

Proseminar Funk- und P2P-Netze

Bluetooth

Thomas Schneider

Bartłomiej Bober

21.4.2003

1 Einleitung

Immer mehr moderne Geräte wollen mit immer mehr anderen kommunizieren. Je einfacher desto besser, je mobiler desto besser. Bis zur Einführung von Bluetooth war es so, dass es keine einheitlichen Übertragungsprotokolle gab, sodass kein Gerät mit dem eines anderen Herstellers kommunizieren konnte. Es gab zwar schon Möglichkeiten zur Funkübertragung, jedoch waren auch diese auf Herstellerspezifische Sendeeinheiten beschränkt. Durch nahezu gar keine bzw. nur sehr schlechte Sicherheitsvorkehrungen und Störungsschutzmassnahmen geschah es immer wieder, dass Pakete abgefangen wurden oder nie beim Empfänger ankamen. Um zukünftig sinnvoll kommunizieren zu können, war somit eine Standardisierung gefragt.

2 Geschichte

Der Handy - Hersteller Ericsson startete 1994 eine interne Initiative, um die drahtlose Kommunikation der Handyperipherie zu erleichtern. Sie benannten diese Bluetooth, nach dem ehemaligen König von Dänemark und Norwegen, Harald Blatand. Darauf folgte 1998, nachdem klar wurde, dass die Ideen von Ericsson durchaus weltweiten Wert hatten, die Gründung der Bluetooth Special Interest Group, die mittlerweile an die 2000 Mitglieder zählt. Mitte '99 wurde von der Bluetooth SIG der Standard 1.0 veröffentlicht und mittlerweile ist 1.1 aktuell und stabil.

3 Was ist Bluetooth?

Bluetooth ist ein Kurzstreckenfunksystem, basierend auf dem 2.4 GHz ISM Band, das ursprünglich als Kabelersatz für Peripherie gedacht war. Heute wird es zusätzlich oft für die Kommunikation

zwischen PDAs, Handys und Computern verwendet. Da die Spezifikation unter anderem auch einschließt, dass ein Bluetooth Modul billig sein muss, könnten sich durchaus zukünftig auch Einsatzgebiete, wie zum Beispiel die Übertragung von Motor- und Tankfüllstandsdaten an der Tankstelle bzw Werkstatt oder auch Preisdaten von Einkäufen an der Supermarktkasse, durchsetzen.

4 Merkmale von Bluetooth

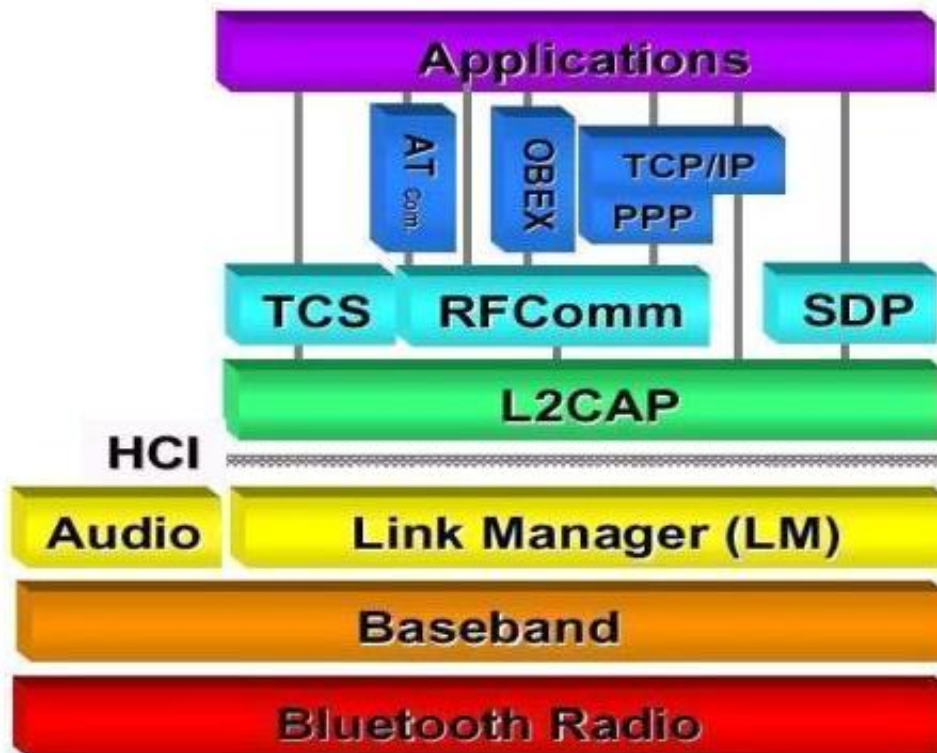
Durch das sogenannte Frequency-hopping (dazu später mehr), und durch verschiedenste Fehlererkennung und -korrektur Mechanismen ist Bluetooth sehr Robust gegenüber Störungen im Übertragungskanal. Auch die Datenverschlüsselung und Authentifizierungsmechanismen sind direkt im System integriert. Wie schon aufgezeigt, wird auch hier, wie bei vielen anderen Funkübertragungssystemen, das 2.4GHz ISM Band verwendet, welches ein offenes, lizenzfrei zu verwendendes Frequenzband ist, das dadurch allerdings auch sehr überfüllt ist. Diese Störeinflüsse werden bei Bluetooth allerdings zum Glück sehr gut umgangen. Ein weiteres, für mobile Endgeräte, sehr wichtiges Kriterium ist sicherlich, dass in der Spezifikation festgelegt ist, dass bestimmte, sehr niedrige, Energieverbrauchswerte nicht überschritten werden dürfen. Weiters gibt es zur Energieeinsparung noch verschiedene Modi, um die Akkulaufzeit zu erhöhen:

Sniff Mode Device hört Pakete nur mit und nimmt nur die an, die direkt an es gerichtet sind

Hold Mode suspend mode, bei dem die Synchronisation erhalten bleibt, das Gerät aber nicht mehr aktiv am Netzwerkverkehr teil nimmt

Park Mode Energiesparmodus, der das Modul in einen Schlafzustand versetzt, bei dem die Synchronisation verlohren geht

5 Der Bluetooth Stack



Die unterste Schicht des Bluetooth Stack ist natürlich der Übertragungsweg, die Funkstrecke. Das Signal wird bei dabei auf das in den meisten Teilen Europas freigegebene Frequenzband von 2,4000 –2,4835 GHz moduliert, was bei Bluetooth 79 Kanäle ergibt. In Spanien und Frankreich ist das Frequenzband auf 23 Kanäle eingeschränkt, da schon andere Institutionen die restlichen Frequenzen verwenden. Um in dem vollen ISM-Band eine Störung durch andere Geräte zu verhindern, wird ein sogenanntes Frequency-hopping Verfahren angewendet, wobei 1600 mal in der Sekunde die Übertragungsfrequenz gewechselt wird. Dieser Frequenzwechsel ist definiert durch eine festgelegte Funktion $C(t)$, die vom Zählerstand und der Adresse des Masters abhängig ist. Um zwei Geräte aufeinander abzustimmen ist somit ein Synchronisation nötig, die beim Verbindungsaufbau durch den Master geschieht. Die Spezifikation des Übertragungsweges umfasst von den Frequenzen, der Abbildungsfunktion, der Antenne bis zu den Sendeleistungsklassen jedes Detail. Die möglichen Leistungsniveaus sind dabei

Class 1 100mW mit ca 100m Reichweite,

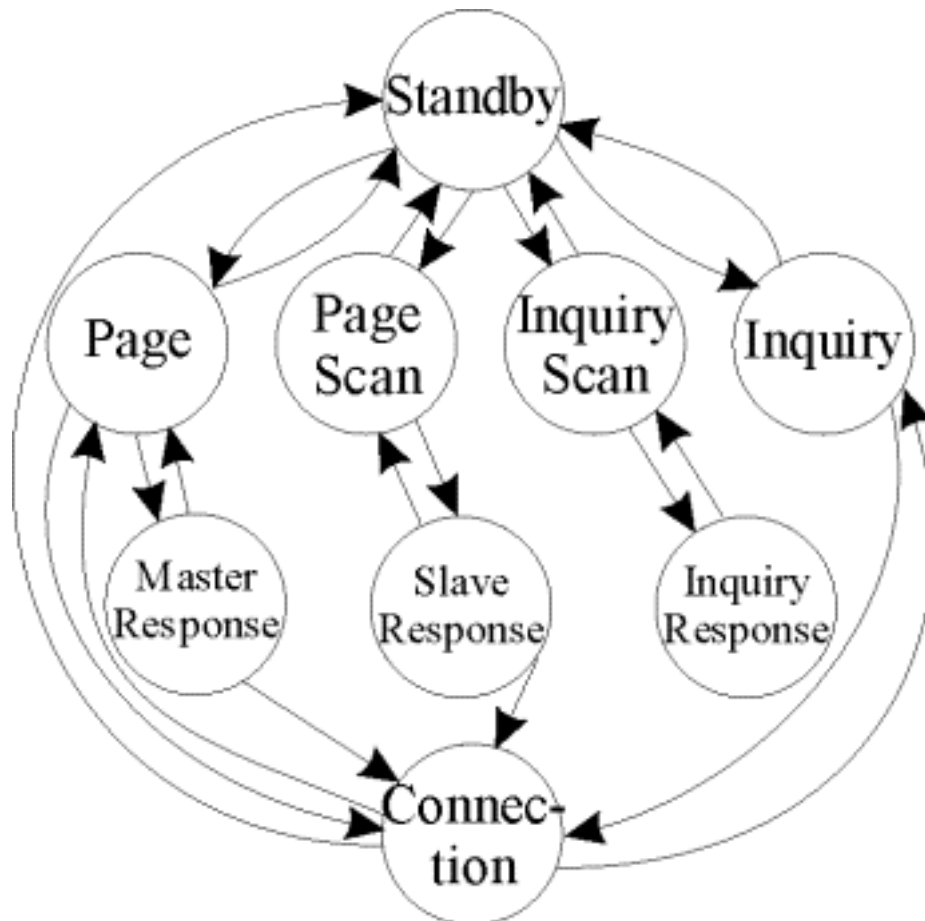
Class 2 2,5mW mit ca 20m Reichweite und

Class 3 1mW mit ca 10m Reichweite,

wobei die dritte Leistungsklasse die am weitesten verbreitete ist.

Zuständig für die eigentliche Übertragung von Daten ist das Baseband, das eine Verschlüsselung von bis zu 128 Bit zulässt, wobei die Schlüssellänge auch bei der Synchronisation ausgehandelt werden muss. Dieses Sicherheitsmanagement läuft über ein Challenge Response Verfahren zur gegenseitigen Authentifizierung. Im Baseband wird weiters noch eine Fehlerkontrolle sowie, soweit möglich,

eine Fehlerkorrektur durchgeführt. Der darauf aufsetzende Link Manager übernimmt die Steuerung von Verbindungsauf- und abbau und bietet ausserdem Funktionen an, um benachbarte Geräte zu finden und sich mit diesen zu synchronisieren. Zur Synchronisation mit diesen muss eine sogenannte Zustandsmaschine gesteuert werden, die als Stromsparmodus den Standby anbietet, wobei das Funk-system abgeschaltet wird. Die Zustände Inquiry beziehungsweise Inquiry Scan dienen zum auffinden von Geräten im Empfangsradius, was eine Verbindungsanfrage oder das warten auf eine solche als Folge nach sich zieht (Page bzw. Page Scan). Bei abgeschlossener Synchronisation wird das Modul in den Connected State geschaltet.



Um die Fähigkeiten von Bluetooth zu erweitern, wurde die Möglichkeit eingeführt, bis zu acht Module in einem sogenannten Piconet zusammenzuschliessen, wobei genau eines dieser Geräte ein Master ist, über den die gesamte Kommunikation läuft, gekennzeichnet ist so ein Piconet durch eine gemeinsame Hopping-Sequenz. Um auch mehr als nur diese kleine Anzahl von Rechnern oder PDAs zu vernetzen, besteht in der Spezifikation die Möglichkeit, mehrere Piconetze entweder über einen gemeinsamen Slave oder über ein Master/Slave Modul zu einem Scatternet zusammen zu schliessen.

Die Datenübertragung erfolgt entweder über einen sogenannten ACL-Link (Asynchronous Connection Less), bei dem jegliche Daten asynchron zwischen Master und Slave geschickt werden. Dabei muss darauf geachtet werden, dass auf jedes Datenpaket des Master, der angesprochene Slave antworten muss. Diese Verbindungsart kennt zusätzlich noch Fehlerkorrekturmechanismen. Sollte ein Paket grösser sein, als es die Länge eines Slots erlaubt, besteht die Möglichkeit, multislot Pakete

zu verschicken, wobei jedoch die Gefahr der Beeinflussung durch Störungen von ausserhalb wieder grösser wird. Die andere Art, Daten zu Übertragen, sind sogenannte SCO-Links, die für isochrone Datenströme eingesetzt werden. Vorallem bei zum Beispiel Audio-Übertragungen sind solche direkten Verbindungen hilfreich. Es können bei dieser Art der Kommunikation bis zu drei Verbindungen zu einem Master gleichzeitig aufgebaut werden, um zum Beispiel auch qualitativ höhere Audiodaten sauber Übertragen zu können.

Als Schnittstelle zwischen dem Bluetooth Modul und dem Rechner beziehungsweise PDA oder Handy dient das HCI, das sogenannte Host Controller Interface. Die Kommunikation wird von der HCI-Firmware über das Hardware Interface zum HCI-Treiber auf dem Host gesteuert und durchgeführt. Es gibt auf dem HCI nur drei verschiedene Pakettypen, die HCI-Commands, Befehle vom Host zum Modul, die HCI-Events, Nachrichten vom Modul zum Host, und schlussendlich die HCI-Datenpakete, die ACL- beziehungsweise SCO-Daten enthalten.

Die Steuerung und das Multiplexing der Datenpakete für die darauf aufsetzenden Anwendungen übernimmt das Logical Link Control and Adaption Protocol, kurz L2CAP, welches auch eine Zusammenfassung mehrerer ACL-Links erlaubt. Um Netzwerkverkehr über ein Bluetooth Modul zu vereinfachen und ältere Protokolle noch verwenden zu können, wurde ein Protokoll entwickelt, das eine RS232 Schnittstelle komplett emuliert. Diese, RFCOMM genannte, Emulation erlaubt es zum Beispiel eine PPP-Verbindung aufzubauen, wodurch normaler TCP/IP Datenverkehr sehr einfach realisierbar wird. Weitere kleinere Protokolle im Bluetooth-Stack sind das Service Discovery Protokoll, um Dienste auf benachbarten Geräten aufzuspüren und die Telephony Control Specification, die zur Steuerung von Telefongesprächen zum Beispiel auf Handys verwendet werden kann.

6 Profile

Da immer mehr neue Anwendungsbereiche für mobile Geräte 'erfunden' werden, muss natürlich auch eine Erweiterung der Funktionalität möglich sein. Diese Funktionalitätserweiterungen wurden bei Bluetooth durch sogenannte Profile ermöglicht. Die Profile spezifizieren die Verwendung der einzelnen Layer im Stack für bestimmte Aufgaben und somit auch die Funktionalität zwischen den Layern.

7 Anwendung von Bluetooth

Es gibt mittlerweile verschiedenste Formen von BT-Hardware, die, je nach Einsatzgebiet speziell auf die Anwendung zugeschnitten sein kann. So gibt es zum Beispiel Integrierte Chips, die, entweder mit oder ohne Funkeinheit, direkt für Eigenkonstruktionen verwendet werden können oder auch externe Module, zum Beispiel für USB, RS232 oder PCMCIA, aber natürlich auch Komplettgeräte wie zum Beispiel Handys, PDAs um untereinander oder mit dem PC Daten auszutauschen. Rechnerseitig wird dazu noch ein sogenannter Host-Stack benötigt, der die Steuerung des Moduls und die Datenpakete vom Rechner verwaltet. Es kursieren mittlerweile einige verschiedene Host-Stacks für die verschiedenen Plattformen, wie zum Beispiel WinStack (MS-Windows), JavaStack, BlueZ, OpenBT (Linux) und auch welche für MacOSX. Trotz der sehr genauen Spezifikation von Bluetooth besteht die Möglichkeit, dass der Stack mit der verwendeten Hardware inkompatibel ist wodurch ein sehr genaues Testen vor der Festlegung auf ein bestimmtes Tool nötig ist.

8 Abschliessende Bemerkungen

Bluetooth ist ein relativ junges und noch nicht sehr verbreitetes Übertragungsmodell, das im Kurzstreckenbereich durchaus vielversprechend wirkt, aufgrund seiner beschränkten Übertragungsgeschwindigkeit von einem Megabit pro Sekunde aber sicher nicht für viel mehr als mal eine Visitenkarte von Handy zu PDA oder oder sonstigen kleinen Datenmengen zwischen verschiedenen mobilen Endgeräten verwendet werden wird. Ein sehr grosser Vorteil wird immer bestehen, dass sehr einfach und zuverlässig Verbindungen zu anderen Geräten anderer Hersteller aufgebaut werden können.