssen die entsprechenden Sicherheitsprozeduren jedoch unterstützen, wenn sie von einem anderen Gerät angefordert werden.

Service Discovery Application Profile (SDAP)

Das SDAP, welches vom GAP abhängig ist, beschreibt die Eigenschaften und Prozeduren, mit denen sich die in anderen Bluetooth-Geräten registrierten Dienste ermitteln lassen und mit denen Informationen über diese Dienste gewonnen werden können. Das SDAP beinhaltet zudem eine Anwendung, die Service Discovery User Application. Dieses Programm, welches die Lokalisierung der Dienste ermöglicht, wird von allen Bluetooth-Geräten benötigt. Wie beim zuvor besprochenen Profil werden auch beim SDAP nur verbindungsorientierte Kanäle verwendet.

Generic Object Exchange Profile (GOEP)

Das GOEP baut auf dem SPP auf und ermöglicht den Austausch von Objekten zwischen Bluetooth-Geräten. GOEP definiert, wie Bluetooth-Geräte die OBEX-Einsatzmodelle unterstützen, zu denen das File Transfer Profile, das Object Push Profile und das Synchronization Profile zählen.

Die GOEP-Spezifikation sorgt für die allgemeine Zusammenarbeit der Anwendungsprofile, die OBEX-Fähigkeiten (Object Exchange) nutzen, und definiert die Anforderungen der unteren Protokollschichten für die Anwendungsprofile in Bezug auf deren Zusammenwirken. Zu den verbreitesten Geräten, die dieses Profil unterstützen, zählen Bluetooth-fähige Notebooks, PDAs und Mobiltelefone.

3.2 Spezifische Profile für die Einsatzmodelle

Nun zu den Profilen, die enger mit den spezifischen Einsatzmodellen in Beziehung stehen.

Intercom Profile

Das Intercom Profile hängt vom GAP ab. Es unterstützt Nutzungsszenarien mit einer direkten Sprechverbindung zwischen zwei Bluetooth-Geräten wie etwa zwei Mobiltelefonnutzer, die miteinander über eine Bluetooth-Verbindung ein Gespräch führen. Dieser spezielle Modus ist auch als Walkie-Talkie Modus bekannt. Obwohl das Gespräch nichts anderes als eine direkte Sprechverbindung zwischen zwei Telefonen

unter Verwendung der drahtlosen Bluetooth-Technologie ist, wird die Verbindung über die auf der Telefonie gründenden Signalisierung hergestellt. Der dabei eingesetzte Sprach-Codec kann sich entweder PCM oder CVSD bedienen. Sobald ein Terminal mit einem anderen eine Intercom-Verbindung herstellen möchte, laufen verschiedene Interaktionen ab. Falls der Initiator des Intercom-Anrufs nicht über die Bluetooth-Adresse des Akzeptors verfügt, muss er diese zunächst unter Verwendung des im GAP beschriebenen Diensterkennungsverfahrens ermitteln. Das Intercom Profile sieht keinen speziellen Sicherheitsmodus vor – falls der Nutzer eines der Geräte (Initiator bzw. Akzeptor) während der Ausführung dieses Profils einen Sicherheitsmechanismus wünscht, muss daher über das Authentifizierungsverfahren des GAP eine sichere Verbindung aufgebaut werden. Sobald die Intercom-Verbindung aufgebaut ist, ist zwischen beiden Terminalnutzern ein zweiseitiges Sprechen möglich. Sobald einer der beiden Nutzer „auflegt“, ist die Intercom-Verbindung aufgehoben.

Cordless Telephony Profile

Das Cordless Telephony Profile (Schnurlostelefon-Profil) hängt vom GAP ab und definiert die Verfahren und Leistungsmerkmale, die bei Anrufen über eine Basisstation und bei direkten Intercom-Verbindungen zwischen zwei Terminals zur Verfügung stehen. Außerdem ist es für den Zugang zu unterstützenden Diensten des öffentlichen Telefonnetzes hilfreich, da diese Betriebsart es erlaubt, bei Mobiltelefonen die drahtlose Bluetooth-Technologie als Träger mit kleiner Reichweite zum Zugang auf Dienste des öffentlichen Telefonnetzes über eine schnurlose Telefonbasisstation zu nutzen. Das Schnurlostelefon-Profil macht außerdem noch Gebrauch vom Baseband, LMP, L2CAP, SDP und der Telephony Control Specification.

Im folgenden werden vier Profile besprochen, die alle auf dem SPP als auch dem GAP aufbauen.

Dial-up Networking Profile

Das Dial-up Networking Profile (DFÜ-Netzwerk-Profil) definiert die Protokolle und Verfahren, die für den Netzzugang eines Computers per Mobiltelefon oder Modem erforderlich sind.

Fax Profile

Damit auch Faxdienste angeboten werden können, wurde das Fax Profile implementiert. Es stellt die Prozeduren und Protokolle für das Nutzen drahtloser Faxgeräte dar, die zum Senden und Empfangen benötigt werden.

Headset Profile

Das Headset Profile definiert die Protokolle und Verfahren für das Einsatzmodell, welches unter der Bezeichnung „Ultimate Headset“ bekannt ist und von Geräten wie Mobiltelefonen und PCs implementiert werden kann. Es werden also die für die

Kommunikation zwischen einem Audio Headset und einem Audio Gateway nötigen Abläufe definiert.

LAN Access Profile

Das LAN Access Profile definiert, wie Bluetooth-Geräte auf die Dienste eines LANs über RFCOMM mit dem heute üblichen Point-to-Point-Protocol zugreifen können.

Die nächsten drei Profile sind vom SPP und GAP abhängig, benutzen aber das GOEP als Basisprofil.

File Transfer Profile

Das File Transfer Profile unterstützt das Einsatzmodell „File Transfer“, das Möglichkeiten zur Übertragung von Datenobjekten von einem Bluetooth-Gerät zu einem anderen zur Verfügung stellt. Bei diesen Geräten handelt es sich typischerweise um PCs, Smartphones oder PDAs. Zu den Objekttypen zählen u.a. Excel-Tabellen, PowerPoint-Präsentationen, Audiodateien, Bilddateien und Microsoft Word-Dokumente. Dieses Einsatzmodell bietet Teilnehmern auch die Möglichkeit, den Inhalt von Ordnern einzusehen, die sich auf dem entfernten Gerät befinden. Neue Ordner können angelegt und vorhandene gelöscht werden.

Object Push Profile

Das Object Push Profile definiert die Anforderungen an Anwendungen zur Unterstützung des Object Push-Einsatzmodells zwischen Bluetooth-Geräten. Zu den verbreitesten Geräten, die das Object Push-Einsatzmodell nutzen könnten, zählen Notebooks, PDAs und Mobiltelefone. Das Object Push Profile erlaubt es Bluetooth-Geräten, Objekte im Dateneingang eines anderen Bluetooth-Gerätes abzulegen. Bei den Objekten kann es sich um Visitenkarten oder Terminankündigungen handeln.

Synchronization Profile

Das Sychronization Profile definiert die Anforderungen an die Protokolle und Prozeduren, die von Anwendungen verwendet werden, die das Einsatzmodell „Synchronization“ unterstützen. Das Modell sorgt für eine Synchronisation der PIM-Informationen (Personal Information Management) zwischen zwei Geräten. PIM-Informationen umfassen typischerweise Telefonverzeichnisse, Terminkalender, Mitteilungen und Notizen, die von Geräten über ein gemeinsames Protokoll und in einem einheitlichen Format übertragen und verarbeitet werden. Das Einsatzmodell umfasst auch Mobiltelefone oder PDAs, für die PCs automatisch die Synchronisation starten, wenn eines der Geräte in den Funkbereich des Rechners gelangt.

Die Bluetooth-SIG hat sich das Recht vorbehalten, auch nach der Veröffentlichung der Spezifikation neue Profile hinzuzufügen. Bereits in Bluetooth 1.1 sind 13 Profile festgelegt. Sie sind zwar für viele Anwendungen ausgelegt, doch für manche neue unzulänglich. Deshalb kamen eine Reihe weiterer hinzu. Abbildung 11 beinhaltet die neu hinzugekommenen Profile. [6], [21], [26]

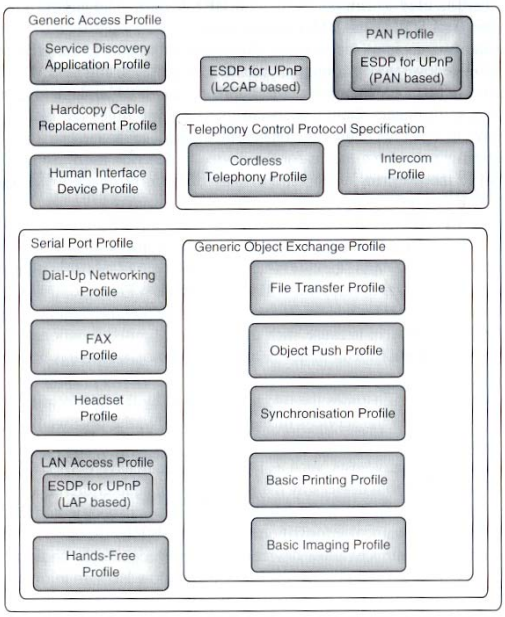


Abbildung 11: Die neuen Bluetooth-Profile

Die neuen Profile lassen sich in drei Gruppen einordnen, je nachdem, ob sie direkt auf GAP, SPP oder GOEP aufsetzen.

Hard Copy Cable Replacement Profile, Human Interface Device Profile und PAN Profile gehören zur *ersten Gruppe.*

Hard Copy Cable Replacement Profile

Das Hard Copy Cable Replacement Profile, das auch die Scanner-Steuerung vorsieht, stellt ein verbessertes Verfahren für Druck-Anwendungen zur Verfügung, das mit weniger Verwaltungsinformation auskommt als das anfangs verwendete SPP.

Human Interface Device Profile (HID-Profile)

Das HID-Profile regelt die Anbindung von schnurlosen Eingabegeräten wie Tastatur oder Maus. Die umständliche Verständigung von PC und Eingabegerät über AT-Befehle gehört damit der Vergangenheit an. Die Kommunikation findet nun wie bei PAN-Geräten unmittelbar über L2CAP statt. Das HID-Profile nutzt wesentliche Teile

des schon für USB spezifizierten Human Interface Device. So können sich Entwickler zum Beispiel auf die bei Windows vorhandenen HID-Treiber stützen. HID nutzt ACL-Verbindungen, für die aber kein QoS spezifiziert ist. Zugesicherte, kurze Latenzzeiten, die für Tastatur- und Mauseingaben unerlässlich sind, sind somit nicht garantiert.

PAN Profile

Eines der gemeinsam vom IEEE und der Bluetooth SIG verfolgten Ziele besteht in der globalen Verwendung drahtloser persönlicher Netzwerke, sogenannter PANs (Personal Area Networks). Das dafür geschaffene PAN Profile ermöglicht das Betreiben von drahtlosen Netzwerkzugangspunkten und das Peer-to-Peer-Networking.

Zur *zweiten Gruppe* gehört das Hands-Free Profile.

Dieses Profil ermöglicht die Nutzung einer Freisprech-Einheit in Verbindung mit einem Audio-Gateway (z.B. Mobiltelefon) in Fahrzeugen. Dabei verständigen sich die Freisprech-Einheit und das Mobiltelefon mittels AT-Kommandos. Für die Sprachübertragung, die beide Seiten jederzeit starten und beenden können, nutzt das Hands-Free Profile SCO-Links. Als Codec wird CVSD eingesetzt.

Basic Printing Profile und Basic Imaging Profile gehören schließlich zur *dritten Gruppe.*

Basic Printing Profile

Das Basic Printing Profile ist für Druckanwendungen speziell für PDAs und Mobiltelefone gedacht, also zum Ausdrucken etwa von Emails oder SMS-Nachrichten.

Basic Imaging Profile

Weder SPP noch Hardcopy Cable Replacement Profile oder Basic Printing Profile berücksichtigen jedoch die Anforderungen von Digitalkameras. Dafür wurde eigens das Basic Imaging Profile konzipiert. Es befördert Bilder, zum Beispiel im jpeg-Format, von einer Digitalkamera zum PC oder Drucker.

Eine besondere Rolle nimmt schließlich das ESDP (Enhanced Service Discovery Profile) ein. Anders als das SDAP soll es die Dienstabfrage und Diensterkennung auf Basis des Universal Plug and Play (UPnP) ausführen. Es sind drei Wege für die Implementierung vorgesehen, einer über die L2CAP-Schicht und je einer über die „Vernetzungs-Profile“ PAN und LAP. ESDP taucht deshalb in Abbildung 11 an drei verschiedenen Stellen auf.

3.3 Beispiele für Einsatzmodelle

In diesem Abschnitt werden abschließend drei Einsatzmodelle (inkl. des erforderlichen Protokollstacks) vorgestellt. [19], [24]

Das drei-in-einem-Telefon

Ein sehr nützliches Einsatzmodell ist das sogenannte drei-in-einem-Telefon. Oft hat man drei verschiedene Telefone: ein Geschäftstelefon im Büro, ein Telefon zu Hause und ein Mobiltelefon für unterwegs. Bluetooth ermöglicht deren Integration in ein einziges Telefon. Unterwegs kann über das Mobilfunknetz, wie mit jedem anderen Mobiltelefon auch, telefoniert werden. Über Sprachzugangspunkte kann mit demselben Gerät im Büro oder zu Hause telefoniert werden. Eine weitere Funktionalität ist der sogenannte Walkie-Talkie-Betrieb. Dadurch ist eine direkte Kommunikation zwischen zwei Geräten möglich. Es wird dafür kein Zugangsnetz benötigt und es fallen somit auch keine Gebühren an. Die begrenzte Reichweite ist hier die größte Einschränkung. Abbildung 12 zeigt den Protokollaufbau für das drei-in-einem-Telefon.

Automatische Dateisynchronisation

Im heutigen Alltag ist es üblich, mehrere mobile Geräte zu nutzen. Die auf diesen Geräten gespeicherten Daten reichen von Telefonnummern bis zu täglichen Terminen. Unter einer Dateisynchronisation versteht man in diesem Zusammenhang das Synchronisieren der verschiedenen Informationen auf allen Geräten. Bis jetzt benötigte man ein spezielles Kabel oder bei einer Infrarot-Schnittstelle Sichtkontakt. Außerdem erfolgte die Aktualisierung nicht immer automatisch. Bei der automatischen Dateisynchronisation von Bluetooth dagegen, werden die einzelnen Datenbanken nach der Bildung eines Ad-hoc-Netzwerkes automatisch synchronisiert, ohne dass dies mit Aufwand verbunden ist. Abbildung 13 illustriert den Protokollaufbau für das Einsatzmodell „Dateisynchronisation“.

Internetanbindung

Es ist möglich, einen PC über Bluetooth mit dem Internet zu verbinden. Dazu wird ein Mobiltelefon oder schnurloses Modem benötigt. Die sogenannte Internetbrücke kann auch zum Versenden von Faxen benutzt werden, ohne dass eine physikalische Kabelverbindung zum Netz besteht. Den Aufbau der Protokollarchitektur zeigt Abbildung 14. Dabei ist zu beachten, dass zusätzlich zum SDP noch zwei weitere Protokollverbindungen benötigt werden, um mittels AT-Befehlen das Mobiltelefon oder Modem zu steuern und über PPP und RFCOMM die Nutzdaten zu transportieren. Beim Versenden von Faxen wird das PPP umgangen, um die Daten direkt über RFCOMM zum Empfänger zu schicken.

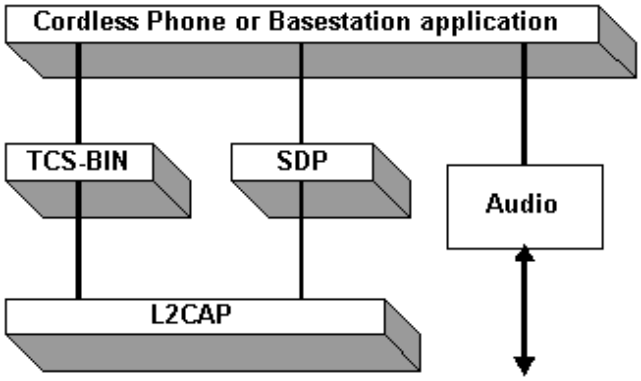


Abbildung 12: Protokollaufbau für das 3-in-1-Telefon

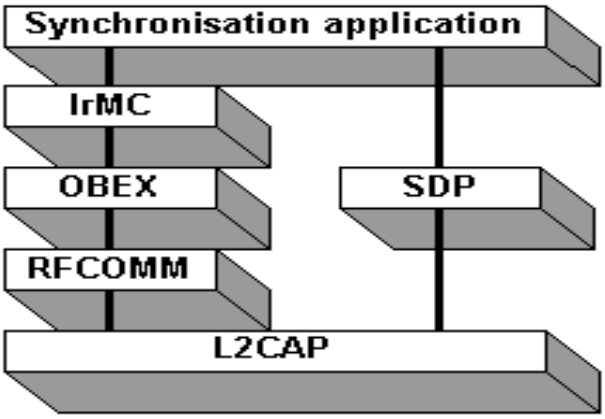


Abbildung 13: Protokollaufbau für die Dateisynchronisation

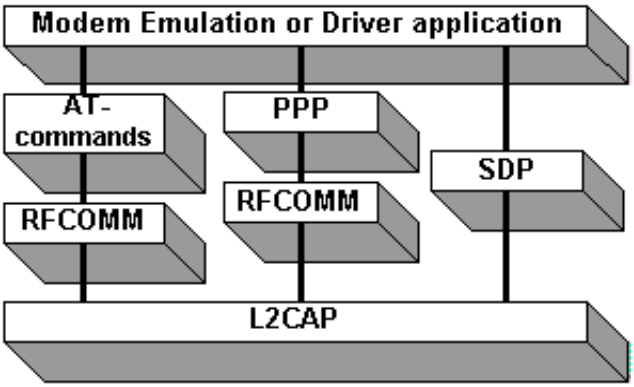


Abbildung 14: Protokollaufbau für Internetanbindung und Fax

4 Bluetooth-Sicherheit

Da Bluetooth ein funkbasiertes Verfahren ist, lassen sich Bluetooth-Signale wie andere Funksignale leicht abhören. Daher sind bestimmte Sicherheitsmechanismen erforderlich, die Lauschangriffen entgegenwirken. Zusätzlich zur begrenzten Reichweite und der Verwendung des Frequenzsprungverfahrens, welches schon von Haus aus das Abfangen von Signalen extrem schwierig macht, sieht die Bluetooth-Spezifikation deshalb auch Funktionen auf der Verbindungsebene wie die Authentifizierung und Verschlüsselung vor.

4.1 Sicherheitsmodi

Da es unterschiedliche Anforderungen an die Datensicherheit gibt, müssen Anwendungen und Geräte über größere Flexibilität beim Einsatz der Sicherheitsvorkehrungen der Sicherungsschicht verfügen. Um diese Anforderungen erfüllen zu können, definiert die Spezifikation im Generic Access Profile drei Sicherheitsmodi, die sich für verschiedene Funktionalitäten und Anwendungen der Geräte eignen. [6], [7], [11], [13]

- Im **Modus 1** (non-secure) werden keine speziellen Sicherheitsmaßnahmen genutzt. Somit ist er für die Übertragung sicherheitsrelevanter Daten nicht zu empfehlen. Der automatische Austausch von Visitenkarten und Terminkalendern (vCard, VCalendar) sind typische Beispiele für die Datenübertragung ohne Sicherheitsvorkehrung.

- Befindet sich ein Bluetooth-Gerät im **Modus 2** (service level enforced security), so werden erste Sicherheitsmaßnahmen erst nach dem erfolgreichen Verbindungsaufbau durchgeführt. Welche Schritte danach ergriffen werden, hängt von dem angeforderten Kanal oder Dienst ab. Die höherliegenden Übertragungsprotokolle oder die Anwendungen selbst sind dabei für die Authentifizierung und Verschlüsselung zuständig.

- Sollen bereits vor dem Verbindungsaufbau Schritte zur Verbesserung der Sicherheit unternommen werden, so muss sich das Bluetooth-Gerät im **Modus 3** (link level enforced security) befinden. Die Sicherheitsfunktionen sind auf der Verbindungsschicht realisiert und zum Großteil bereits in der Firmware des jeweiligen Bluetooth-Geräts implementiert. Auf der Verbindungssschicht bietet der Bluetooth-Standard zwei Sicherheitsdienste: eine kryptographische Authentifizierung sowie die Verschlüsselung der übertragenen Nutzdaten. Die Authentifizierung ist in Modus 3 Bestandteil des Verbindungsaufbaus; die Verschlüsselung ist dagegen nur optional.

Bevor in Abschnitt 4.3 genauer auf die Authentifizierung sowie die Verschlüsselung eingegangen wird, erfolgt eine kurze Beschreibung der dabei verwendeten Schlüssel.

4.2 Schlüssel-Management

Alle Sicherheitsmaßnahmen zwischen zwei oder mehreren Bluetooth-Geräten basieren auf dem Verbindungsschlüssel (Link Key). Dieser ist eine 128 Bit große Zufallszahl, die in der Authentifizierung und als Parameter zur Bildung des bei der Verschlüsselung verwendeten Chiffrierschlüssels (Encryption Key) benutzt wird.
In der Spezifikation werden vier Arten von Verbindungsschlüsseln definiert. [7], [13], [24]

Wenn zwei Bluetooth-Geräte Sicherheitsmechanismen nutzen wollen, müssen sie zuvor miteinander „gepaart" werden. In der Regel wird dabei ein nur für die Verbindung dieser beiden Geräte genutzter, 128 Bit langer **Kombinationsschlüssel** (Combination Key) aus den beiden (48 Bit langen) Geräteadressen und einer Zufallszahl je Gerät erzeugt und in beiden Geräten für die zukünftige Nutzung als Verbindungsschlüssel gespeichert.

Für die gesicherte Übertragung der Zufallszahlen wird ein **Initialisierungsschlüssel** (Initialization Key) verwendet, der sich aus einer weiteren Zufallszahl, einer (1 bis 16 Byte langen) PIN (Personal Identification Number) und der Geräteadresse des Claimant (Antragsteller) berechnet. Dazu muss in beide Geräte die gleiche PIN eingegeben werden.

Der **Geräteschlüssel** (Unit Key) wird bei der erstmaligen Verwendung eines Bluetooth-Gerätes erzeugt und normalerweise nicht mehr geändert. Geräteschlüssel werden beispielsweise verwendet, wenn ein Gerät nicht genügend Speicherplatz für weitere Schlüssel besitzt. Für ein Bluetooth-Gerät sind der Geräteschlüssel und der Kombinationsschlüssel funktionell nicht zu unterscheiden. Der Unterschied besteht nur in der Weise, wie sie generiert werden. Der Geräteschlüssel ist für ein bestimmtes Gerät festgelegt und wird intern erzeugt. Der Kombinationsschlüssel wird dagegen durch die Informationen zweier Geräte erzeugt und ist für diese festgelegt. Jede andere Kombination von Geräten hat auch ihren eigenen Kombinationsschlüssel.

Der **Master-Schlüssel** (Master Key, auch Temporärschlüssel genannt) kann für die Dauer einer Bluetooth-Sitzung zwischen mehreren Geräten (temporär) vereinbart werden, d.h. er ersetzt kurzzeitig den derzeit aktiven Verbindungsschlüssel. Dies wird beispielsweise dann verwendet, wenn ein Master mehrere Geräte unter Verwendung desselben Chiffrierschlüssels erreichen möchte.

4.3 Sicherheitsmechanismen

Sind zwei Geräte nun erfolgreich „gepaart" worden, d.h. beide Geräte haben in der Initialisierungsphase einen gemeinsamen Verbindungsschlüssel erzeugt und vereinbart, so können sie die beiden folgenden kryptographischen Sicherheitsmechanismen von Bluetooth nutzen. [6], [7], [13], [24], [29]

Authentifizierung

Mit einer Authentifizierung wird der unerwünschte Zugriff auf kritische Daten und Funktionen verhindert. Die Sicherheitsarchitektur der Bluetooth-Spezifikation authentifiziert nur Geräte, nicht aber Anwender. Ein ausgewiesenes Gerät kann also gestohlen oder ausgeliehen werden und sich dabei immer noch wie ein Gerät verhalten, das

sich noch in der Hand des rechtmäßigen Besitzers befindet. Falls zusätzliche Authentifizierungsprozeduren für Benutzer notwendig werden, kann dies über entsprechende Sicherheitsverfahren auf der Anwendungsebene realisiert werden, etwa für E-Commerce-Anwendungen über die Eingabe eines Benutzernamens und Passworts.

Für jede Verbindung kann eine einseitige Authentifizierung mit Hilfe des Challenge-Response-Verfahrens angefordert werden (Algorithmus SAFER+ mit einer Schlüssellänge von 128 Bit). Sollen sich beide Geräte gegenseitig authentifizieren, so wird die einseitige Authentifizierung durchgeführt und anschließend mit vertauschten Rollen wiederholt.

Die einseitige Authentifizierung, d.h. ein Gerät (Claimant) authentifiziert sich gegenüber einem anderen Gerät (Verifier), läuft wie folgt ab (vgl. Abbildung 15):

Der Claimant bekommt vom Verifier eine Zufallszahl (au_rand) überreicht und durch das Wissen eines Verbindungsschlüssels (Key) und seiner eigenen Geräteadresse (Master BD_ADDR) ist es ihm möglich, daraus einen 32 Bit langen Code (sres) zu erzeugen. Dabei berechnet er gleichzeitig einen 96 Bit langen sog. Authenticated Cipher Offset (ACO), der in beiden Geräten gespeichert und geheim gehalten wird. (ACO wird später zur Generierung des Chiffrierschlüssels für die Verschlüsselung benötigt). Anschließend wird sres an den Verifier geschickt, der ihn dann mit dem von ihm erzeugten Code vergleicht. Er benutzt dazu denselben Crypto-Algorithmus (E1) und dieselben Angaben. Sind beide identisch, so wird der Claimant bei ihm als authentifiziert registriert, ansonsten wird jegliche weitere Aktion verweigert.

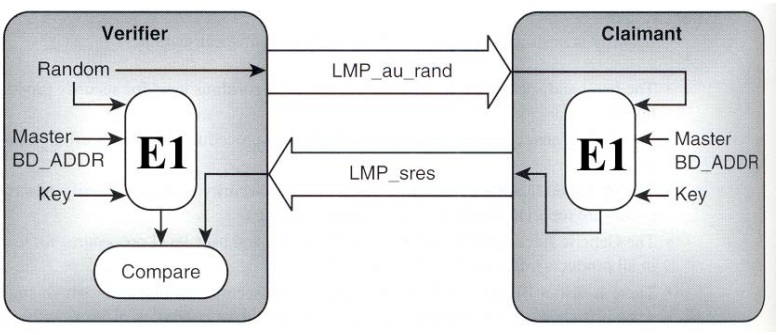


Abbildung 15: Ablauf der Authentifizierung

Verschlüsselung

Mit der Verschlüsselung werden die Daten während der Übertragung unkenntlich gemacht und damit das Abhören verhindert. Wurde die Authentifizierung in mindestens eine Richtung erfolgreich abgeschlossen, so kann (optional) mit der Verschlüsselung begonnen werden. Dabei können Schlüssellängen von 8 bis 128 Bit (in Vielfachen von 8) eingesetzt werden. Verschlüsselt wird grundsätzlich nur der Payload. Die Verschlüsselung kann sowohl vom Master, als auch vom Slave beantragt werden; sie wird jedoch immer vom Master gestartet, nachdem er die notwendigen Parameter mit dem Slave ausgehandelt hat. Dazu einigen sich die beiden Geräte zunächst auf die Länge des zu verwendenden Schlüssels.

Anschließend startet der Master die Verschlüsselung, indem er eine Zufallszahl (EN_RAND_A) an den Slave sendet (vgl Abbildung 16). Zum Verschlüsseln wird ein Stream Cipher (E_0) eingesetzt, der aus drei Komponenten besteht. Für jedes Datenpaket wird er aus der Geräteadresse des Masters (BD_ADDR_A) und dessen Zeittakt ($clock_A$), sowie einem Chiffrierschlüssel (K_C) erzeugt.

Dieser Chiffrierschlüssel berechnet sich bei Punkt-zu-Punkt-Verschlüsselung aus dem aktuellen Verbindungsschlüssel, dem bei der Authentifizierung erstellten ACO und der vom Master an den Slave gesendeten Zufallszahl EN_RAND_A. Bei Punkt-zu-Mehrpunkt-Verschlüsselung wird dagegen die Geräteadresse des Masters (BD_ADDR_A) als Cipher Offset verwendet. Außerdem muss der Verbindungsschlüssel durch einen Master-Schlüssel ersetzt werden, bevor mit der Verschlüsselung begonnen wird.

Durch eine XOR-Verknüpfung der Daten und des Schlüsselstroms K_{Cipher} wird ein verschlüsselter Datenstrom erzeugt. Verschlüsselt sind die Daten aber nur während des Transports per Funk. Vor der Aussendung bzw. nach dem Empfang liegen die Daten in den beteiligten Geräten unverschlüsselt vor.

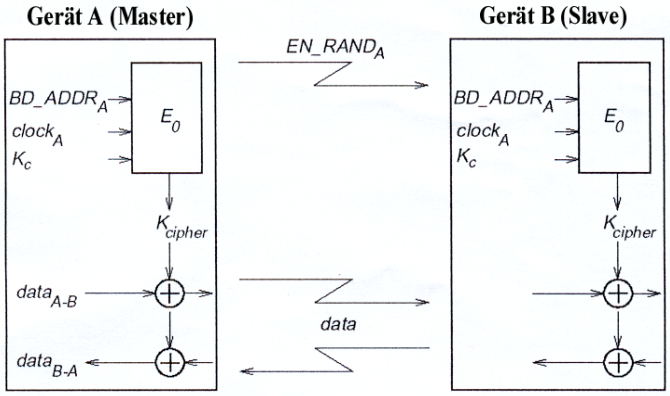


Abbildung 16: Ablauf der Verschlüsselung

4.4 Wie sicher ist Bluetooth? - Schwächen im Sicherheitskonzept

Im folgenden werden einige Schwächen im Sicherheitskonzept von Bluetooth kurz beschrieben. Wie sicher Bluetooth ist, hängt bis zu einem gewissen Punkt auch vom Benutzer bzw. Hersteller eines Geräts ab (optionale Sicherheitseinstellungen). [7], [13], [15]

- **Verschlüsselung ist nicht grundsätzlich vorgeschrieben**

Unabhängig vom verwendeten Sicherheitsmodus ist die Verschlüsselung der übertragenen Daten optional und muss von den Anwendungen explizit beantragt werden.

- **Die PIN als unzuverlässiger Sicherheitsparameter**

Die PIN als einzig geheimen Parameter bei der Verbindungsschlüsselerzeugung ist als sicherheitskritisch anzusehen. Wird bei der Gerätepaarung eine „schwache“ PIN verwendet, kann ein Angreifer die PIN erraten und damit den aus der Paarung resultierenden Verbindungsschlüssel berechnen. Dazu muss er nur die Paarung und die folgende Authentifizierung abhören. Anhand der Aufzeichnungen der abgehörten Protokolle kann der Angreifer überprüfen, ob die PIN vom ihm korrekt erraten wurde.

- **Geräteschlüssel sind unsicher**

Werden Geräteschlüssel von einem Gerät als Verbindungsschlüssel verwendet, so wird für jede Verbindung mit diesem Gerät immer der gleiche Schlüssel benutzt. Gelingt es dem Angreifer eine Verbindung mit diesem Gerät aufzubauen, ist er anschließend in der Lage, sich als dieses Gerät auszugeben oder jede Kommunikation mit diesem Gerät abzuhören.

- **Qualität des Zufallsgenerators**

Zur Zufallserzeugung sind im Bluetooth-Standard keine Mechanismen festgelegt worden, d.h. es wurden keine Algorithmen vorgeschrieben oder spezifiziert. Die Güte der Zufallsgeneratoren variiert folglich hersteller- und implementierungsabhängig.

- **Nur Geräte-Authentifizierung**

Authentifizieren muss sich bei Bluetooth nur das Gerät, in der Regel aber nicht der Benutzer gegenüber dem Gerät. Bei Abhandenkommen mobiler, gepaarter Geräte sind diese also ohne weiteres durch unbefugte Dritte nutzbar.

- **Unsichere Voreinstellungen sind nicht grundsätzlich ausgeschlossen**

Voreinstellungen sind von Seiten des Herstellers oft unsicher konfiguriert. Sicherheitsfunktionen wie Authentifizierung und Verschlüsselung sind häufig abgeschaltet und PINs auf „0000“ eingestellt.

Die genannten Punkte verdeutlichen, dass Bluetooth bzgl. der Sicherheit an einigen Stellen durchaus verbessert werden kann. Bluetooth ist aber für kleine Ad-hoc-Netzwerke oder den Austausch von nicht-sicherheitsrelevanten Daten ausreichend sicher. Wer größtmögliche Sicherheit haben möchte, kann auf Sicherheitsmechanismen in der Anwendungsschicht zurückgreifen (Benutzername, Passwort etc.).

5 Vergleich zu konkurrierenden Technologien

Bluetooth erweist sich zwar in vielen Bereichen als eine sehr bequeme, preiswerte und einfache Lösung Daten (auch größere Mengen) drahtlos über kurze Distanzen hinweg zu übertragen. Jedoch ist diese Technologie auf dem Markt nicht allein vorherrschend. Infrarot (IrDA), WLAN und eine neuartige Technologie zur drahtlosen Datenübertragung, genannt ZigBee, treten mit Bluetooth in Konkurrenz. ZigBee glänzt mit einem geringen Stromverbrauch und einer bis zu zehnmal größeren Übertragungsreichweite. WLAN bietet die Übertragung großer Datenmengen über mehrere 100 Meter und mit IrDA existiert bereits seit 1994 ein Standard, der den kabellosen Austausch von Daten ermöglicht. Da fällt es Bluetooth natürlich nicht einfach als Marktführer hervorzugehen. Hinzu kommt, dass ZigBee und WLAN die gleichen Frequenzbänder wie Bluetooth verwenden und so gegenseitige Störungen nicht auszuschließen sind.

Im folgenden werden die Unterschiede, sowie Vor- und Nachteile der konkurrierenden Technologien aufgezeigt und eventuell auftretende Störungen mit in Betracht gezogen.

5.1 IrDA

5.1.1 Was ist IrDA?

Der Infrarot-Standard IrDA wurde von der Infrared Data Association entwickelt. IrDA wird für kurzstreckige Punkt-zu-Punkt-Verbindungen zum Austausch von Daten oder Synchronisieren von Dateien eingesetzt und bietet eine Übertragungsrate von bis zu 16 Mbit/s bei einer Reichweite von etwa einem Meter. Dabei muss eine direkte Sichtverbindung zwischen den kommunizierenden Geräten hergestellt werden und der Sichtwinkel darf 30° nicht überschreiten. Die Vorteile der Infrarottechnik sind die einfachen und sehr günstigen Sender und Empfänger, die heutzutage in praktisch allen mobilen Geräten integriert sind und der geringe Energieverbrauch. Die meisten dieser Geräte folgen dem IrDA 2000-Standard. Weiterhin können andere elektrische Geräte die Infrarotübertragung nicht stören. Die Übertragung reagiert jedoch empfindlich auf Umgebungslicht und reflektierende Gegenstände. So sinkt die Reichweite bei direkter Sonneneinstrahlung auf ca. 10 cm.

Die Zusammenarbeit zwischen der Infrared Data Association und der SIG zeigt, dass der Auftritt von Bluetooth nicht den Untergang der IrDA-Technologie bedeuten wird. Eine der grundlegendsten Funktionen der beiden Standards ist der Austausch von Daten wie beispielsweise die Synchronisation der persönlichen Informationen eines PDA mit einem PC. Dafür setzen beide dasselbe Protokoll OBEX ein. Auf diese Weise kann eine Anwendung sowohl über IrDA als auch über Bluetooth ablaufen. Tabelle 3 zeigt einen Vergleich von IrDA und Bluetooth. [6], [12], [17]

	IrDA	Bluetooth
Verbindungsart	Point-to-Point	Point-to-Point, Point-to-Multipoint
Datenübertragungsrate	bis zu 16 Mbit/s	max. 1 Mbit/s
Übermittlungsdistanz	max. 1,2 m, Sichtkontakt	~10 m, ohne Sichtkontakt
Übertragungsumkreis	30°-Winkel	omnidirektional
Anzahl unterstützter Geräte	2	8 pro Piconet
Sicherheitsfeatures auf	Softwareebene	Hardwareebene
Bidirektionalität	symmetrisch	symmetrisch und asymmetrisch
Daten und Sprache ?	nur Daten	Daten und Sprache

Tabelle 3: IrDA und Bluetooth im Vergleich

5.1.2 Infrarot oder Bluetooth? – Geeignete Einsatzgebiete

Welche Technologie ist nun die bessere? Anhand zweier Szenarien soll gezeigt werden, dass immer dort, wo die Infrarotlösung von Nachteil ist, Bluetooth-Geräte durch ihre Vorzüge glänzen und umgekehrt. [25]

Austausch von Visitenkarten zwischen zwei Geräten

Diese Art von Anwendung findet typischerweise in einem Besprechungsraum statt, in dem sich eine Reihe von Geräten befinden, die alle dieselbe Funktion auszuführen versuchen. In einer solchen Situation ist Infrarot die bessere Lösung. Beim Austausch von Visitenkarten ist es normal, dass sich die Personen nahe beieinander befinden, was die Ausrichtung zweier Geräte aufeinander begünstigt. Die begrenzte Reichweite und der schmale Winkel von Infrarot ermöglicht es den Anwendern, auf sichere Weise und ohne gegenseitige Störungen gleichartige Aktivitäten durchzuführen.

Ein Bluetooth-Gerät würde sich in einer solchen Situation nicht wie ein Infrarot-Gerät verhalten. Da es omnidirektional abstrahlt, müsste ein Bluetooth-Gerät erst einmal den richtigen Empfänger ausfindig machen. Der Anwender kann nicht einfach auf den Empfänger zielen, sondern das Bluetooth-Gerät müsste zunächst einmal eine Suchoperation ausführen, deren Ergebnis vermutlich mehrere andere Bluetooth-Geräte wären, die sich in Reichweite befinden. Der Anwender ist daher gezwungen, unter mehreren entdeckten Geräten auszuwählen und ein Sicherheitsverfahren anzuwenden, welches unberechtigte Zugriffe verhindert. All diese Faktoren würden den Einsatz von Bluetooth-Geräten für den Visitenkartenaustausch zu einer mühsamen und unnötig zeitraubenden Angelegenheit machen.

Datensynchronisation zwischen Mobiltelefon und Notebook

Mit Bluetooth kann man beispielsweise das Mobiltelefon mit dem Notebook synchronisieren. So ist es möglich, eine am Notebook neu eingegebene Adresse direkt in das Telefonbuch des Mobiltelefons zu übertragen, ohne dieses aus der Jacke oder Tasche hervorholen zu müssen. Die Verwendung von Produkten mit der drahtlosen Bluetooth-Technologie für die Synchronisation setzt nicht voraus, dass sich das Telefon an einer bestimmten, immer gleichen Stelle befindet. Die Synchronisation kann auch stattfinden, während man mit dem Telefon in der Jackentasche umherwandert, sofern sich das Mobiltelefon und das Notebook innerhalb einer Reichweite von zehn Metern befinden.

Mit Infrarot wäre dies nicht möglich, da das Signal keine festen Objekte durchdringen kann. Außerdem müssen sich die Geräte innerhalb einer Reichweite von einem Meter befinden. Darüber hinaus erfordert die Verwendung von Infrarot, dass beide Geräte während der Synchronisation stationär verbleiben.

Aufgrund der aufgezeigten Stärken und Schwächen beider Technologien wird Bluetooth eher eine Ergänzung in der Nahbereichskommunikation als eine Konkurrenztechnologie zu IrDA darstellen.

5.2 ZigBee

Im Oktober 2002 wurde die ZigBee Allianz, ein Zusammenschluss von Halbleiterherstellern, Entwicklern und Anwendern, derzeit bestehend aus 50 Mitgliedern, gegründet. Dazu gehören Firmen, wie Bosch, France Telecom, Motorola, Mitsubishi, Honeywell, Philips oder Samsung. Der Standard baut auf der IEEE-Spezifikation 802.15.4 auf.

Die Technologie soll im lizenzfreien ISM 2,4 GHz-Band, im europäischen 868 MHz-Band und im US-amerikanischen 915 MHz ISM arbeiten. Dabei erreicht ZigBee im 2,4 GHz-Band eine Übertragungsgeschwindigkeit von bis zu 250 kbit/s, in den niedrigen Frequenzbändern 20 bzw. 40 kbit/s. Die maximale Übertragungsrate bei Bluetooth beträgt im 2,4 GHz-Band 1 Mbit/s. ZigBee besitzt die Fähigkeit, automatisch nach freien Frequenzkanälen zu suchen. Der Zugriff auf den Funkkanal erfolgt über ein zufalls- bzw. zeitschlitzgesteuertes CSMA/CA-Verfahren.

Wesentliche Merkmale dieser Technologie sind vor allem die geringen Kosten in der Herstellung sowie der minimale Stromverbrauch der Geräte. Die kurzen Aktivierungszeiten, als auch der häufige Stand-by-Betrieb ermöglichen einen sehr niedrigen Energieverbrauch, so dass ein batteriebetriebenes Gerät bis zu 2 Jahre funktionstüchtig bleiben kann. Der Standard zielt auf eine hohe Übertragungssicherheit durch hohe Redundanz und dynamische Kanalwahl. IEEE entwickelt gerade mögliche Verschlüsselungstechniken, die vor dem unbefugten Zugriff auf gesendete Daten schützen sollen.

Das Adressierungsschema von ZigBee bietet in einem Master-Slave-Netz bis zu 254 Netzknoten, wohingegen Bluetooth eine Einschränkung auf nur 7 aktive Slaves findet. ZigBee hat eine Sendereichweite von 30 bis 100 Meter, Bluetooth dagegen sendet in der Basisversion nur bis zu 10 Meter.

Obwohl beide Technologien das 2,4 GHz Frequenzband nutzen, treten kaum Interferenzen auf. Die Arbeitszyklen in ZigBee-Netzen sind kürzer und durch den überwie-

genden Stand-by-Betrieb auch seltener als bei Bluetooth. Die Wahrscheinlichkeit eine Bluetooth-Übertragung zu stören ist somit relativ gering. Beeinflusst umgekehrt ein Bluetooth-Datentransfer ein ZigBee-Netz, so werden die zerstörten Datenpakete erneut gesendet.

Anwendung findet ZigBee in vielen Bereichen. Möglich ist z.B. der Einsatz in Türöffnern oder Notrufsystemen für ältere oder behinderte Menschen, in Feuermeldern, Stereoanlagen, Fernsehern und Videorecordern, sowie in Universal-Fernbedienungen, mit der TV-Geräte und Stereoanlagen bedient werden können. In der Gebäudeautomatisierung kann es zur Fernsteuerung von Lampen oder Jalousien als auch im Security-Bereich wie beispielsweise in Rauchmeldern, Schadstoffdetektoren und Alarmanlagen angewendet werden. Besonders eignen soll sich die Funktechnik in Fabriken für Kontrollfunktionen mit geringen Datenmengen und für Telemetrie-Applikationen, wie Fernüberwachung durch automatische Übertragung von Messwerten. Geplant sind auch Funkschnittstellen etwa für intelligente Haushaltsgeräte und die Ersetzung teurer Vernetzungen von Industrieanlagen. [8], [14], [22]

In Tabelle 4 wird ein Vergleich der beiden Funktechnologien dargestellt.

	ZigBee	**Bluetooth**
Frequenzbereich	2,4 GHz	2,4 GHz
Maximale Datenrate	250 kbit/s	1 Mbit/s
Übertragungsreichweite	30 bis 100 m	nur bis zu 10 m (Standardversion)
Anzahl unterstützter Geräte	bis zu 254 aktive Slaves	bis zu 7 aktive Slaves
Stromverbrauch (im Schlafmodus)	wenige Mikroampere	100 Mikroampere

Tabelle 4: ZigBee und Bluetooth im Vergleich

5.3 WLAN

5.3.1 Allgemeines

WLAN steht für Wireless Local Area Network und basiert auf dem vom Institute of Electronic and Electrical Engineers (IEEE) definierten IEEE Standard 802.11, welcher zum Standard 802.11b erweitert wurde.

WLAN arbeitet wie Bluetooth im 2,4 GHz ISM-Band. Diese Technologie bietet die Möglichkeit mit geringem Aufwand drahtlose Netzwerke aufzubauen oder bestehende drahtgebundene Netzwerke zu erweitern.

Aufgrund der einfachen Installation werden Funk-LANs auch für temporär zu installierende Netze, wie z.B. auf Messen verwendet. Weitere Einsatzmöglichkeiten bieten sich an öffentlichen Plätzen wie Flughäfen oder Bahnhöfen, wo sogenannte Hot Spots angeboten werden können, um mobilen Benutzern Verbindungen in das Internet oder in ihr Home-Office zu ermöglichen.

Die maximale Datenrate beträgt beim 802.11 2 Mbit/s, beim 802.11b 11 Mbit/s. Der Standard unterstützt zwei unterschiedliche Funkverfahren. Das Direct-Sequence-Spread-Spectrum- und das auch bei Bluetooth verwendete Frequency-Hopping-

Spread-Spectrum-Verfahren. In Tabelle 5 wird der IEEE 802.11 Standard mit Bluetooth verglichen. [8], [23]

Wir möchten an dieser Stelle auf die Ausarbeitung „IEEE 802.11“ von Uli Bareth und Matthias Röckl verweisen, in der ausführlichere Informationen zu finden sind.

	IEEE 802.11 Standard	**Bluetooth**
Frequenzbereich	2.4 GHz (802.11, 802.11b), 5 GHz (802.11a)	2.4 GHz
Physikalische Ebene	FHSS oder DSSS (802.11), DSSS (802.11b), OFDM (802.11a)	FHSS
Maximale Datenrate auf physikalischer Ebene	2 Mbps (802.11), 11 Mbps (802.11b), 54 Mbps (802.11a)	1 Mbps
Verschlüsselung	Ja	Ja
Medienzugriff	CSMA/CA	TDMA/TDD
Verbindungen	verbindungslos	verbindungsorientiert und verbindungslos
Unterstützung zeitkritischer Anwendungen	Optional durch die CFP	Durch SCO
Jahr der Veröffentlichung	1997 (802.11) 1999 (802.11a) 1999 (802.11b) (DRAFT)	1999

Tabelle 5: WLAN und Bluetooth im Vergleich

5.3.2 Interferenzen zwischen Bluetooth und WLAN

Das Problem der gegenseitigen Störung von Bluetooth und WLAN tritt auf, da beide Funktechnologien ihre Signale im identischen 2,4-GHz-Band übertragen. Die Koexistenz von Bluetooth und WLAN bringt Einbrüche in der Übertragungsleistung.

Simulationen und Messungen ergaben, dass insbesondere der Durchsatz einer WLAN-Verbindung drastisch einbrechen kann, wenn in unmittelbarer Nähe ein Bluetooth-Netz betrieben wird. Dabei kann eine 11 Mbit/s WLAN-Verbindung schnell auf eine Datenrate von 1 Mbit/s zurückgehen. Die Folge ist dann eine längere Übertragungszeit und damit verbunden eine noch größere Störanfälligkeit gegenüber Bluetooth-Signalen.

Die sogenannten Spreizspektrumstechniken machen die Übertragung gegenüber Störsignalen robust, da sie die digitalen Nutzsignale auf dem gesamten Frequenzbereich verteilen. Befinden sich die verschiedenen WLAN- und Bluetooth-Netze im ausreichenden räumlichen Abstand zueinander, greift diese Technik erfolgreich. Ist der Abstand jedoch zu gering, sind Störungen die Folge.

Wenn zum Beispiel ein Bluetooth-fähiges Gerät direkt neben einem WLAN-fähigen Gerät sendet, werden so die WLAN-Signale während des Sendens übertönt. Genau das ist der Fall, wenn ein Notebook beispielsweise gleichzeitig über Bluetooth

die Bilder einer Digitalkamera einliest und diese dann über WLAN auf einem Server ablegen will.

Problematisch wird es auch, wenn sich die Geräte zufällig treffen. Ein Bluetooth-Handy, welches auf dem Schreibtisch liegt, kann ein Notebook mit WLAN-Netzanschluss besonders stören. Gefährdet sind ebenso neuere Szenarien wie Automobilanwendungen, in denen die Fahrzeuge über WLANs miteinander in Verbindung stehen und gleichzeitig innerhalb des Autos Geräte mit Bluetooth kommunizieren. Schließlich kann also WLAN durch Bluetooth beeinflusst werden. Bluetooth hingegen gilt als weitgehend störungssicher.

Die im Moment erhältlichen WLAN- und Bluetooth-Geräte unterstützen noch kein Verfahren zur Vermeidung von Störungen. Es wird aber zur Zeit an einem Verfahren gearbeitet, welches die Koexistenz und somit den parallelen Einsatz beider Technologien ermöglichen soll. [9]

6 Aktuelles & Ausblick

Im Herbst dieses Jahres hat die Bluetooth Special Interest Group (SIG) die Spezifikationen für den neuen Bluetooth-Standard 1.2 verabschiedet, die vor allem für weniger Komplikationen mit Wireless LAN-Funknetzen sorgen soll. [32]

Da WLAN der Standards 802.11b und 802.11g wie Bluetooth im 2,4 GHz Frequenzband arbeitet, gab es bisher öfter Probleme beim parallelen Betrieb beider Funktechnologien (vgl. Kapitel 5). Mit Bluetooth 1.2 soll dieses Störverhalten der Vergangenheit angehören. Dafür sorgt das Adaptive Frequency Hopping (AFH), welches im Gegensatz zum bisherigen Frequency Hopping Rücksicht auf bestehende WLANs nimmt. Dabei erkennt ein System „verrauschte“ Frequenzbereiche und vermeidet deren Nutzung, denn dort würden sowieso nur Datenpakete verloren gehen. Das System „hüpft“ somit nicht mehr durch den gesamten Frequenzbereich, sondern nur noch durch einen Teilbereich, der beispielsweise zwei Drittel des Gesamtbandes ausmacht. In der Praxis heißt das, dass die Performance von Bluetooth erhöht wird, während sich gleichzeitig die Interferenzen verringern.

Daneben wird mit dem erweiterten Standard Enhanced Voice Processing eingeführt, womit die Qualität der Sprachübertragung mit einer Fehlererkennungs-Technologie verbessert werden soll. Auch Quality-of-Service-Funktionen sind nun integriert, wodurch einzelnen Bluetooth-Diensten im Parallelbetrieb unterschiedliche Prioritäten zugewiesen werden können

Die Bluetooth SIG geht davon aus, dass Bluetooth 1.2 in den nächsten 12 bis 18 Monaten den Markt erobern wird. Erste Geräte mit Bluetooth 1.2 sollen 2004 auf den Markt kommen. Da Bluetooth 1.2 abwärtskompatibel konzipiert ist, sollen die Geräte mit Version 1.1 problemlos mit den neuen kommunizieren können.

Allein in Deutschland sind mehrere Hundert verschiedene Bluetooth-Geräte mit Version 1.1 erhältlich, weltweit sogar über 1200 zertifiziert. Die neueste Studie von der Markforschungsgruppe Cahners In-Stat prognostiziert weltweit 1,4 Milliarden verkaufte Bluetooth-Geräte im Jahr 2005. Laut SIG stiegen im 3. Quartal dieses Jahres erstmals die weltweiten Produktauslieferungen auf über eine Million Stück in der Woche. [18]

Demnächst wird eine neue Bluetooth-Generation, Bluetooth 2.0, den bislang eher schwachen Standard verbessern und attraktiver gestalten. Vor allem die recht geringe

Bandbreite von nur 1 Mbit/s soll der neue Standard vergrößern. Bluetooth 2.0 soll mit Bruttotransferraten von bis zu 12 Mbit/s operieren. Diese höheren Transferraten erzielt das Verfahren u.a. durch die Nutzung eines Schmalbandkanals unter Verzicht auf Bandspreizung. Die Reichweite bleibt jedoch auch weiterhin auf zehn Meter beschränkt. Für Bluetooth 2.0 spricht auch das Lösen von bisherigen Problemen in Bluetooth-Netzwerken. Bislang gab es beim Wechsel des Masters im Netz immer wieder Probleme durch Verbindungsabbrüche. Mit dem neuen Standard soll dies dann der Vergangenheit angehören. Insgesamt wird Bluetooth 2.0 wohl eine lohnende Erweiterung des aktuellen Bluetooth-Standards sein.

7 Fazit

Bluetooth bietet dem Benutzer viele Vorteile, was sicherlich auch ein entscheidendes Kriterium in der Marktdurchsetzung bedeuten könnte. Die drahtlose Kommunikation, die es dem Benutzer erlaubt, mit unterschiedlichen Geräten ohne Sichtkontakt zu kommunizieren ist in der heutigen Zeit eine sehr ansprechende und fortschrittliche Technologie. Die geringen Produktionskosten und der geringe Stromverbrauch sind weitere Aspekte, die in der Massenproduktion große Beachtung finden. Die Entwicklung der Technologien zeigt auch ganz deutlich, dass die Zukunft sich nicht nur auf kabelloses Telefonieren konzentrieren wird. In vielen Bereichen wird sich Bluetooth etablieren und Anwendung finden. Doch die Konkurrenz schläft nicht. Auch ZigBee wird eine große Zukunft vorausgesagt. Allein die Übertragungsreichweite und der niedrigere Stromverbrauch sprechen dafür. Welche Technologie sich letztendlich durchsetzen wird, liegt jedoch beim Anwender.

Literaturverzeichnis

1. Andersson, Christoffer: GPRS and 3G wireless Application - The Ultimate Guide to Maximizing Mobile Internet Technologies, Canada 2001, S. 81-104
2. ARS Software GmbH: Bluetooth - ein Standard für drahtlose Kommunikation im Nahbereich, http://www.ars2000.com/Bluetooth-White-Paper.pdf, 2002
3. Barth, Stephan: Drahtlose Gerätekommunikation: IrDA, Bluetooth, WLAN, http://www.uni-hildesheim.de/~mobinf/folien/Mobileinformation.pdf, WS 2002/03
4. Bleier, Bernhard: Bluetooth & Co Security. http://www.iemw.tuwien.ac.at/files/189.pdf, 2002
5. Borchers, Detlef: http://www.heise.de/mobil/artikel/2003/02/08/bluetooth/, 2003
6. Bray Jennifer and Sturman Charles F: Bluetooth 1.1: Connect Without Cables. Prentice-Hall 2002
7. Bundesamt für Sicherheit in der Informationstechnik: Bluetooth – Gefährdungen und Sicherheitsmaßnahmen, http://www.bsi.de/literat/doc/bluetooth/bluetooth.pdf, 2003
8. Bundesamt für Sicherheit in der Informationstechnik: Drahtlose lokale Kommunikationssysteme und ihre Sicherheitsaspekte, http://www.bsi.de/literat/doc/drahtloskom/drahtloskom.pdf, 2003
9. Computerwoche Archiv: Bluetooth stört WLAN-Kreise http://www.computerwoche.de/heftarchiv/2002/20020308/a80106785.html, 8.3.2002
10. Consulting Ambord: Bluetooth, http://www.acshop.ch/shop/de/faq_bluetooth.html, 2003

11. Detken, Kai-Oliver: Bluetooth – Technik, Einsatzgebiete, Sicherheit und Marktbetrachtung, http://www.decoit.de/whitepapers/DECOIT-BLUETOOTH0303.pdf, März 2003
12. Diepold, Michael: Infrarotkommunikation mit IrDA, http://dreamteam.fernuni-hagen.de/seminar01/01919_SS01.pdf, Juni 2001
13. Eggert, Torsten: Bluetooth – Funktionsweise, Sicherheitslücken, Lösungsansätze, http://web.f4.fhtw-berlin.de/messer/LV/PKI-SS03/Arbeiten/Bluetooth.pdf, 1.7.2003
14. FMK: Andere Funksysteme: Bluetooth, ZigBee und W-LAN, http://fmk.at/mobilkom/dl/FMK_2-7.pdf, 14.10.2002
15. Fox, Dirk: Bluetooth Security – Secorvo White Paper, http://www.secorvo.de/whitepapers/secorvo_wp05.pdf, 9.9.2002
16. Fujitsu Siemens Computers: Bluetooth-Technologie der drahtlosen Kommunikation der Zukunft *http://www.fujitsusi-mens.de/rl/produkte/wireless/download* /lifebook_whitepaper_*bluetooth*_technologie_neu.pdf, 26.1.2001
17. Gmür, Chrigi: Bluetooth, http://www.elektronik-kompendium.de/public/chrigi/bluetooth.htm
18. heise mobil: Bluetooth 1.2 verabschiedet, http://www.heise.de/mobil/newsticker/meldung/41758, 6.11.2003
19. Hochschule Mittweida (FH): Mach`s gut, Kabelsalat, http://telecom.htwm.de/bluetooth/bluetooth/motivati.htm, 21.5.2001
20. http://www.hedylamarr.at
21. http://www.palowireless.com
22. IfKom Landesverband Hessen: http://www.lv1.ifkomhessen.de/bluetooth.htm#S1
23. IVS - Otto-von-Guericke-Universität Magdeburg: Andere Standards: Bluetooth, http://ivs.cs.uni-magdeburg.de/EuK/Lehre/Wintersemester_01_02/DN_Bluetooth.pdf
24. Merkle, A./ Terzis, A.: Digitale Funkkommunikation mit Bluetooth, Poing : Franzis` Verlag, 2002
25. Muller, Nathan J: Bluetooth, Bonn : MITP-Verlag, 2001
26. Özkilic, Murat/ Zivadinovic, Dusan: Vertikale Schnitte – 13 neue Bluetooth-Profile, http://www.heise.de/mobil/artikel/2003/04/18/bluetooth-profile/default.shtml, 18.4.2003
27. Schneider, Thomas/ Bober, Bartlomiej: Proseminar Funk- und P2P-Netze – Bluetooth, http://www.bode.cs.tum.edu/Lehrstuhl/Lehre/Seminare/SS2003/blue.pdf, 21.4.2003
28. Sommer, Dieter: Bluetooth, http://www.itec.uni-klu.ac.at/~hellwagn/Seminare/AngewandteInformatik/bluetooth-draft-paper.pdf, 2002
29. Stallings, William: Wireless, Communications and Networks, New Jersey : Prentice-Hall, 2002, Kapitel 15
30. Thiele, Lothar/ Beutel, Jan: Eingebettete Systeme – Bluetooth, http://www.tik.ee.ethz.ch/tik/education/lectures/ES/WS00/Bluetooth.pdf
31. TU Dresden: Bluetooth, http://www.rn.inf.tu-dresden.de/scripts_lsrn/lehre/mobile/print/11.pdf
32. Vollmer, Alfred: Bluetooth steht erst am Anfang, http://dbindustrie.work.svhfi.de/AI/resources/bb4f0ac261c.pdf, 8.7.2003