Standards drahtloser Übertragung: Von Bluetooth zu IEEE 802.15.4/ZigBee

Michael Bürge
Betreuung: Christian Frank

ETH Zürich – Departement Informatik
Seminar Verteilte Systeme zum Thema Smart Environments SS2004

Abstract

Die fortschreitende technische Entwicklung ermöglicht es, immer kleinere und leistungsfähigere Geräte zu bauen. Zusammen mit dem allgegenwärtigen Trend zur Vernetzung dieser Geräte sind ganz neue Anwendungsszenarien entstanden, die bisher nicht denkbar waren. Eine wichtige Voraussetzung für die Realisierung dieser Szenarien ist das Vorhandensein geeigneter drahtloser Übertragungsverfahren, die vielfältigen Anforderungen genügen müssen. Im Rahmen dieser Arbeit werden mit Bluetooth und IEEE 802.15.4/ZigBee zwei Standards betrachtet, die zur drahtlosen Vernetzung von Kleingeräten gedacht sind.

1. Einleitung

Die fortschreitende Miniaturisierung und die damit einhergehende Kostenreduktion von Mikroprozessoren haben dazu geführt, dass einerseits immer mehr Alltagsgegenstände mit Elektronik aufgewertet und andererseits völlig neue Geräte und Anwendungen realisierbar wurden. Ein zusätzliches Potential ergibt sich durch die Vernetzung, erst durch diese kann eine Umgebung "smart" werden. Es besteht also ein grosser Bedarf an geeigneten drahtlosen Kommunikationsprotokollen, wobei die heute existierenden Standards nicht alle Bedürfnisse abdecken können. Insbesondere für all die kleinen und vielfach batteriebetriebenen Geräte mit moderaten Bandbreitenforderungen, die in den Szenarien des ubiquitous Computing vorkommen, sind die existierenden Technologien entweder zu komplex, zu teuer oder verbrauchen zu viel Energie.
In einigen Fällen konnte mit Bluetooth eine geeignete Lösung gefunden werden, dieser Standard soll denn im folgenden auch besprochen werden. Es bleibt aber immer noch ein Segment, in dem Einfachkeit, geringe Kosten und niedriger Energiebedarf wichtiger sind alles andere, für den noch kein geeignetes standardisiertes Funkverfahren zur Verfügung steht. Mit IEEE 802.15.4/ZigBee steht nun ein vielversprechender Standard kurz vor der Marktreife, der diese Lücke füllen soll. Das Vorstellen und die Besprechung dieses jüngsten Spross in der Familie drahtloser Übertragungsverfahren wird denn auch den Grossteil dieser Arbeit ausmachen.

2. Bluetooth

Nach einem dänischen König des 10ten Jahrhunderts benannt, dem es durch sein diplomatisches Geschick gelungen war, die unzähligen zu der Zeit rivalisierenden Stämme zu einem Königreich zu vereinen, schickte sich der Funkstandard Bluetooth vor einigen Jahren an, die Kommunikation zwischen Geräten verschiedenster Art zu vereinheitlichen und der Vielzahl von zueinander inkompatiblen Kabelverbindungen ein Ende zu bereiten. Nachdem die Verbreitung anfänglich etwas zögerlich vorankam, es dauerte eine Weile, bis die Hersteller den komplexen und umfangreichen Standard in den Griff bekamen, sind Bluetooth-Chips heute beinahe in jedem besseren Handy, PDA oder Laptop verbaut. Der Standard hat sich etabliert und die Flut von Bluetooth-fähigen Geräten wird mit Sicherheit noch zunehmen.

Bluetooth operiert im lizenzfreien ISM-Band bei 2.4 GHz. Um Robustheit gegenüber Störungen und Interferenzen zu erreichen, wird ein Frequenzsprungverfahren (Frequency Hopping) eingesetzt, bei dem das Frequenzband in 79 Kanäle eingeteilt wird, die 1600 Mal in der Sekunde nach einer Pseudozufallsreihenfolge gewechselt werden. In der kommenden Bluetooth-Revision 1.2 wird dieses Verfahren mit Adaptive Frequency Hopping noch verbessert, indem gestörte Kanäle erkannt und gemieden werden. Die Brutto-Datenrate beträgt 1 Mbps, für Anwendungen nutzbar sind davon unter besten Bedingungen rund 700 Kbps bei asymmetrischen und etwa 500 Kbps bei symmetrischen Verbindungen.

Ein Bluetooth-Netzwerk, Piconet genannt, besteht aus einem Master und bis zu 7 Slaves. Der Master gibt die Hop-Sequenz vor, vergibt Geräteadressen und steuert die gesamte Kommunikation. Ein Slave wird nie von sich aus aktiv, sondern muss darauf warten, bis er vom Master einen Sendeslot zugewiesen bekommt. Ein Piconetz stellt eine Stern-Topologie dar mit dem Master im Zentrum, eine direkte Kommunikation zwischen zwei Slaves ist nicht möglich. Um grössere Netzwerke aufzubauen, können mehrere Piconetze zu einem Scatternetz verbunden werden. Gewisse Slaves sind dabei im Timesharing-Verfahren in zwei Piconetzen aktiv, wodurch sie als Gateway agieren und Routing-Funktionen wahrnehmen können. Die Implementierung von Scatternetzen ist komplex. Die unterschiedlichen Piconetze sind untereinander nicht synchronisiert, die Slotgrenzen stimmen nicht überein und die Frequenzreihenfolgen sind komplett unabhängig voneinander, woraus sich eine ganze Reihe von Timingproblemen ergeben. Ein Slave, der als Bindeglied fungieren will, muss zudem mit zwei unabhängigen Mastern aushandeln, wann er im jeweiligen Piconetz aktiv ist. Weiterhin bietet der Bluetooth-Stack keinerlei Routing-Funktionalität, welche folglich auf Applikationsebene implementiert werden muss. Abgesehen von akademischen Arbeiten existieren bislang keinerlei Anwendungen, die Scatternetze verwenden. Ein praktischer Beweis, dass sich Scatternetze nutzbringend einsetzen lassen, steht also immer noch aus.

Um sich zu einem Piconetz formieren zu können, müssen sich beteiligte Geräte erst einmal finden können, ein Vorgang, der durch das Frequency-Hopping erheblich erschwert wird. Ein Gerät kann nicht einfach zu einem bestehenden Piconetz hinzustossen, da es dessen Frequenzreihenfolge und Timing nicht kennt. Um diesen essentiellen Vorgang zu ermöglichen, kennt Bluetooth einen Inquiry genannten Device-Discovery-Mechanismus, welcher zwei Rollen vorsieht. Im Inquiry-Modus versendet ein Gerät mit doppelter Hop-Rate (3200 hops/s) spezielle Inquiry-Pakete, die Synchronisationsinformationen enthalten. Das Gegenstück dazu ist der Inquiry Scan-Modus, in dem mit einer sehr kleinen Hop-Frequenz (ein Wechsel alle 1.28 s) die Kanäle gescannt werden. Wird ein Inquiry-Paket empfangen, kann mit Hilfe der darin enthaltenen Informationen der richtige Zeitpunkt und Kanal errechnet werden, um eine Antwort zurückzusenden. Nach erfolgter Bekanntmachung können die Geräte die gewonnenen Informationen nutzen, um mittels des Paging-Mechanismus, der ähnlich abläuft wie das Inquiry, ein Piconetz zu formieren. Von einer ausführlichen Beschreibung wird an dieser Stelle abgesehen, denn im Detail sind die Abläufe recht komplex. Wichtig ist jedoch die Feststellung, dass aufgrund der statistischen Natur des Inquiry-Verfahrens keine Garantien darüber möglich sind, in welcher Zeit sich zwei Geräte finden werden. Im praktischen Einsatz dauert ein Inquiry mindestens 3 s, wobei ungünstige Bedingungen die benötigte Zeit schnell auf 10 - 20 s anwachsen lassen. Insbesondere für Anwendungen, in denen nur geringe Datenmengen in grossen zeitlichen Abständen übermittelt werden, stellt die lange Verbindungsaufbauzeit einen grossen Nachteil dar.

3. IEEE 802.15.4/ZigBee

Die Begriffe IEEE 802.15.4 und ZigBee werden vielerorts als Synonyme verwendet, obwohl zwischen ihnen eine klare Abgrenzung besteht, die an dieser Stelle kurz verdeutlicht werden soll.
Der vom Institute of Electrical and Electronics Engineers erarbeitete Standard 802.15.4 spezifiziert die Radioeinheit (physical Layer, PHY) und den Medienzugriff (Medium Access Control, MAC), was den untersten beiden Ebenen des OSI-Schichtenmodells entspricht. Mit einiger Verspätung wurde der

Standard IEEE 802.15.4 [1] Anfang Mai 2004 ratifiziert, abgesehen von einigen zu erwartenden Berichtigungen und Verdeutlichungen gelten die Arbeiten daran nun also als abgeschlossen.
Die ZigBee Alliance [2] wurde von einigen grossen Firmen aus der Halbleiterbranche ins Leben gerufen mit dem Ziel, auf der Basis von IEEE 802.15.4 eine komplette Protokollsuite für drahtlose Kommunikation bis hinauf zu der Applikationsschnittstelle zu entwickeln. Eine Draft-Spezifikation wurde schon fertiggestellt, ist aber leider nur für Mitglieder der Allianz zugänglich und stand deshalb nicht zur Verfügung. Die finale (öffentliche) Version der ZigBee-Spezifikation wird Ende 2004 erwartet.
Erwähnenswert ist in diesem Zusammenhang noch, dass der IEEE 802.15.4-Standard in keiner Weise an die ZigBee Alliance gebunden ist. Es steht also grundsätzlich jedermann die Möglichkeit offen, auf der Basis von IEEE 802.15.4 eigene Entwicklungen zu starten.

3.1 Ziele und Positionierung

Mit Chips für IEEE 802.15.4/ZigBee lassen sich so genannte Wireless Personal Area Networks (WPAN) aufbauen, deren Anwendungen von der Industrie und Automatisierungstechnik (z.B. Anlagensteuerung per Funk) sowie Spedition und Logistik (Güterüberwachung) über die Heim- und Gebäudeautomatisierung (kabelfreie Steuerung von Geräten und Anlagen), die Medizintechnik (drahtlose Patientendaten-Übertragung) bis hin zur Bedienung von Computer-Peripherie und Unterhaltungselektronik reichen [3,5,6].
IEEE 802.15.4/ZigBee ist auf Anwendungen mit geringen Bandbreitenanforderungen zugeschnitten, was an den maximal erreichbaren 250 KBps erkennbar ist. Weiter wurde davon ausgegangen, dass viele Geräte nur sporadisch und sehr wenig Daten zu versenden oder zu empfangen haben und somit einen Grossteil der Zeit in einem Standby-Modus verbringen, also einen geringen duty-cycle aufweisen. Um eine gute Energieeffizienz erreichen zu können wurde deshalb besonders darauf geachtet, den Aufwand gering zu halten, den ein Gerät betreiben muss, bevor es nach einem Wechsel in den aktiven Zustand Nutzdaten versenden kann. Erklärtes Ziel ist es, dass einfachste Geräte (z.B. Sensoren) Batterielaufzeiten bis zu mehreren Jahren erreichen können.
Alle erwähnten Anwendungen haben gemeinsam, dass in den zugehörigen Märkten hohe Stückzahlen produziert werden und deshalb sehr preissensitiv sind. Eine wichtige Anforderung bei der Entwicklung von IEEE 802.15.4 und ZigBee war es denn auch, die Chips möglichst einfach zu halten, um eine billige Herstellung zu ermöglichen. Die ZigBee Alliance erhofft sich, mit ZigBee einen Standard zu schaffen, der die im Embedded-Bereich bisher existierenden proprietären Funkverfahren ablösen wird. Viele Analysten erwarten, dass dieser Markt durch die durch ZigBee entstehende Herstellerinteroperabilität neue Impulse erhalten wird und sagen für die kommenden Jahre ein grosses Wachstum voraus.

3.2 Überblick

Der Standard sieht mit Full Function Devices (FFD) und Reduced Function Devices (RFD) zwei verschiedene Geräteklassen vor. Ein FFD beherrscht den kompletten Protokollstack und benötigt dafür weniger als 32KB Speicher. Ein FFD kann mit RFDs oder anderen FFDs kommunizieren, während ein RFD nur mit genau einem FFD kommunizieren kann. Dafür ist die Implementierung eines RFD sehr viel simpler und kommt mit 4-8 KB Speicher aus.
Geräte die miteinander kommunizieren bilden ein Personal Area Network (PAN), das jeweils durch einen PAN-Identifier gekennzeichnet ist, der von dem Gerät bestimmt wird, das das PAN initiiert hat. Im einfachsten Fall bilden die teilnehmenden Geräte eine Stern-Topologie. Für grosse und ausgedehnte Netze sind aber auch Multihop-Szenarien vorgesehen, in denen Peer-to-Peer-, Mesh- und Cluster-Tree-Topologien zum Einsatz kommen.
Es gibt drei Modi, in denen sich ein Gerät befinden kann: PAN-Koordinator, Koordinator und Teilnehmer (Device). Jedes PAN hat genau einen PAN-Koordinator, dem einige wichtige Verwaltungsaufgaben wie die Vergabe von Adressen und das Unterhalten einer Pairing-Tabelle zufallen, wofür zusätzlicher Speicher benötigt wird. Ein Koordinator, von denen es mehrere geben kann, stellt Synchronisationsdienste für den Medienzugriff zur Verfügung. Alle übrigen Geräte haben den Status eines Teilnehmers, wobei FFD's noch

eine gewisse Routing-Funktionalität wahrnehmen können.

3.3 IEEE 802.15.4 - PHY

Die Funktschnittstelle von IEEE 802.15.4 bietet ingesamt 27 Kanäle in drei verschiedenen Frequenzbändern, einen Überblick bietet Tabelle 1. Als Funkstandard mit kleiner Reichweite, der für eine Massenanwendung im Consumer- und Industriebereich ausgelegt ist, war es aus praktischen Gründen zwingend, die verwendeten Frequenzen in den lizenzfreien ISM-Bändern anzusiedeln. Im weltweit verfügbaren 2.4GHz-Band stehen 16 Kanäle mit einer Bruttodatenrate von jeweils 250 Kbps zur Verfügung. Nebst diesen Kanälen mit einer relativ hohen Datenrate sollte IEEE 802.15.4 auch für Anwendungen geeignet sein, die bezüglich Datenrate noch viel geringere Anforderungen haben und so wurde von Anfang an der Ansatz verfolgt, die Funkschnittstelle auch mit Kanälen auf geringeren Frequenzen auszustatten. Im angestrebten Bereich um 900 MHz steht aber unglücklicherweise kein weltweit lizenzfrei nutzbares Band zur Verfügung, so dass eine weitere Aufteilung nötig wurde. 10 Kanäle mit einer Bruttodatenrate von jeweils 40 Kbps sind im Frequenzband um 915 MHz definiert, welche nur in Amerika nutzbar sind. In Europa und Asien sind die Frequenzen in diesem Bereich leider sehr stark belegt, weshalb für diese Gebiete gerade mal ein Kanal bei 868 MHz definiert werden konnte, der zudem sehr schmalbandig ist und deshalb nur eine Bruttodatenrate von 20 Kbps bieten kann. Chips, die IEEE 802.15.4 beherrschen, werden zwei Radioeinheiten aufweisen, die Bänder um 868 und 915 MHz liegen ausreichend nahe beieinander, um die gleichen Schaltkreise verwenden zu können.
Es stellt sich die Frage, wie gut sich in Europa und Asien der eine Kanal im unteren Band nutzen lässt. Mehrere unabhängige Anwendungen, die diesen verwenden möchten, werden sich zwangsläufig gegenseitig stören. Natürlich bietet sich die Möglichkeit, auf das 2.4 GHz-Band auszuweichen, aber für Anwendungen mit geringsten Bandbreitenanforderungen wären niedrigere Frequenzen vorteilhaft, da weniger Energie für die Übertragung benötigt wird und somit längere Batterielaufzeiten möglich wären. Mit steigender Frequenz nimmt auch die Absorption von elektromagnetischen Wellen an Hindernissen wie Mauern und Vegetation zu, weswegen niedrigere Frequenzen aufgrund ihrer günstigeren Ausbreitungseigenschaften in vielen Umgebungen von Vorteil wären.
Eine weitere wichtige Funktion der Funkschnittstelle ist die Leistungsregelung. Dabei wird die Qualität der Übertragung laufend überwacht und die Sendeleistung so weit heruntergeregelt, dass eine zuverlässige Kommunikation gerade noch möglich ist. Dies dient haupsächlich der Schonung von Energieressourcen, reduziert aber gleichzeitig auch die Gefahr, Netze in der Nachbarschaft zu stören, die den gleichen Kanal verwenden möchten.

Frequenz	Kanäle	Datenrate	Verfügbarkeit
868 MHz	1	20 Kbps	Europa/Asien
915 MHz	10	40 Kbps	USA/Pazifik
2.4 GHz	16	250 Kbps	Weltweit

Tabelle 1: Von IEEE 802.15.4 verwendete Frequenzbänder

3.4 IEEE 802.15.4 - MAC

Die MAC-Ebene hat grundsätzlich die Aufgabe, eine zuverlässige Verbindung zwischen den MAC-Entitäten verschiedener Geräte aufzubauen und aufrechtzuerhalten.
Zur Adressierung wird die 64 bit lange Struktur der erweiterten IEEE-Adressen (Extended Addresses) verwendet, womit ausreichend Adressen verfügbar sind, um jedes Gerät mit einer weltweit eindeutigen Adresse auszustatten. Um den Overhead in den Paketheadern zu reduzieren, werden innerhalb eines PAN Kurzadressen mit einer Länge von 16 bit zur Adressierung verwendet, wodurch die maximale Anzahl Geräte in einem PAN auf 65536 begrenzt ist. Die Vergabe und Verwaltung dieser Kurzadressen ist

Aufgabe des PAN-Koordinators und geschieht bei der Anmeldung (Association) eines Geräts am PAN. Die maximale Paketgrösse auf MAC-Ebene liegt bei 127 Bytes, wovon nach Abzug des für den Header und die Checksumme benötigten Platzes noch höchstens 105 Bytes für Nutzdaten der höheren Schichten zur Verfügung stehen.

3.4.1 Medienzugriff

IEEE 802.15.4 stellt zwei verschiedene Medienzugriffsverfahren bereit. Im einfacheren Fall eines nonbeacon-Netzwerks erfolgt der Kanalzugriff nach einem CSMA/CA-Verfahren (Carrier Sensing Multiple Access/Collision Avoidance), das im wesentlichen ein Standard ALOHA-Protokoll darstellt. Bevor ein Gerät zu senden beginnt überprüft es erst den Kanal während eines durch eine Zufallszahl bestimmten Zeitraums (Random Backoff Period) auf Aktivität von anderen Geräten. Funkt in diesem Zeitraum jemand dazwischen, wird der Versuch abgebrochen, eine neue Random Backoff Period aus einem doppelt so grossen Intervall bestimmt und der Vorgang beginnt von neuem, bis entweder das Paket erfolgreich versendet werden konnte oder die maximale Anzahl Versuche erreicht worden ist. Die Vorteile des gerade beschriebenen Verfahrens sind seine einfache Implementierung und die Eigenschaft, dass durch die Gleichberechtigung aller Teilnehmer beliebige Geräte direkt miteinander kommunizieren können, die sich hören können. Jedoch besteht die Notwendigkeit, dass alle Empfänger immer eingeschaltet sind, da zu jedem Zeitpunkt eine Übertragung beginnen kann. Dies stellt für Geräte, die nur sporadisch Daten senden oder empfangen, eine unnötige Energieverschwendung dar.

Die effektivste Strategie zur Schonung von Energieressourcen in einem Funkverfahren besteht darin, die Radioeinheit über möglichst grosse Zeiträume komplett abzuschalten. Das zweite angebotene Medienzugriffsverfahren bietet Mechanismen, diese Strategie anzuwenden. In einem beacon-enabled-Netzwerk wird eine so genannte Superframe-Struktur verwendet, die in Abbildung 1 dargestellt ist. Diese Struktur kann sehr flexibel den Anforderungen der jeweiligen Anwendung angepasst werden. Ein Koordinator nimmt deren Konfiguration und Verwaltung vor. Im einfachsten Fall einer Stern-Topologie sind die Funktionen des PAN- und Superframe-Koordinators üblicherweise in dem Knoten vereint, der im Zentrum des Sterns sitzt. In ausgedehnteren Netzwerken können aber durchaus mehrere voneinander unabhängige Superframe-Strukturen präsent sein. Eine Superframe-Struktur zeichnet sich durch die vom Koordinator periodisch versendeten Beacon-Frames aus, in denen die Konfigurationsinformationenen enthalten sind. Das Intervall zwischen zwei Beacons und somit die Dauer eines einzelnen Superframes kann im Bereich von 15 ms bis 252 s gewählt werden. Ein Superframe besitzt eine aktive Phase, in der die Kommunikation stattfindet, und eine inaktive, in der der Koordinator seine Radioeinheit abschaltet. Die aktive Phase besteht aus 16 Slots gleicher Länge, die unterteilt sind in eine Contention Access Period (CAP) und eine Contention Free Period (CFP). Der Medienzugriff während der CAP ist wettbewerbsbasiert, es kommt eine slotted-Variante des CSMA/CA-Algorithmus zum Einsatz, in dem die Timer für die Random Backoff Period immer am Anfang eines Slots gestartet werden. Die CFP stellt einen Quality of Service-Mechanismus dar. Ein Gerät kann beim Koordinator garantierte Timeslots (GTS) anfordern, die es, falls sie gewährt werden, alleinig nutzen darf, wodurch auch die Verwendung von CSMA/CA hinfällig wird. Festzuhalten ist noch die Tatsache, dass innerhalb einer Superframe-Struktur eine direkte Kommunikation nur mit dem Koordinator stattfindet.

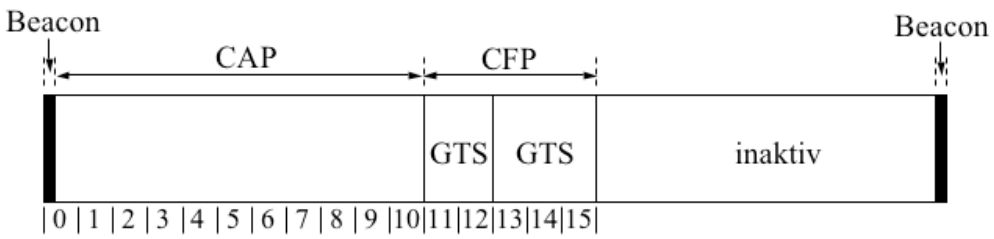

Abbildung 1: Superframe-Struktur

3.4.2 Datentransaktionen

Es soll nun betrachtet werden, wie die Datenübertragung innerhalb der Superframe-Struktur in der CAP im Detail abläuft. Der Ablauf der Übertragung eines Datenpakets von einem Teilnehmer zum Koordinator ist in Abbildung 2 dargestellt. Der Teilnehmer bewirbt sich dazu mittels CSMA/CA um einen Slot und versendet schliesslich das Paket. An dieser Stelle sei noch darauf hingewiesen, dass Bestätigungen (Acknowledgements) von Datenpaketen optional sind und von den Anwendungen explizit angefordert werden müssen, indem das entsprechende Bit im Paketheader gesetzt wird. Etwas aufwendiger gestaltet sich die Übermittlung eines Datenpakets vom Koordinator zu einem Teilnehmer, wo eine indirekte Übertragung zum Einsatz kommt (dargestellt in Abbildung 3). Das für den Teilnehmer bestimmte Datenpaket wird vom Koordinator erst einmal zwischengespeichert. Beim nächsten Versenden eines Beacon-Frames wird nun die Adresse des Empfängers in eines der dafür vorgesehenen Felder geschrieben (pending address fields). Diese Felder werden von einem Teilnehmer jedesmal auf die eigene Adresse überprüft. Kommt diese vor, so weiss der Teilnehmer, dass ein Datenpaket "zum Abholen" bereit liegt. Dazu sendet er ein data request-Kommando an den Koordinator, der dieses erst bestätigt und danach die eigentlichen Daten übermittelt. Kommt in einem Beacon die eigene Adresse eines Teilnehmers nicht vor, kann die Radioeinheit bis zum nächsten Beacon vollständig deaktiviert werden. Je grösser das Beaconintervall gewählt wurde, desto grösser ist auch das Energiesparpotential. Dabei muss aber beachtet werden, dass durch ein grösseres Intervall auch die Latenz steigt. Erfordert eine Anwendung, dass ein Datenpaket in einer bestimmten Zeit bei einem Teilnehmer einer Superframe-Struktur ankommen muss, darf das Beaconintervall auf keinen Fall grösser als die maximal zulässige Latenz sein. Für Geräte, die nur Daten versenden aber nie empfangen müssen, besteht keine Notwendigkeit, die Beacon-Frames auf bereitstehende Daten zu untersuchen. Ein solches Gerät kann sich in einem non-tracking-Modus befinden und nur dann aktiv werden, wenn es selber Daten zu versenden hat. In diesem Fall muss es sich erst einmal wieder auf die Superframe-Struktur synchronisieren, wozu mit eingeschaltetem Empfänger das nächste Beacon abgewartet wird. Da dies je nach Beaconintervall sehr lange dauern kann, existieren auch einige spezielle MAC-Kommandos, die ebenfalls eine Synchronisierung ermöglichen, ohne ein Beacon abwarten zu müssen.

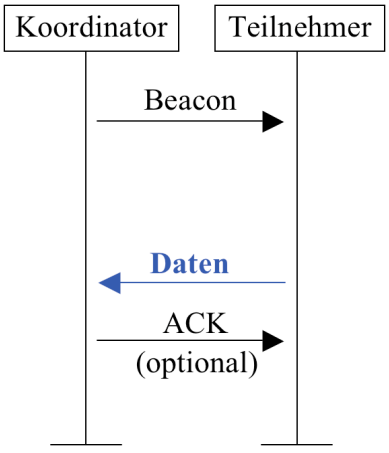

Abbildung 2: Datenübertragung von einem Teilnehmer zu einem Koordinator

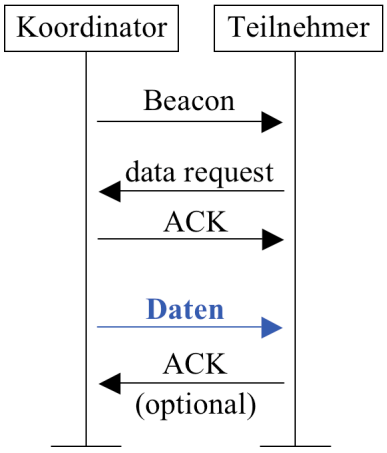

Abbildung 3: Datenübertragung von einem Koordinator zu einem Teilnehmer

3.4.3 Assoziation/Disassoziation

Bisher noch nicht angesprochen wurde die Art und Weise, wie ein Gerät ein existierendes PAN finden und sich an diesem anmelden kann. Dazu wird ein Scan auf den Kanälen durchgeführt, auf denen ein PAN vermutet wird. Bei einem aktiven Scan wird ein beacon request-Kommando versendet, das von einem

potentiell anwesenden Koordinator innerhalb einer vorgegeben Zeitspanne beantwortet wird. Bei einem passiven Scan wird einfach der Empfänger eingeschaltet und auf ein reguläres Beacon gewartet. Die passive Variante ist vor allem für RFD's gedacht, die active Scans nicht zwingend unterstützen müssen. Um im PAN partizipieren können, muss ein association request an den PAN-Koordinator gesendet werden. Wird die Anfrage gutgeheissen, erhält das Gerät eine Kurzadresse zugewiesen. Analog dazu erfolgt das Abmelden von einem PAN mit einem disassociation request.
Das Anmelden kann inklusive des vorhergehenden Scans sehr schnell ablaufen. Bei minimalem Beaconintervall dauert es höchstens 15 ms, bis der Scan abgeschlossen ist. Wird im anschliessenden Superframe gleich ein association request versendet, dauert der ganze Vorgang nur rund 30 ms.

3.4.4 Sicherheit

Die MAC-Ebene sieht drei Sicherheitsstufen vor, wobei die beiden „sicheren" Stufen optional sind: erstens „keine Sicherheitsvorkehrungen“, zweitens den Einsatz einer einfachen Zugriffsbeschränkung auf Basis der Geräteadressen (Access Control Lists, ACL) sowie drittens die symmetrische Verschlüsselung unter Nutzung des AES-Algorithmus mit einer Schlüssellänge von 128 bit. Diese Mechanismen können mittels der darüberliegenden ZigBee-Protokolle verwaltet werden.

3.5 ZigBee Upper Layers

Wie weiter oben bereits erwähnt wurde, ist die ZigBee-Draft-Spezifikation leider nicht öffentlich verfügbar. Dieser Abschnitt kann deshalb lediglich einen groben Überblick der Aufgaben der höheren Schichten liefern.
Der ZigBee Network Layer (NWK) realisiert ein Protokoll für verbindungslose Ende-zu-Ende-Übertragungen. Dazu gehören Aufgaben wie die Konfiguration und Administration der Netzwerk-Topologie und der logischen Verbindungen zwischen den einzelnen Knoten mit Hilfe von Pairing-Tabellen, die sich unter den Begriffen Paket Routing und Route Management zusammenfassen lassen. Diese Aufgaben sollen aus Sicht einer Anwendung transparent ablaufen. Eine Bewertung der Implementierung ist derzeit nicht möglich, da nicht bekannt ist, was für ein Routing-Verfahren und welche Kostenfunktionen zum Auffinden von optimalen Pfaden zum Einsatz kommen werden. Es sei darauf hingewiesen, dass die in diesem Zusammenhang auftretenden Probleme alles andere als trivial sind. Man darf also gespannt sein, wie gut die von der ZigBee Alliance entwickelten Lösungen sind, zumal diese auch noch möglichst schonend mit Energieressourcen umgehen sollen.
Das General Operational Framework (GOF) ist als Verbindungsschicht zwischen dem NWK und den Applikationen zu verstehen. Die wichtigste Aufgabe ist das Multiplexing von Daten von verschiedenen Anwendungen, ähnlich dem Konzept der Ports beim TCP/IP. Des weiteren werden in dieser Schicht Geräteeigenschaften gespeichert und den Anwendung zugänglich gemacht.
Zuoberst im Protokollstack befinden sich die ZigBee Device Objects (ZDO), die die eigentlichen Applikationen darstellen. Zu den Aufgaben eines ZDO gehört auch das Fragementieren von grösseren Datenmengen, falls diese die maximale Paketgrösse der darunterliegenden Schichten übersteigen. Dass dies den Applikationen überlassen wird verdeutlich noch einmal, wie sehr ZigBee auf kleine Datenmengen ausgerichtet ist.
In ZigBee wird es Applikationsprofile ähnlich denen von Bluetooth geben, die die Herstellerinteroperabilität der Geräte sicherstellen sollen. Zum jetzigen Zeitpunkt ist erst ein einziges Profil definiert, Commercial and Residential Lighting, sobald ZigBee aber fertig spezifiziert ist dürften schnell weitere hinzukommen.

4. Bluetooth vs. ZigBee

Wenn von ZigBee die Rede ist, taucht immer auch die Frage auf, inwiefern eine Konkurrenz zu Bluetooth vorhanden ist. Dabei werden die Mitglieder der ZigBee Alliance nicht müde zu betonen, dass die beiden Standards unterschiedlichen Zwecken dienen und sich deshalb nicht konkurrieren sondern ergänzen. Das

Bluetooth-Lager scheint sich in dieser Frage nicht ganz so einig zu sein und ist tendenziell eher darauf bedacht, die Bedeutung von ZigBee herunterzuspielen.
Die wichtigsten heutigen Einsatzgebiete von Bluetooth sind Dateiübertragungen, Sprachverbindungen und die Synchronisation von Kontaktinformationen. Diesen Anwendungen ist gemeinsam, dass sie kurzzeitige Punkt-zu-Punkt-Verbindungen aufbauen, während denen die zur Verfügung stehende Bandbreite ausgereizt wird. Im Vergleich zu Bluetooth bietet ZigBee nur einen Bruchteil der Bandbreite und stellt im Protokollstack auch keinerlei Audiofunktionalität bereit, kann somit die Position von Bluetooth in diesen Anwendungsbereichen nicht gefährden.
Die Vorzüge von ZigBee sollen am Beispiel eines batteriebetriebenen drahtlosen Sensors illustriert werden, etwa ein Temperaturfühler oder ein Regenmelder. Ein solcher Sensor überträgt pro Transaktion jeweils nur wenige Bytes und es besteht kein Bedarf, Daten zu empfangen. Es liegt also nahe, die Radioeinheit in den langen inaktiven Phasen zwischen den einzelnen Transaktionen zu deaktivieren, um die Energieressourcen zu schonen. Wird in diesem Szenario Bluetooth verwendet, so ist vor jeder Transaktion ein mehrere Sekunden dauernder Verbindungsaufbau erforderlich, während die anschliessende Übertragung des gemessenen Wertes nur einige Millisekunden in Anspruch nimmt. Dementsprechend schlecht ist Energieeffizienz, nur rund ein Tausendstel des verbrauchten Stroms konnte für das Versenden von Nutzdaten verwendet werden. Die Energieeffizienz von Bluetooth wird noch ungünstiger, wenn eine geringe Latenz benötigt wird, beispielsweise bei einem drahtlosen Lichtschalter. In diesem Fall ist es erforderlich, ständig mit dem zugehörigen Piconetz synchronisiert zu bleiben, da es inakzeptabel ist, wenn der Benutzer nach dem Betätigen eines Lichtschalters mehrere Sekunden warten muss, bis das Licht angeht. Bei einer Implementierung mit ZigBee entsteht dieser riesige Overhead nicht. Befindet sich der Sensor in Reichweite eines Koordinators, der eine Superframe-Struktur mit minimalem Beaconintervall unterhält, besteht der ganze Vorgang aus dem Abwarten des nächsten Beacons mit anschliessenden Senden der Nutzdaten und dauert im Mittel so lange wie ein Beaconintervall, also 15 ms. Nicht unerwähnt bleiben darf die Tatsache, dass nicht alle Geräte in einem ZigBee-Netzwerk gleichermassen effizient operieren können. Im soeben beschriebenen Beispiel wurde die Energieeffizienz des Lichtschalters auf Kosten des Koordinators erreicht, der in kurzen Abständen Beacons versenden muss, um die erforderliche geringe Latenz zu gewährleisten. Aus diesem Grund wird dieser Koordinator wohl am Stromnetz angeschlossen werden müssen, da eine Batterie in diesem Fall keine praktikable Laufzeit ermöglichen kann. In den von der ZigBee Alliance beschriebenen Anwendungsszenarien wird denn auch meist davon ausgegangen, dass sich typische ZigBee-Netze mit vielen Teilnehmern zusammensetzen werden aus einer Infrastuktur, bestehend aus vom Stromnetz gespiesenen Koordinatoren und Knoten mit Routing-Funktionalität, und einfachen Endgeräten, die potentiell batteriebetrieben sind. Komplett batteriebetriebene Netze mit langer Laufzeit sind nicht gänzlich unmöglich, werden sich aber nur für Anwendungen realisieren lassen, die geringe Anforderungen an die Latenz haben, so dass auch Koordinatoren einen Grossteil der Zeit in einem Standby-Modus verbringen können.
Zusammenfassend lässt sich über die jeweiligen Einsatzgebiete sagen, dass Bluetooth für grössere Datenmengen in kleinen Netzen geeignet ist, während ZigBee auf kleinste Datenmengen in grossen Netzen optimiert wurde.

5. Fazit

Durch offensichtliche Vorteile wie einfachere Handhabung und wegfallende Installationskosten lösen Funkprotokolle in vielen Bereichen kabelbasierte Lösungen ab. Die Zahl der Anwendungen, in denen drahtlose Übertragungsverfahren eingesetzt werden, wird in den kommenden Jahren mit Sicherheit noch einmal stark ansteigen.
Es hat zwar länger gedauert als ursprünglich erwartet, aber mittlerweile hat sich Bluetooth in vielen Bereichen etabliert und bei den Herstellern von entsprechenden Geräte hat sich viel Erfahrung im Umgang mit dieser Technologie angesammelt. Es kann davon ausgegangen werden, dass die Einsatzmöglichkeiten noch lange nicht ausgeschöpft sind.
Für den Einsatz des ZigBee-Standards ist die Zeit zwar noch nicht gekommen, aber die technischen Eigenschaften sind sehr vielversprechend. Auf einen geringen Preis getrimmt will ZigBee diejenigen

Märkte erreichen, in denen der Einsatz von drahtlosen Übertragungsverfahren bislang aus Kostengründen nicht möglich ist. Durch die gute Energieeffizienz sollen auch neue Anwendungen realisierbar werden, in denen mit existierenden Funkverfahren keine ausreichenden Laufzeiten möglich sind. Insgesamt lässt sich sagen, dass mit ZigBee ein Standard mit einem beachtlichen Innovationspotential geschaffen wurde. Auf die ersten Produkte, die im Verlauf des Jahres 2005 erscheinen werden, darf man also gespannt sein.

6. Referenzen

[1] Institute of Electrical and Electronics Engineers (Ed.): *IEEE Standard for Information technology -- Telecommunication and information exchange between systems -- Local and metropolitan area networks -- Specific requirements. Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LR-WPANs)*.IEEE Computer Society, New York, NY, USA, October 2003

[2] ZigBee Alliance, http://www.zigbee.org

[3] Patrick KinneyZigBee Technology: *Wireless Control that Simply Works*. http://www.zigbee.org/resources, October 2003

[4] Chris Evans-Pughe: *Bzzzz zzz -- ZigBee wireless standard*.IEEE Review, Vol. 49 No. 3, pp. 28 -- 31, March 2003

[5] E. Callaway, P. Gorday, L. Hester, J.A. Gutierrez, M. Naeve, B. Heile, V. Bahl: *Home networking with IEEE 802.15.4: a developing standard for low-rate wireless personal area networks*.IEEE Communications Magazine, Vol. 40 No. 8, pp. 70--77, August 2002

[6] J.A. Gutierrez, M. Naeve, E. Callaway, M. Bourgeois, V. Mitter, B. Heile: *IEEE 802.15.4: a developing standard for low-power low-cost wireless personal area networks*. IEEE Network, Vol. 15 No. 5, pp. 12-19, 2001

[7] M. Gaalev: *Home Networking with ZigBee*. April 2004, http://www.us.design-reuse.com/articles/article7675.html

[8] J. Bray, C. Sturman: *Bluetooth 1.1 - Connect Without Cables*. Prentice Hall, ISBN 0-13-066106-6, 2002.