Ubiquitous Computing

Maija Korsunskaja und Antje Sämann

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

“The most profound technologies are those that disappear. They weave themselves into the fabric of everyday life until they are indistinguishable from it.
[…]
Specialized elements of hardware and software, connected by wires, radio waves and infrared, will be so ubiquitous that no one will notice their presence.”
Mark Weiser

Zusammenfassung. Der von Marc Weiser geprägte Begriff Ubiquitous Computing benennt eine neue Ära des Einsatzes von Computern. Hier betrachten wir Weisers Vision des UbiComp und gehen näher auf die Technologien, Anwendungen und Probleme ein, die aus dem Einsatz des UbiComp entstehen. Besonders interessieren uns hier der Einsatz dieser Technologien im Automotive Bereich sowie die Voraussetzungen, die überhaupt vorhanden sein müssen, damit Ubiquitous Computing erfolgreich sein kann, auch seitens der Wirtschaft.

1. Die Vision des Ubiquitous Computing

Eine Zukunft im Sinne der Vision des Ubiquitous Computing, auch kurz UbiComp genannt, bedeutet, dass Computer in allen Gegenständen und Geräten eingebettet werden und sich dabei nahtlos, für den Menschen völlig unbemerkt, in seine Umgebung und in seinen Alltag integrieren. Wie in Abbildung 1 dargestellt, enthalten alle Geräte Sensoren und sind miteinander vernetzt, um Daten und Informationen aufzunehmen, zu analysieren und auszutauschen, um dem Menschen Arbeit abzunehmen und den Alltag zu erleichtern.

Fig. 1. Der Mensch in der Welt des UbiComp [28]

1.1 Grundidee des Ubiquitous Computing

> *„In the 21st century the technology revolution will move into the everyday, the small and the invisible."*
>
> Marc Weiser

UbiComp ist die dritte Welle der Computergeschichte, nach den Mainframes und der Ära des Personal Computing.
Ubiquitous bedeutet: allgegenwärtig, überall zu finden.

> *ubiquitous: (adj) seeming to be everywhere or in several places at the same time.*
>
> Oxford Advanced Learner's Dictionary

Unter UbiComp ist also die Allgegenwärtigkeit der Informationsverarbeitung und der daraus resultierende jederzeitige Zugriff auf Informationen bzw. personalisierte Dienste, unabhängig von Standort und Zugangsart, zu verstehen.
Der Begriff selbst wurde erstmals 1991 von Marc Weiser (*1952-♣1999, leitender Wissenschaftler am Forschungszentrum XEROX) in seinem visionärem Artikel „The Computer for the 21st Century" [12] eingeführt. Er propagierte UbiComp als das Gegenteil der virtuellen Realität, als ein kompliziertes Zusammenwirken von Mensch, Informatik, Technik und Sozialwissenschaften. Computer unterstützen hier unsichtbar und unaufdringlich den Menschen bei seinen Tätigkeiten und befreien ihn so weit wie möglich von lästigen Routineaufgaben. Möglich wird dies alles durch die rasante

Entwicklung der Informationstechnik (nach Moore verdoppelt sich die Leistungsfähigkeit der Prozessoren und des Speichers alle 1 ½ Jahre) sowie der drahtlosen Informationsübertragung.
Parallel zum Begriff der Ubiquitous Computing hat sich auch der Begriff Pervasive Computing durchgesetzt.

> *pervasive: (adj) present and seen or felt everywhere.*
> Oxford Advanced Learner's Dictionary

Während Weiser UbiComp eher als unaufdringliche, auf den Menschen zentrierte Technik beschrieben hat, mit der alles durchsetzt ist und die nur als Mittel zum Zweck verwendet wird, setzt die Industrie bei Pervasive Computing den Schwerpunkt auf mögliche e-Commerce-Szenarien und web-basierte Geschäftsprozesse. In dieser Ausprägung beginnt das UbiComp in der Praxis bereits Fuß zu fassen.

1.2 Paradigmen des UbiComp

Es gibt viele neue Herausforderungen, die durch die Realisierung des UbiComp entstehen. Als zentrale und fundamentale Anforderungen an Geräte, Software, Protokolle und alle anderen beteiligten Technologien gelten folgende vier Paradigmen [6]:

- Dezentralisierung
- Diversifikation
- Konnektivität
- Einfachheit

1.2.1 Dezentralisierung

In den 50er Jahren, als die ersten Computer Einzug in das Leben der Menschen hielten, gab es nur einzelne Mainframes, also Rechner, die ganze Räume einnahmen und gleichzeitig von vielen Anwendern genutzt wurden. Dieses zentralisierte Konzept wurde durch die Verbreitung der Personal Computer mit ihrer Client-Server-Architektur bereits in Richtung Dezentralisierung verändert.

Diese beiden Entwicklungen sind in Abbildung 2 gut zu erkennen, ebenso wie der starke Anstieg der Verkaufszahlen im Bereich des UbiComp in den letzten 10 Jahren.

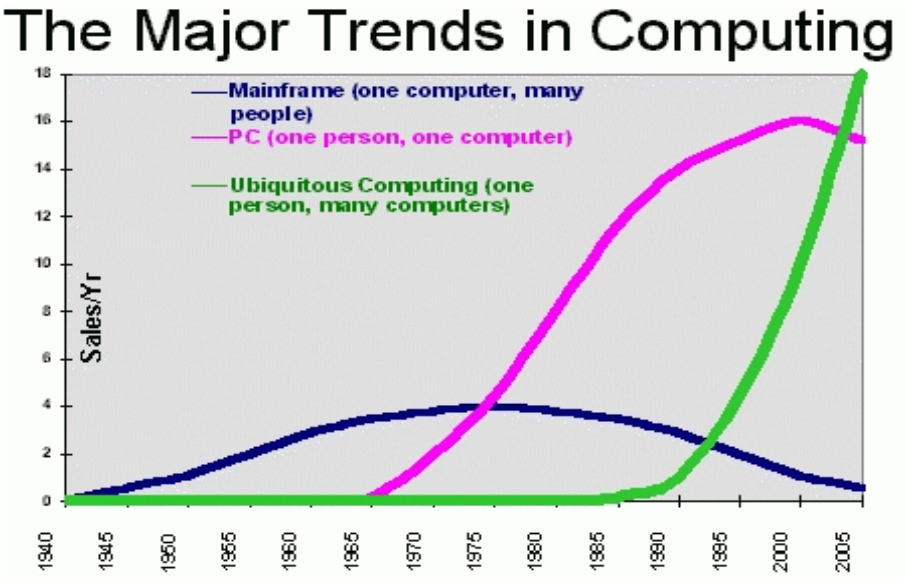

Fig. 2. Major Trends in Computing [14]

Den letzten Schritt hin zur Dezentralisierung erreichen wir mit dem Konzept des UbiComp. Hier gibt es nicht mehr einen Server, mit dem die angeschlossenen Clients Daten austauschen, kommunizieren und der das gesamte Management und die Verwaltung übernimmt, sondern diese Verantwortung wird, anhängig von der Anwendung, auf eine Vielzahl von kleinen Geräten verteilt. Es gibt keine "universelle Maschine" für alle benötigten Anwendungen mehr, sondern es findet eine Spezialisierung auf wenige Aktivitäten und Funktionen statt. All diese Geräte bilden also ein dynamisches Netzwerk durch das sie untereinander in Verbindung stehen und sich "austauschen".

Trotz dieser Konstellation muss es natürlich weiterhin möglich sein, dass die Geräte und ihre Anwendungen zu jedem Zeitpunkt auf die benötigten Daten zugreifen können. Da diese (Informationen) aber über alle Geräte des Netzes verteilt sind, müssen die Geräte in der Lage sein, sich sowohl spontan untereinander, als auch mit Desktop Applikationen (z.B. Kalender, Adressbücher) zu synchronisieren und dabei die Datenkonsistenz zu erhalten.

1.2.2 Diversifikation

Hier wird die Funktionalität der Computer bzw. Geräte betrachtet. Wie bereits erwähnt, hat der Nutzer in der Welt des UbiComp nicht mehr eine universell einsetzbare Maschine, sondern die gesamte Funktionalität wird auf viele spezialisierte Geräte aufgeteilt. Dabei ist jedes Gerät genau auf eine Situation und Umgebung

zugeschnitten. Natürlich ist es dabei möglich, dass sich einige Geräte in ihrem Einsatzbereich überschneiden, aber der Nutzer wird das für ihn passende auswählen. So hat er beispielsweise die Möglichkeit zuhause über ein “Internet Screenphone” im Internet zu surfen und dabei Multimedia in bestmöglicher Qualität zu genießen. Um unterwegs auf Informationen (z.B. Börsenkurse) aus dem Internet zuzugreifen, wird er sein Handy (WAP) benutzen und hier gerne die reduzierten grafischen Möglichkeiten in Kauf nehmen.

Um diese hohen Anforderungen zu erfüllen, ist es notwendig, die eingesetzten Technologien, wie das Betriebssystem und den Chipsatz an die Anforderungen der Applikationen (Applikation: nahtlose Integration von Hard- und Software) anzupassen. Diese vielfältigen Fähigkeiten und Charakteristika der unterschiedlichen Geräte zu koordinieren und möglichst allgemeingültige Applikationen für sie bereitzustellen, ist eine weitere große Herausforderung. Hierbei müssen besonders die großen Unterschiede im User Interface beachtet werden, wie die Darstellungsmöglichkeiten im Display, oder die unterstützen Eingabemechanismen (Stylus, function key, speech, handwriting).

1.2.3 Konnektivität

> *Everybody´s software, running on everybody´s hardware, over everybody´s network.*
>
> Lou Gerstner, CEO of IBM

Diese Aussage scheint unter den aktuellen Bedingungen nicht realisierbar zu sein. Abhängig vom verwendeten Prozessor, dem Betriebssystem, dem zur Verfügung stehendem Speicher oder Anschlüssen gibt es eine Vielzahl von Restriktionen und Unterschieden. Um diese Hürden zu überwinden, um Interoperabilität und Konnektivität zu erreichen, müssen allgemeingültige Standards für Applikationen entwickelt und etabliert werden. Und das nicht nur für die unterschiedlichen Geräte, sondern auch für die Kommunikation, Markup-Sprachen und plattformübergreifende Software.

Neue Standards in diesem Sinne sind beispielsweise WAP, UMTS, Bluetooth und IrDA, in denen nicht nur die notwendigen Kommunikationsprotokolle definiert werden, sondern auch die Basis, d.h. die physikalischen Verbindungen.
Für den Austausch von Daten und Applikationen gibt es bereits verschiedene Ansätze (Möglichkeiten). Aufgrund ihrer Plattformunabhängigkeit werden viele Anwendungen in JAVA geschrieben oder auch XML (Extensible Markup Language) zum Datenaustausch und zur Datenrepräsentation verwendet.

Auf die Konzepte von Dienstvermittlungen wie Jini, UpnP oder HAVI, die Ressourcen verwalten und Zugriffe regeln, kommen wir in Kapitel 2.2 zu sprechen.

1.2.4 Einfachheit

Die Vielzahl der Fähigkeiten, die unsere heutigen Computer besitzen, machen sie für die Mehrheit der Endbenutzer sehr kompliziert. Bereits die Installation neuer Software stellt eine Herausforderung dar und viele Anwendungen sind ohne Vorkenntnisse oder Anleitungen nicht leicht zu bedienen.

Um sich erfolgreich im alltäglichen Leben behaupten zu können, müssen die neuen Geräte und Applikationen vor allem leicht und intuitiv bedienbar sein. Jeder muss sie schnell und komfortabel nutzen können, am besten sogar intuitiv, ohne die Anleitung lesen zu müssen. Dafür muss die komplexe Technologie des Gerätes in einem sehr nutzerfreundlichen Interface versteckt werden, was hohe Ansprüche an die Entwicklung und das Design stellt, aber mit Sicherheit ein sehr entscheidender Faktor für die Akzeptanz dieser neuen Generation der Computer ist.

1.3 Perspektiven des Ubiquitous Computing

Das Paradigma des UbiComp wurde nun sehr ausführlich erläutert. Was aber sind die Dienste, die diesem zum Durchbruch verhelfen werden und wie weit ist die Technologie bereits fortgeschritten?

1.3.1 Stand der Enabling Technologies

Die Gerätegröße stellt, wie wir bereits festgestellt haben, kaum mehr ein Problem dar. Geräte wie PDAs und Subnotebooks sind mittlerweile alltäglich geworden. Computer werden testweise in alle möglichen Alltagsgegenstände integriert. Einzig der Stromverbrauch und die Stromversorgung nicht netzangebundener Geräte stellt noch ein großes Problem dar, an dem allerdings mit Hochdruck gearbeitet wird.
Dank der raschen Entwicklung der drahtlosen Netze, IrDA und Bluetooth (lokal), GPRS und UMTS (global), ist auch die Vernetzung der Klein- und Kleinstgeräte kein Problem mehr. Als Vermittlungssysteme dienen dabei die oben erwähnten Systeme wie Jini, UpnP oder HAVI, bald müsste auch die Interoperabilität dieser möglich sein. Auch die Unsichtbarkeit wird durch die Integration der Geräte in Alltagsgegenstände möglich sein. Als Eingabemöglichkeiten eignen sich Touchscreens und –pads, sowie sprach- und gestengesteuerte Geräte. Aber auch über portable Geräte soll der Dienstzugriff weiterhin möglich sein. Voraussetzung dafür ist ein portables Eingabeinterface (z.B. mittels XML oder Java implementiert, damit die Plattformunabhängigkeit gewährleistet ist).

1.3.2 Anwendungen

Auf all diesen Technologien aufbauend, unterscheidet man drei Gruppen von Anwendungen.

- **Adaptionen herkömmlicher Applikationen**: betrifft vor allem PDAs, die weiterhin eine Art überall mitnehmbarer persönlicher Minicomputer darstellen. Solche Anwendungen sind z.B. Terminkalender oder auch persönliche Adressbücher.

- **Informations- und Zugangsvermittlung**: Hierbei handelt es sich um bereits etablierte Internettechnologien, bei denen über beliebige Geräte ein Zugang zu Diensten ermöglicht wird, z.B. Kühlschrank mit integriertem Webbrowser. Dazu gehört auch die Möglichkeit, Nachrichten auf ihrem Weg in verschiedene Formate umzuwandeln (unified messaging), z.B. Sprache -> Email -> SMS -> Fax -> ...
- **Kontextsensitive Anwendungen (context-aware applications)**: Dies sind Anwendungen, deren Markteinführung noch bevorsteht. Solche Anwendungen versuchen zur Dienstbereitstellung das Umfeld (Kontext) einer Benutzerinteraktion zu erfassen und durch die Informationsauswertung dem Benutzer einen auf die momentane Situation angepassten Dienst von sich aus anzubieten.

Zum Gebiet einer kontextsensitiven Anwendung gehören der Aufenthaltsort, die Rolle des Benutzers, die Position der Geräte zum Benutzer und zueinander (location-awareness). Es wird also ein topologisches Modell der Umgebung aufgestellt.
Kontextinformationen können durch Sensoren erfassbar sein (Zeit, Licht, Temperatur) oder müssen manuell eingegeben werden (Name, Sprache, Benutzerrolle). Manuell eingegebene Informationen können aus früheren Interaktionen erlernt worden sein.
Alle diese Kontextinformationen müssen gesammelt und in eine Beziehung zueinander gebracht werden. Aus vielen konkreten Informationen entstehen so einige wenige abstrakte. Fehler sind da natürlich nicht zu vermeiden.
Aufgrund diverser möglicher Abstraktionsstufen muss für kontextsensitive Anwendungen ein Gerüst (framework) zur Verfügung gestellt werden, so dass der Zugriff auf die Informationen möglich ist, diese in Beziehung zueinander gesetzt werden, aus speziellen Informationen dann wenige spezielle hergeleitet werden und diese Kontexte dann dauerhaft gespeichert werden können.[16]

2 Technologien und Benutzerschnittstellen

2.1 Smart Devices – Smart Appliances

Mobile Geräte wie Laptops, Handys oder PDAs kennt und benutzt heutzutage fast jeder. Um Ideen wie z.B. das Intelligente Haus, das von selbst das Licht einschaltet wenn es dunkel wird und der Bewohner zuhause ist, zu realisieren, müssen Geräte aber noch zusätzliche Eigenschaften haben: Sie müssen auf Veränderungen ihrer Umwelt reagieren können, d.h. sie müssen Kontexte aufnehmen und verarbeiten können.

Dabei muss man vier verschiedene Definitionen unterscheiden [11]:

- Situation oder Situationskontext
  beschreibt die reale Welt
- Sensordaten oder situationsbezogene Daten

beschreiben die aufgenommenen Daten um die Situation wiederzugeben
- Kontext oder Kontextwissen
  ist eine abstrakte Beschreibung der Situation der realen Welt
- Kontextbezogene Applikationen oder Kontextsensitive Applikationen
  sind Verbindungen zu Applikationen, die ihr Verhalten an den Kontext anpassen

Beispiele für solche Sensoren sind Lichtsensoren, Mikrophone, Temperatursensoren, Biosensoren oder Lokalisierungssensoren (benutzen GPS oder GSM).
Auf diese Weise können Situationen der realen Welt erfasst, für die spätere Verarbeitung gespeichert werden. Entsprechend der Kombinationen von Daten kann dann eine Reaktion ausgeführt werden.

2.2 Die Middleware

Service Discovery

In Zukunft wird es immer mehr intelligente Geräte in unserem privaten und beruflichen Leben geben, die uns und sich untereinander ihre Dienste offerieren.
Dieses Serviceangebot zu organisieren, um eigene Dienste anzubieten oder nach einem bestimmten Dienst zu suchen, kann nicht durch eine zentrale Einheit gesteuert werden. Es muss eine Möglichkeit gefunden werden, dass die Geräte selbständig und dynamisch miteinander agieren, Dienste anbieten und benötigte Dienste finden.
Innerhalb eines Netzwerkes muss ein Gerät, selbständig, d.h. ohne Administration, in der Lage sein, andere Komponenten von seiner Existenz in Kenntnis zu setzen, seine Dienste anzubieten und zu beschreiben, nach speziellen Diensten zu suchen und mit anderen Geräten zu interagieren um eigene Aufgaben zu erfüllen.

Einige der bisher entwickelten Softwarearchitekturen werden nun etwas genauer betrachtet.

2.2.1 Universal Plug and Play (UpnP)

> *UPnP defines common protocols and procedures to guarantee interoperability among network-enabled PCs, appliances, and wireless devices.*
>
> Edward F Steinfeld,
> Automata International Marketing -- EDN, 13.09.2001

Das UpnP [22, 6], entwickelt von Microsoft, basiert auf TCP/IP als Kommunikationsprotokoll und nutzt XML um angebotene Dienste und Fähigkeiten zu beschreiben. Jedes Gerät, Kontrollpunkt genannt, muss eine IP- Adresse besitzen, was meist durch die Verwendung eines DHCP (Dynamic Host Configuration Protocol) Servers realisiert wird. Hierbei handelt es sich um eine Client- Server Architektur zur Verwaltung und Zuordnung von IP Adressen. Voraussetzung ist, dass die Geräte einen DHCP Client besitzen. Falls dieser nicht zur Verfügung steht, wird

die IP- Adresse mittels Auto IP ermittelt, d.h. aus einer Anzahl reservierter IP Adressen wird eine freie Adresse ausgewählt und einem Gerät zugeordnet.

2.2.1.1 Ablauf des UPnP

Das UPnP Protokoll lässt sich in fünf Schritte aufteilen:

- Discovery
- Description
- Control
- Eventing
- Presentation

Discovery

In einem Netzwerk gibt es unterschiedliche Kontrollpunkte. Das können entweder die Geräte selbst oder Service Provider sein. Diese Kontrollpunkte führen eine Liste mit allen für sie interessanten Geräten und Diensten, die in dem Netzwerk angeboten werden.

Neue Geräte beschreiben durch das Senden einer Broadcast oder Multicast Nachricht (HTTPU, oder HTTP Multicast UDP) sich selbst sowie ihre Dienste. Die Kontrollpunkte antworten durch Senden einer Nachricht in HTTPU oder HTTP Unicast UDP und fügen das Gerät bei Interesse einer Liste hinzu. Ebenso sucht ein Kontrollpunkt der neu ein Netzwerk betritt, durch das Senden einer Nachricht an alle Geräte nach interessanten Diensten. Dieser Vorgang wird durch das Simple Service Discovery Protocol (SSDP) realisiert.

Description

Die Kontrollpunkte erhalten noch in der Discovery-Phase einen URL der eine Beschreibung des Gerätes enthält. Diese Beschreibung ist ein XML Dokument und basiert auf einem UpnP Device Template. Das UPnP Forum teilt alle Geräte in Klassen ein, wobei jedem Gerät mindestens ein UPnP Template mit Vorgaben zu Inhalt und Datenpräsentation zur Verfügung steht.
Sie beinhaltet den Gerätetyp, URLs für die noch folgenden Schritte des UpnP Protokolls (Control, Eventing, Presentation), und Angaben zum Hersteller wie den Namen, Seriennummer, Produktcode usw.
Zu diesem Zeitpunkt ist der Kontrollpunkt aber noch nicht in der Lage, auf Grund der Beschreibung nach speziellen Geräten zu suchen.

Control

In diesem Schritt erhält der Kontrollpunkt die Beschreibung aller Dienste die von einem Gerät angeboten werden. Wieder basierend auf dem UpnP Template, enthält dieses XML-Dokument auch eine Liste von Aktionen mit jeweils den zugehörigen Argumenten. Der Status des Dienstes wird durch ein Set von Variablen angegeben.

Um einen Dienst in Anspruch zu nehmen, sendet der Kontrollpunkt eine “control message”, mit den Definitionen aus der Beschreibung an das Gerät. Diese Informationen werden durch das Simple Object Access Protocol (SOAP) [25] ausgetauscht, ein XML- basiertes Protokoll zum Informationsaustausch in dezentralen Umgebungen.

Eventing

Um über Änderungen der Statusvariablen eines Dienstes informiert zu werden, müssen sich die Kontrollpunkte bei dem betreffenden Gerät registrieren. Dazu sendet der Kontrollpunkt eine Nachricht an das Gerät und bekommt als Antwort die Gültigkeitsdauer seiner Einschreibung mitgeteilt. Es liegt also in der Verantwortung des Kontrollpunktes seine Registrierung bei Bedarf zu erneuern.

Haben sich eine oder mehrere Variablen geändert, so sendet das Gerät an alle registrierten Kontrollpunkte eine Nachricht (Notify). Wenn sich eine Variable zu schnell ändert, wird nicht jede Änderung einzeln gemeldet, sondern der Kontrollpunkt muss den Status abfragen.
Zum Senden und Empfangen von diesen Nachrichten über HTTP über TCP und UDP wird GENA (General Event Notification Architecture) verwendet, eine Erweiterung zu HTTP.

2.2.1.2 Protokolle des UPnP

Wie Abbildung 3 zeigt, basiert und beginnt alles mit IP [21]. Für Discovery und Events wird UDP genutzt da es multicastfähig ist. Description, Control und Presentation wird durch TCP realisiert. Die Geräte nutzen HTTPMU um ihre Präsenz im Netzwerk zu broadcasten, die Kontrollpunkte um nach den vorhandenen Geräten zu fragen. HTTPMU ist kein Bestandteil des HTTP Standard, sondern wurde, genau wie HTTPU (zur Response) extra für UPnP entwickelt.

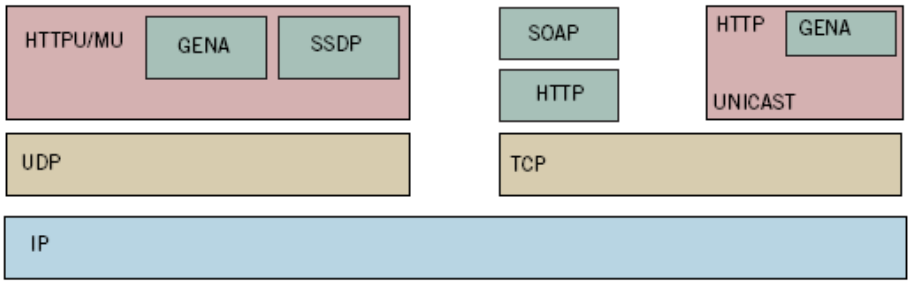

Fig. 3. UPnP - verwendete Protokolle [21]

UPnP macht keine Service Invocation. Die Geräte und ihre Dienste werden in XML-Dokumenten beschrieben, aber wie die Geräte untereinander interagieren und die Dienste nutzen, wird nicht festgelegt.

2.2.2 Jini

Jini ist ein Service Discovery System [20, 6]das auf Java basiert. Ein solches System besteht aus unterschiedlichen Komponenten, Diensten und einem Programmiermodel.

Ziel ist ein Netzwerk dynamisch zu machen, so dass es Nutzern leicht gemacht wird, auf alle im Netzwerk vorhandenen Geräte und Ressourcen zuzugreifen – auch wenn sich der eigene Standort ändert.

2.2.2.1 Infrastruktur

Alle Geräte des Netzwerkes müssen als Basis über die Java VM (Virtual Machine) verfügen und die Möglichkeit haben, entfernte Objekte mittels RMI (Remote Method Invocation) aufrufen zu können. Alternativ kann ein Proxy diese Funktionen übernehmen und die Kommandos weiterleiten, falls ein Gerät keine Java VM besitzt.
Neue Geräte (Service Provider), die ein Netzwerk betreten, nutzen als erstes das Discovery Protokoll um einen geeigneten Lookup Service ausfindig zu machen. Hierzu wird eine Nachricht im Netzwerk gebroadcastet, um alle Lookup Services von seiner Existenz zu unterrichten.

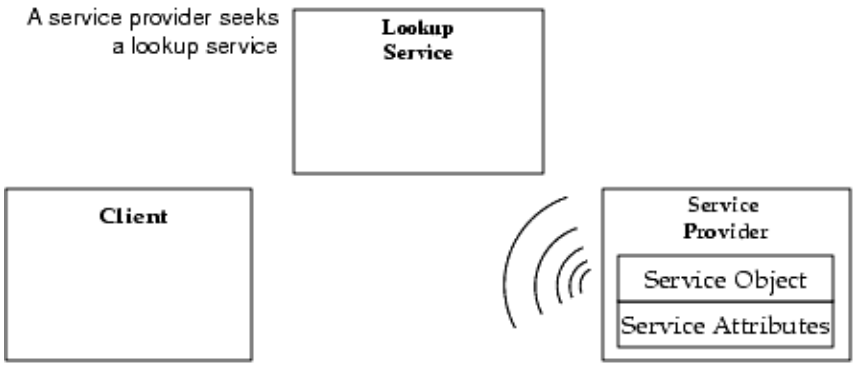

Fig. 4. Jini - Discovery [20]

Anschließend nutzt es das Join Protokoll, um sich zu registrieren und so seine Dienste anzubieten. Dazu sendet es ein Service Objekt mit Java Language Interfaces und Service Attributen an den Lookup Service.

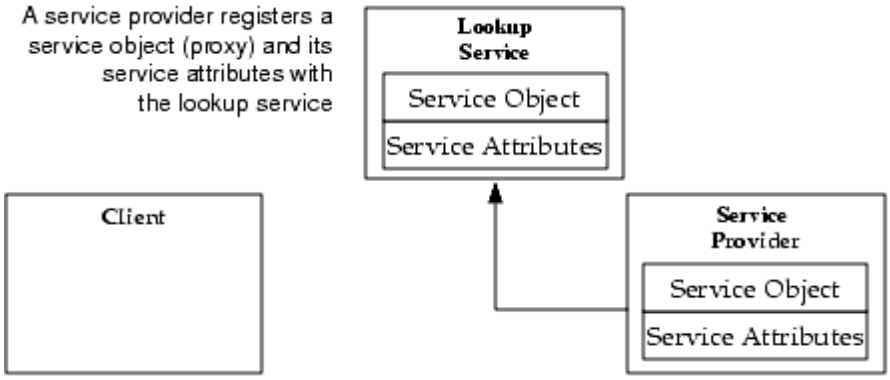

Fig. 5. Jini – Join [20]

Diese Informationen werden von dem Lookup Service in Form von Java Objekten in seiner zentralen Datenbank gespeichert und können von jedem Gerät heruntergeladen werden, das diesen Dienst in Anspruch nehmen möchte. Ein Nutzer sucht nach einem Dienst über den Typ oder eine Beschreibung.

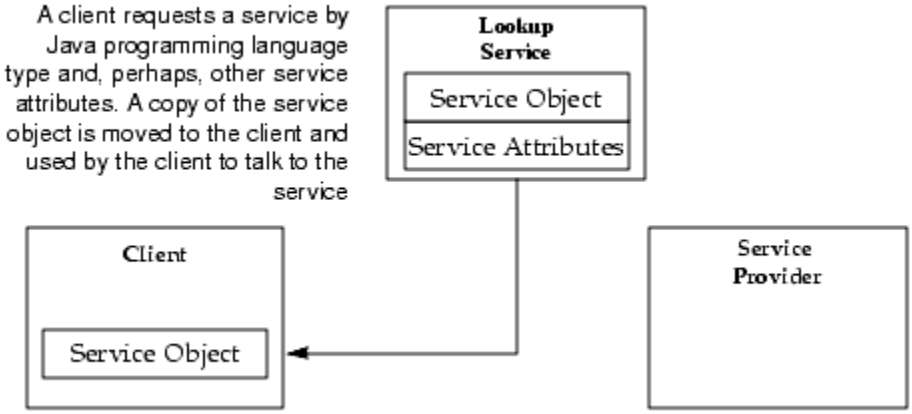

Fig. 6. Jini – Lookup [20]

Der Lookup Service stellt den zentralen Punkt des Systems dar und ist auch die Kontaktstelle zwischen dem Jini System und den Nutzern.
In dem heruntergeladenen Service Objekt sind alle Informationen enthalten, die der Nutzer benötigt, um sich zur Nutzung des gewünschten Dienstes direkt mit dem Service Provider in Verbindung setzen zu können.

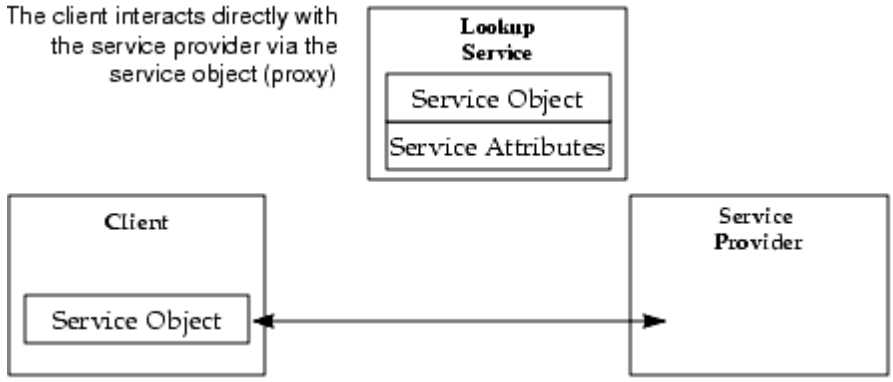

Fig. 7. Jini – Der Client nutzt den Dienst [20]

Die Einträge werden von dem Lookup Service nur für eine bestimmte Zeitspanne in der Datenbank gehalten und müssen dann von den Geräten erneuert werden, um nicht gelöscht zu werden. Auf diese Weise wird die Verwaltung der Datenbank sehr einfach und es gibt keine ungültigen, nicht mehr verfügbaren Einträge. Kommt ein neuer Eintrag in die DB hinzu oder wird gelöscht, so sendet der Lookup Service eine Benachrichtigung (Event) darüber an alle Geräte, die sich vorher dafür registriert haben.
Objekte eines Lookup Services können auch andere Lookup Services beinhalten. Auf diese Weise kann dann eine hierarchische Struktur entstehen. Außerdem können Objekte enthalten sein, die Namensdienste oder Directory Services sind und so eine Verbindung zwischen den Jini System und anderen Systemen herstellen.
Jini besitzt auch ein Transaktions-Protokoll, durch das gesichert wird, dass Transaktionen oder Dienste vollständig ausgeführt werden. In der Voting Phase werden alle beteiligten Objekte gefragt, ob sie vollständig ausgeführt wurden. Anschließend wird an die Objekte eine Bestätigung gesendet. Auf diese Weise wird sichergestellt, dass entweder alle oder keines der notwendigen Kommandos ausgeführt werden.

2.2.2.2 Das Programmiermodel

Die besondere Infrastruktur von Jini ermöglicht erst ein solches Programmiermodel.
Die Dienste, die in der physikalischen Umgebung des Jini Systems existieren, basieren auf einer Zahl von Interfaces, die die Kommunikationsprotokolle definieren und von den Diensten und der Infrastruktur genutzt werden. Diese Interfaces stellen zusammen die Erweiterung des Java Standards dar, auf dem das Jini Programmiermodel basiert.

Solche Interfaces sind beispielsweise das Transaktionsinterface oder das Leasing Interface, das festlegt, wie Ressourcen gefunden und wieder freigegeben werden (durch Nutzung eines Modells, das auf der Bearbeitungsdauer basiert).
Das Leasing Interface erweitert das Java Programmiermodel, indem es eine Zeitkomponente zu den Attributen der Referenz einer Ressource hinzufügt. Auf diese Weise ist sichergestellt, dass Referenzen auch unabhängig von eventuellen Netzwerkausfällen nach Ablauf einer festgelegten Zeit wieder freigegeben werden.
Durch die Interfaces für Event und Notification, den Erweiterungen des Event Models mit JavaBeansTM, wird eine eventbasierte Kommunikation zwischen Diensten, welche die Jini Technologie nutzen, ermöglicht.
Der Vorteil von Jini gegenüber UPnP besteht zum einen darin, über Attribute und Value Pairs nach Diensten zu suchen, was zu besseren Ergebnissen führt, und zum anderen durch die Nutzung von mobilem Code. Es besteht die Möglichkeit nicht nur Beschreibungen in der Datenbank zu speichern, sondern ganze Java Klassen, die dann von den Nutzern heruntergeladen und zum Zugriff auf den Dienst genutzt werden können.

2.3 Übertragungstechniken: IrDA, Bluetooth, WLAN

Um mobile Geräte miteinander kommunizieren zu lassen, kann eine Vielzahl unterschiedlicher Technologien genutzt werden. Jede von ihnen hat Vor- und Nachteile und spezielle Einsatzbereiche für die sie optimiert sind.

Die Einsatzbereiche lassen sich, wie in Abbildung 8 [24] dargestellt, beispielsweise durch die Übertragungsreichweite oder die Anzahl an Clients bestimmen.

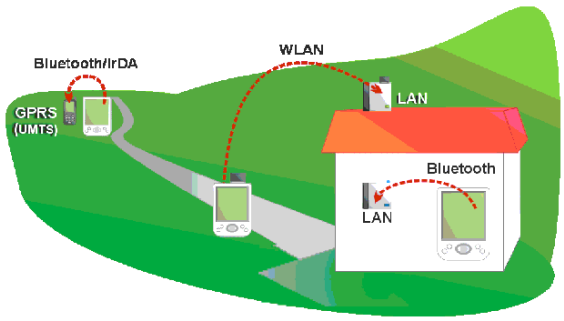

Fig. 8. Einsatzszenario [24]

Wireless LAN IEEE 802.11 (WLAN)

WLAN hat schon jetzt eine große Verbreitung und kann aufgrund seiner Reichweite und Übertragungsgeschwindigkeit auf Ethernet basierte Netzwerke ersetzen. Dieses Materie wird ausführlich im Hauptseminarthema IEEE 802.11 behandelt.

Bluetooth Standard

Mit Bluetooth sollen Funknetze mit kleiner Reichweite gebildet werden, die bisherige, auf Kabeln basierende Lösungen ersetzen oder erweitern, ad-hoc neue Netze bilden (wie in Abbildung 9 dargestellt) und gleichzeitig eine digitale Brücke zu bestehenden Netzen darstellen.

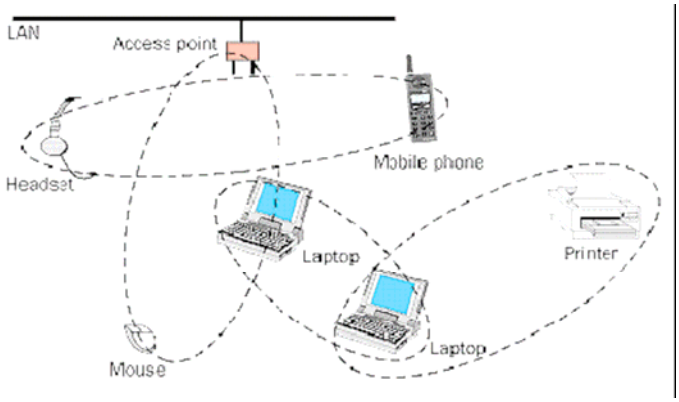

Fig. 9. Ad-Hoc Netz zwischen Bluetooth-fähigen Geräten [29]

Mehr dazu im Vortrag und der Ausarbeitung zum Thema Bluetooth.

Infrarot Kommunikation (IrDA)

Bei der Kommunikation über IrDA wird Licht im nicht sichtbaren Bereich (900 nm) verwendet, wobei zwischen sendendem Gerät und empfangendem Gerät „Sichtkontakt“ bestehen muss. Das Ziel ist eine einfache Punkt-zu-Punkt Verbindung zwischen 2 Geräten, wobei eine Bandbreite von bis zu 4Mbit/s erreicht werden kann.

Die folgende Tabelle vergleicht diese drei Technologien anhand ausgewählter Eigenschaften:

	WLAN	**Bluetooth**	**IrDA**
Durchsatz (theoretisch)	11 MBit/s	1 MBit/s	4 MBit/s (Fast IrDA)
Durchsatz (praktisch)	5 MBit/s	700 KBit/s	700 KBit/s
Reichweite	über 300 Meter	bis 100 Meter mit spez. Antennen	1 Meter
Übertragungs-	360 °	360 °	30 °

winkel			
max. Clients	256	8	2
Verbreitung/ Akzeptanz	groß, viele Implementierungen	klein, wächst aber in PDAs, Handys, Notebooks	groß (in PDAs, Handys integriert)

Tabelle 1. Gegenüberstellung der Technologien [24]

Auf Probleme und Sicherheitsaspekte dieser Technologien kommen wir in Kapitel 4 zurück.

3. Einsatzbereiche des Ubiquitous Computing

In welchen Bereichen ist nun der Einsatz von UbiComp vorstellbar?
Die Hauptforschungsfelder liegen vor allem im Bereich des Haushaltes, des Arbeitsplatzes, des Lernens und des Konsums, da diese Bereiche im täglichen Leben die meiste Zeit einnehmen.
Das vollelektronische Haus wurde schon vor längerer Zeit als Begriff eingeführt, auch sind bereits Prototypen verfügbar, obwohl sich wohl nicht die Idee als Ganzes, sondern nur Teile durchsetzen werden. Ähnliches gilt für „intelligente“ Kleidungsstücke (wearable computing). Die Akzeptanz der Entwürfe wird vor allem von ihrer Tragbarkeit und der praktischen Umsetzung abhängen.
Im Bereich des intelligenten Büros gab es frühe Forschungsprojekte von Xerox PARC, USA (1992-1994) und von GMD IPSI in Darmstadt (collaborative workspaces, collaborative learning, intelligente Möbel). Auch gibt es erste Ergebnisse und Versuche im Bereich des elektronischen Reiseführers.
Allerdings werden alle diese Projekte noch nicht aktiv im alltäglichen Leben eingesetzt. Objekte, die zur Kommunikation untereinander und mit dem Menschen besonders gut geeignet sind, sind beispielsweise Fahrzeuge. Für diese gibt es eine große Menge an Diensten, die Kommunikationseinrichtungen benötigen, außerdem sind sie aufgrund ihrer Größe, des ohnehin hohen Preises, sowie der mitgelieferten Batterie besonders für UbiComp-Anwendungen geeignet.
Im ersten Teil dieses Kapitels gehen wir auf die verschiedenen Arten der vom Fahrzeug selbst ausgehenden Kommunikation ein; besonders auf direkte Fahrzeug-Fahrzeug-Kommunikation. Dabei unterscheiden wir zwischen Client- / Server- und Peer-to-Peer-Architekturen mit den daraus resultierenden unterschiedlichen Systemgestaltungen und Kommunikationsanforderungen [7,9].
Im zweiten Teil wird noch kurz ein anderes Anwendungsbeispiel vorgestellt: die Media Cup.

3.1 Telematik

Telematik ist ein Teilgebiet der Informatik, das sich mit allen Aspekten der technischen Kommunikation zwischen räumlich getrennten Geräten und Subjekten beschäftigt. Das Wort setzt sich aus den Wörtern Informatik und Telekommunikation zusammen.
Fahrzeuge werden mit immer intelligenteren Fahrerinformationssystemen (FIS) ausgestatten. Schon jetzt gehört ein GPS-basierter Routenservice zum wählbaren Ausstattungspaket beim Autokauf. In den USA wird beispielsweise ein integriertes Notrufsystem angeboten. In nächster Zukunft soll der Fahrer die Möglichkeit erhalten, die aktuelle Verkehrssituation und weitere Informationen interaktiv im Fahrzeug z.B. aus dem Internet abzurufen, d.h. er wird, wie in der Vision des UbiComp, genau mit den Informationen versorgt die er benötigt und genau zu dem Zeitpunkt, zu dem er sie benötigt. Für das Fahrzeug bedeutet dies, dass außer der Vernetzung seiner internen Steuergeräte, auch noch eine Fahrzeugplattform für Multimedia und Infotainment mit externen Geräten geschaffen werden muss.

3.1.1 Dienste

Das Dienstangebot in Fahrzeugen wird durch drei Geräte ermöglicht: dem Autoradio, mit dem Rundfunksignale empfangen werden, dem Mobiltelefon zum Zugriff auf zellulare Netze sowie dem Navigationssystem zur Interpretation von GPS-Signalen. Aus einer Kombination bzw. Erweiterung dieser drei Grundfunktionen resultieren nun die im Fahrzeug verfügbaren Dienste. Man unterscheidet im Allgemeinen folgende drei Dienste: insassenbezogene, fahrzeugbezogene und fahrtbezogene Dienste [7].

- **Insassenbezogene Dienste:** solche Dienste erfahren sowohl innerhalb, als auch außerhalb des Fahrzeugs ihren Zweck. Die Grenzen zwischen den einzelnen Unterkategorien sind zwar schwer zu ziehen, man unterscheidet aber Informationsdienste (z.B. Auskunft, kontext-abhängige Informationen), Produktivitätsdienste (z.B. mobiles Büro) und Unterhaltungsdienste (z.B. Digital Audio Broadcast). Solche Dienste werden meistens vom Fahrzeughersteller dazugekauft.
- **Fahrzeugbezogene Dienste:** Wartungsdienste erlauben das Prüfen/ Überwachen von Fahrzeugfunktionen. Schutzdienste überprüfen dagegen die Berechtigung des Fahrers oder die Fahrzeugposition um z.B. einen Diebstahl zu vermeiden. Komfortdienste sollen die Benutzung und Bedienung des Fahrzeugs verbessern (z.B. Fahrzeugpersonalisierung). Hier hat der Automobilhersteller einen wesentlichen Anteil an der Entwicklung und Ausgestaltung.
- **Fahrtbezogene Dienste:** Diese Dienstklasse liegt thematisch zwischen den insassenbezogenen und fahrzeugbezogenen Diensten. Man unterscheidet dabei zwischen Effizienzdiensten, die sich mit Fragen der Verbrauchssteuerung beschäftigen, Sicherheitsdiensten zur Unfallvermeidung und Mobilitätsdiensten, wie z.B. dem Navigator. Aus Forschungssicht ist diese Kategorie wohl am interessantesten.

3.1.2 Bedienkonzept

Vor allem in Fahrzeugen muss das Bedienfeld so gestaltet sein, dass der Fahrer darauf zugreifen kann, ohne seine Aufmerksamkeit von der Strasse nehmen zu müssen. Deswegen sind die Input- und Outputmöglichkeiten zwar besser als bei kleinen portablen Geräten wie z.B. PDAs, jedoch ist das Desktopparadigma für FIS nicht geeignet, selbst wenn man die ausschließliche Bedienung durch den Beifahrer in Kauf nehmen würde. Das ist mit ein Grund warum man momentan möglichst sprachgesteuerte Ein- und Ausgabemöglichkeiten vorzieht.
Es haben sich einige Regeln zur Gestaltung der Multimedia-Dienste im Fahrzeug herausgebildet:

- Visuelle Ausgaben sollten möglichst nah an der Wurzel der Windschutzscheibe platziert werden. Es wird viel Wert auf eine zurückgenommene, an die unmittelbare Aufgabe orientierte Darstellung gelegt (zumindest in Europa und Nordamerika, in Japan ist genau das Gegenteil der Fall).
- Schalter sollen so positioniert sein, dass der Fahrer sie „blind“ erreichen kann. Das spricht gegen die Verwendung von Touchpads in Fahrzeugen und für multifunktionale Schalter in der Mittelkonsole und an der Mittelarmlehne.
- Einzelne Transaktionen sollen innerhalb einer kurzen Frist, meistens von nur ein paar Sekunden, abgeschlossen sein. Daher sollte die Bedienung der oben erwähnten Kombinationsschalter intuitiv möglich sein.
- Es ist jedoch immer zu beachten, dass die Aufmerksamkeit des Fahrers in erster Linie immer der Strasse zugewandt sein muss. Das führt jedoch dazu,

dass der Grat zwischen den Sicherheitsinteressen und der Bevormundung des Nutzers schmal ist. Bei einem Navigationssystem, das nur bei stillstehendem Fahrzeug bedient werden darf, stellt sich z.B. die Frage, warum während der Fahrt keine Bedienung durch den Beifahrer möglich ist.

Außer dem Problem des Bedienfeldes stellt sich die Frage nach der Personalisierung der angebotenen Dienste. Sie sollten in der Lage sein, sich in die Fahrzeugumgebung nahtlos zu integrieren, sowie den Bedürfnissen verschiedener Fahrer und Mitfahrer anpassbar sein, so dass der jeweilige Fahrer bereits beim Einsteigen ins Fahrzeug sein gewohntes und gewähltes Umfeld (Sitzeinstellung, Radiokanal, usw.) vorfindet, d.h. die Dienste sollen sich an den jeweiligen Kontext selbstständig anpassen.
Wir unterscheiden dabei zwischen adaptiven Systemen wie dem ABS und statischen Systemen, die nur auf Benutzereingaben und nicht auf Messwerte reagiert.

3.1.3 Zukünftige Dienste

Beispiele zukünftig möglicher Dienste sind ortsabhängige Dienste wie das Auffinden nahegelegener Hotels, Tankstellen, Restaurants oder auch Verkehrsinformationsdienste wie Stau- und Gefahrenwarnungen, Parkinformationen oder Notrufsysteme. Vorstellbar sind auch Multimediadienste, wie das interaktive Abrufen von Spielen, VoIP (Voice over IP, z.B. Internet-Telefonie), SMS und Email.
Die Kommunikation zwischen externen und internen Geräten wäre z.B. über Wireless LAN denkbar. Derzeit werden Ansätze untersucht in wie weit sich IEEE 802.11b für den Bereich der Fahrzeug-Fahrzeug-Kommunikation eignet. Denkbar wären Anwendungen wie Navigationsroutenübertragung vom Fahrzeug auf ein mobiles Gerät, die Informationensynchronisation oder auch das bargeldlose Bezahlen.
Das Ziel soll hier eine Reihe von Hilfs-, Unterstützungs- und Sicherheitsfunktionen sein.
Diese Inhalte werden ausführlich in den Ausarbeitungen zu den Hauptseminarthemen „Ortsabhängige Dienste“ und „Sicherheit“ behandelt.

3.2 Fahrzeuge in einer Client/Server-Architektur

Internet-Fahrzeuge (hier: jede Art der technisch-vermittelten Kommunikation in einem Netz benutzend) sind schon länger in der Autoindustrie bekannt. Das erste Exemplar dieser Art steht mittlerweile in einem Museum in Washington. Jedoch erst in den letzten Jahren kam es zu einer Serienfertigung von Fahrzeugen mit Internetanschluss.
Wie auch bei allen anderen Anwendungen kann man bei Internet-Fahrzeugen zwei Konfigurationen unterscheiden: die Nutzung als Client oder als Server. Konfigurationsabhängig entstehen nun verschiedene Nutzungsmöglichkeiten, die jedoch auch parallel existieren können. Bei insassenbezogenen Diensten fungiert das Fahrzeug beispielsweise als Client, bei fahrzeugbezogenen als Server und fahrtbezogene Dienste fallen unter eine Peer-to-Peer Architektur, die im nächsten Punkt behandelt wird.

3.2.1 Fahrzeug als Client

Als Internet-Client dient das Fahrzeug primär der Bedienung des Fahrers und der Passagiere, dabei erhält man über einen ins Fahrzeug integrierten Browser Informationen aus dem Internet. Diese Informationen sind nicht immer fahrzeugabhängig, sie werden oft auch außerhalb des Fahrzeuges benutzt, wie Nachrichten, eMail oder Unterhaltungsprogramme, die typischerweise im Internet zur Verfügung stehen. Bedienkonzepte solcher Angebote wurden bereits weiter oben abgehandelt.

Ortsbezogene Dienste

Das wohl bekannteste Beispiel ortsbezogener Dienste ist der Navigationsdienst. Hier wurden in den letzten Jahren immer mehr verschiedene Attribute hinzugefügt, so dass die Systeme nun zu mehr in der Lage sind, als nur die Fahrstrecke von A nach B zu ermitteln. Sie zeigen auch ortsbezogene Informationen, sogenannte „Points of Interest“ an, z.B. Restaurants, Einkaufsmöglichkeiten, Tankstellen oder auch Museen.

Zur Positionsbestimmung wird das GPS (Global Positioning System) benutzt. Die Genauigkeit beträgt sofern auf bordeigene Sensoren zugegriffen werden kann etwa 10m. Bei nicht ins Fahrzeug eingebauten Navigationssystemen, z.B. auf PDA-Basis, ist die Genauigkeit viel geringer, da unter bestimmten Umständen, z.B. in Tunneln oder Häuserschluchten, bei einem Signalverlust ein Wiederaufsetzen notwendig ist.
Da GPS ein amerikanisches Produkt ist, wurde von den Europäern das Satellitensystem Galileo entwickelt, das die gleiche Leistung erbringt, aber eine höhere Verfügbarkeit des Signals hat und vor allem politisch motiviert ist.
Zukünftig ist zu erwarten, dass das Kartenmaterial an dem sich Navigationssysteme orientieren, nicht mehr statisch z.B. auf CD-ROM oder DVD vorliegt, sondern direkt aus dem Internet geladen werden kann, so dass schnellere und unkompliziertere Aktualisierungen ermöglicht werden können.

3.2.2 Fahrzeug als Server

Anders etwa als bei der Verwendung des Fahrzeuges als Client lassen sich bei einer Verwendung als Server von außen Informationen vom Fahrzeug abrufen oder auch Aktionen im Fahrzeug veranlassen. Hier sind die realisierten Dienste eng mit dem Fahrzeug verbunden, wie die Fahrzeugverfolgung oder das Nachladen der Steuergeräte-Software. Besonders Fragen der IT-Sicherheit und des Datenschutzes sind dabei von Belang.

Software-Fernwartung

Aus Herstellersicht stellt die Software-Fernwartung einen vielversprechenden Dienst dar, denn mit zunehmender Komplexität der Steuergeräte und dem damit verbundenen steigenden Anteil an Software in Fahrzeugen, steigt die Wahrscheinlichkeit fehlerhafte Software aufzuspielen. Durch Software-Fernwartung

können diese Fehler behoben werden ohne dass das Auto in eine Werkstatt gebracht werden muss.
Dies jedoch setzt mehrere Aspekte voraus:

- Die Steuergerät-Software muss ersetzbar sein, d.h. sich auf einem Speicher befinden, der überschrieben werden kann.
- Die Software muss so aufgebaut sein, dass sie in Teilen ausgetauscht werden kann, damit die Menge der zu übertragenen Daten möglichst gering ausfällt. Das bedeutet, dass der Software eine gewisse Architektur zugrunde liegen muss.
- Das Einspielen der Software unterliegt strengen Sicherheitsmechanismen (Authentifizierung, Verschlüsselung usw.), damit unzulässige Manipulationen unterbleiben und auch keine Fehlfunktion mit sicherheitsrelevanten Auswirkungen auftreten kann. Hier ist zu überdenken, ob das Software-Update nur auf den Komfortbereich und nicht auf den Fahrbereich angewandt werden soll.
- Es müssen Wartungsintervalle festgelegt werden und auch der richtige Zeitpunkt der Wartung. Wartung während der Fahrzeugnutzung kann zur Folge haben, dass Funktionen eine bestimmte Zeit lang nicht verfügbar sind. Bei einer Wartung während des Fahrzeugstillstands, wie z.B. beim Parken, können wiederum Probleme mit der Energieversorgung auftreten. Auch fallen die Kontrollmöglichkeiten des Fahrers bei diesen zwei Optionen unterschiedlich aus.

Fernwartung bietet zusätzlich die Möglichkeit, komplett neue Funktionen ins Fahrzeug zu bringen. Manche davon werden allerdings ähnlich wie bei PCs auf veralteter Hardware nicht laufen. Die Fernwartung ersetzt jedoch nicht die herkömmliche Inspektion und Reparatur technischer Bestandteile, kann aber durch das Übertragen gemessener Werte, Störungen oder Schäden diese Vorgänge sehr erleichtern.

Datenschutz

Bei Datenübertragungen aus dem Fahrzeug heraus stellt sich die Frage nach dem Datenschutz. Wie sollen diese Daten verschlüsselt werden, wie sehen die Authentifizierungsalgorithmen aus bzw. inwieweit werden die Bewegungen des Fahrzeuges aufgezeichnet.
Für die Verkehrsinformation beispielsweise ist es irrelevant, welches Fahrzeug den Stau meldet, sondern dass ein Fahrzeug im Stau an einer bestimmten Strasse im Stau steht. Anders ist es jedoch, wenn keine Anonymisierung gewünscht oder ermöglicht wird.

3.3 Fahrzeug im P2P-Netzwerk

Außer der Client/Server-Kommunikation sind Anwendungen denkbar für die zwei oder mehr Fahrzeuge notwendig sind, die gleichberechtigt agieren. Bei solchen Anwendungen ist es meistens nicht von vorne herein festgelegt, welches Fahrzeug als

Server und welches als Client agiert. Zusätzlich sind sich die Fahrzeuge meist erst einmal unbekannt.
Als Beispiel: Bei einem Unfall kann ein verwickeltes Fahrzeug an andere, sich in einem bestimmten Umkreis befindliche Fahrzeuge eine Gefahrenmeldung ausstrahlen, wie im Bild 10 dargestellt.
Auch die Routenführung kann als P2P-Anwendung realisiert werden. Jedes Fahrzeug sammelt die von anderen Verkehrsteilnehmern gesendeten Informationen und rekonstruiert damit dezentral die Verkehrslage. Ein zentraler Dienst wird damit obsolet [7, 9].

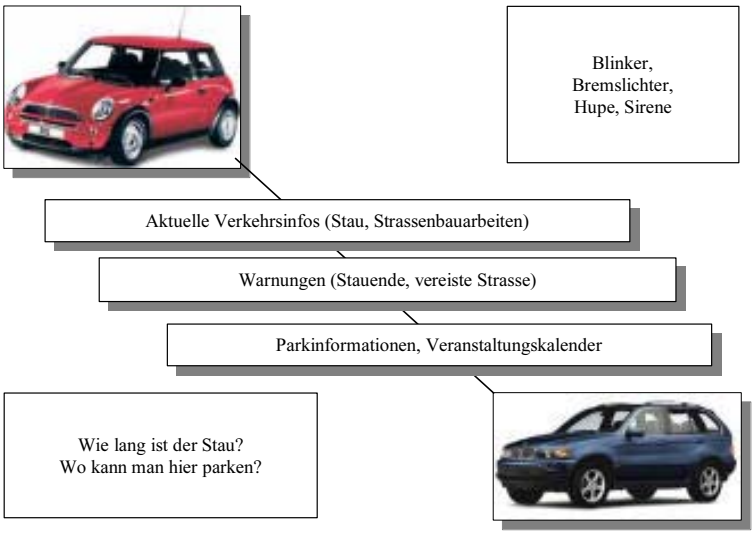

Fig. 10. Fahrzeug-Fahrzeug-Kommunikation [1]

3.3.1 Lokale, spontane Kommunikation

P2P-Kommunikation ist eng mit der Idee verbunden, dass Fahrzeuge freiwillig Daten bereit stellen, was in großem Stil nur möglich ist, wenn dies nicht mit Kosten verbunden ist. Kostenfreie Kommunikation ist aber nur möglich, sofern keine Netz-Infrastruktur neu geschaffen werden muss. So beschränkt sich die Wahl auf einfache Sender mit geringer Reichweite.
Hier ist die Idee der spontanen Interaktion von Maschinen, wie im UbiComp- Ansatz beschrieben, am besten umgesetzt. Die Interaktion muss sich dabei nicht nur auf Fahrzeuge beschränken, sondern kann auch auf die Interaktion zwischen Infrastruktur und Fahrzeug ausgedehnt werden. So kann auch die Strasse selbst eine Warnmeldung rausschicken oder die Feuerwehr bei Ölverlust alarmieren. Im Bild 11 sind Beispiele möglicher Fahrzeug-Infrastruktur-Kommunikationen dargestellt.

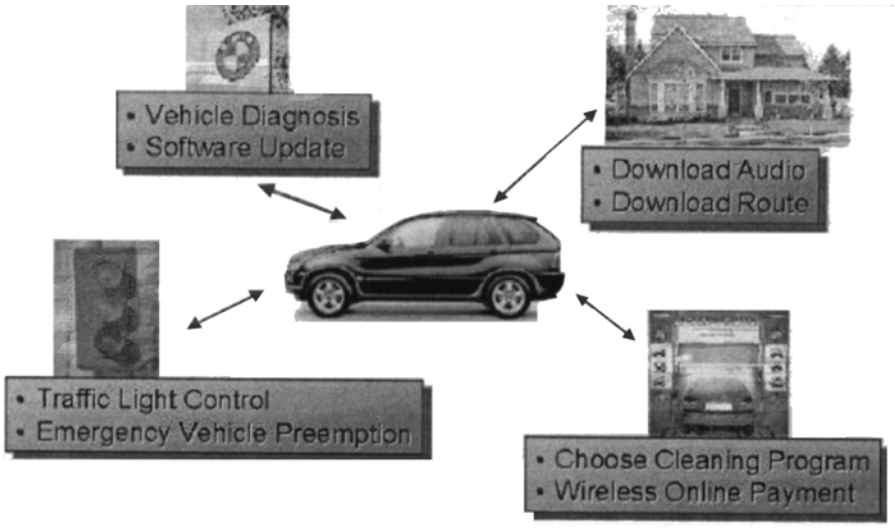

Fig. 11. Fahrzeug-Infrastruktur-Kommunikation [1]

Ein Problem stellt jedoch die Durchsetzung dar. P2P-Netzwerke funktionieren erst dann, wenn andere Teilnehmer in der Nähe sind. Wenn sich aber auf diesem Streckenabschnitt keine bzw. keine anderen mit den notwendigen Kommunikationssystemen ausgestatteten Fahrzeuge befinden, ist auch eine Kommunikation zwischen Fahrzeugen nicht möglich. Im Gegensatz dazu entscheidet der Fahrer eines mit Client oder Server-Diensten ausgestatteten Fahrzeuges, ob und wann er einen Dienst nutzen möchte.

3.3.2 Kommunikationssysteme

Alle in diesem Kapitel beschriebenen Fahrzeuge gehen von dem Vorhandensein eines Kommunikationssystems aus, das möglichst ins Fahrzeug selbst eingebaut ist und zum Senden und Empfangen von Daten verwendet wird. Das Kommunikationssystem selbst muss drahtlos und mobil sein und möglichst noch folgende Anforderungen erfüllen [7].

- Durchsatz / Bandbreite ist für Anwendungen die große Datenmengen versenden relevant.
- Die Latenzzeit eines Systems, also die Zeit, die maximal zwischen Senden und Empfangen einer Nachricht verstreicht, sollte für sicherheitsrelevante Anwendungen so kurz wie möglich sein.
- Anschaffungs- und Nutzungskosten des Kommunikationssystems spielen für die Aktualität der Anwendungen eine große Rolle.
- Verfügbarkeit des Kommunikationssystems sollte hoch sein. Man unterscheidet zwischen Weitverkehrsnetzen und lokalen Netzen, auf die hier jedoch nicht näher eingegangen wird.

Zusätzlich stellen verschiedene Anwendungen unterschiedliche Anforderung an das Kommunikationssystem. Die Zusammenhänge kann man in der Tabelle 2 gut erkennen.

Anwendungstyp	Bsp.	Adressierung und Lokalisierung	Multihop Routing [1]	Filter	Inhalts-Caching	Internet Protokolle	Sicherheit
Asynchrone Fzg-Fzg-Kommunikation	Verkehrs-informationen		X	X	X	(X)	X
Synchrone Kommunikation	Sprache-, Daten-übertragung	X	X			X	X
Lokaler Zugangspunkt	Internet-Zugriff	X	X		X	X	X
Informations-bereitstellung	Location based services			X	X	(X)	X

Tabelle 2. Anforderungen an unterschiedliche Anwendungen [1]

3.3.3 Adhoc P2P-Netzwerke

Wie bereits weiter oben erläutert, dienen P2P-Anwendungen der direkten Fahrzeugkommunikation. Informationen, die die Sensoren des einen Fahrzeuges sammeln, werden an alle anderen Fahrzeuge weitergeleitet, die an diesen interessiert sind, so z.B. Stau- und Unfallwarnungen, Bauarbeiten, Straßenschäden usw.
Multihop-Routing ist eines der Forschungsthemen in diesem Bereich. Bisherige Algorithmen speicherten und aktualisierten die Routing-Tabellen in den Netzwerkknoten und waren daher für eine große Teilnehmeranzahl und die Dynamik vieler Fahrzeug-Fahrzeug-Kommunikationsanwendungen ungeeignet. Vorteile der ad-hoc-Routing Algorithmen machen diese aber aufgrund ihrer Skalierbarkeit und geographischen Routing-Strategien für genau diese Anwendungen interessant [1].

Proaktive Protokolle

Proaktiv bedeutet, dass jemand etwas ohne Aufforderung tut, in diesem Zusammenhang z.B. wenn ein mobiler Knoten ohne Aufforderung anfängt eine Weiterleitungsforderung für eine Nachricht zu verarbeiten. Dazu speichert die Einheit Routing-Tabellen, die Informationen über den nächsten Knoten, der eine Nachricht an

das eigentliche Ziel weiterleitet, beinhalten, die den Status des Gesamtnetzwerks darstellen und ständig aktualisiert werden (s.h. Bild 12).
Ein einfacher Algorithmus wäre hier der Distributed Bellman-Ford Algorithmus, im Internet unter RIP bekannt.

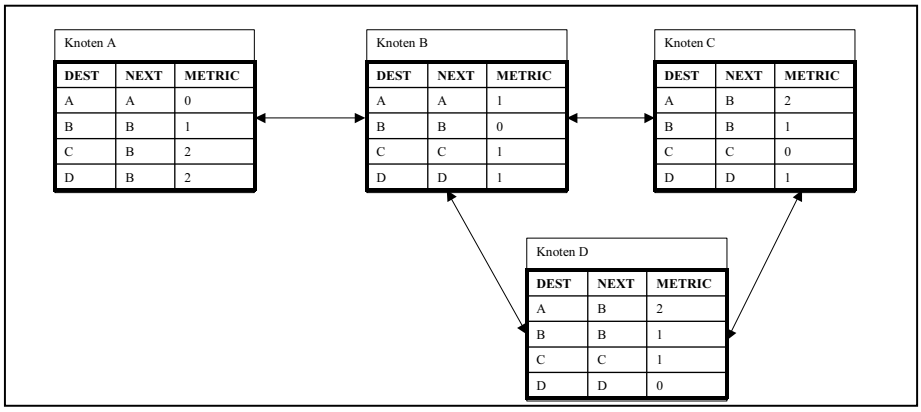

Fig. 12. Destination-Sequence-Distance-Vector Routing[1]

Hohes Verkehrsaufkommen und häufiger Standortwechsel führen jedoch zu einem sehr hohen Control Traffic. Bei sehr großen und sich schnell ändernden Netzen können die Tabellen nicht schnell genug aktualisiert werden, was zu veralteten Einträgen führt. Auch wenn diese Schwächen beseitigt werden sollten, sind proaktive Protokolle für große Netzwerke nicht geeignet.

Reaktive Protokolle

Solche Protokolle speichern in ihrer einfachsten Version keinerlei Daten über das Netzwerk im Voraus. Das bedeutet, dass der Knoten seine Arbeit aufnimmt ohne die Routingpfade zu kennen und muss diese jedes Mal neu aufbauen.
Bekannte Protokolle sind das Dynamic Source Routing (DSR) und das Ad Hoc On-Demand Distance-Vector Routing (AODV).

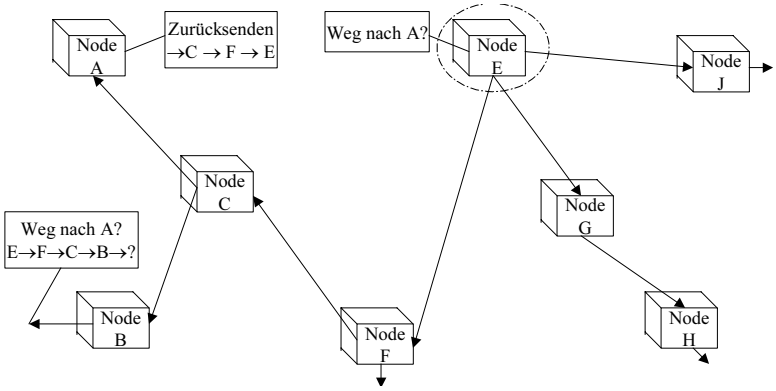

Fig. 13. DSR [1]

Bild 13 zeigt ein Beispiel dafür, wie bei DSR der Weg zu einem Knoten entwickelt wird. Knoten E schickt eine Weg-Anfrage-Nachricht (Route-Request: RREQ)an alle Knoten mit dem Ziel den Weg zu A zu erfahren. Wenn die RREQ den Zielknoten A erreicht, sendet dieser eine Antwort-Nachricht (Route-Reply: RREP) zurück. Diese beinhaltet alle Knoten-IDs, die benötigt werden um die Nachricht an die Zieladresse weiterzuleiten. Der Rückweg ist dabei nicht notwendigerweise symmetrisch. Die Quelle packt die empfangene Liste in den Datenpaket-Header. Jeder Knoten, der dieses Paket empfängt, liest diese Liste und entscheidet, ob er die Nachricht weiterleitet oder nicht.
Der Algorithmus kann bereits bekannte Routen benutzen, so dass die RREQ nicht unbedingt das Ziel erreichen muss,um die endgültige Nachricht zuzustellen, wenn anderen Knoten der Weg zum Ziel bereits bekannt ist.
Das hat natürlich auch seine Grenzen, z.B. funktioniert das Protokoll nur bei einem Netzwerk, das unter 200 Knoten besitzt, da die Routing-Liste proportional zur Anzahl der Weiterleitungen wächst. Außerdem ist durch die Notwendigkeit den Weg zu „entdecken“, sowie bei großer Mobilität, der Control Traffic sehr hoch.

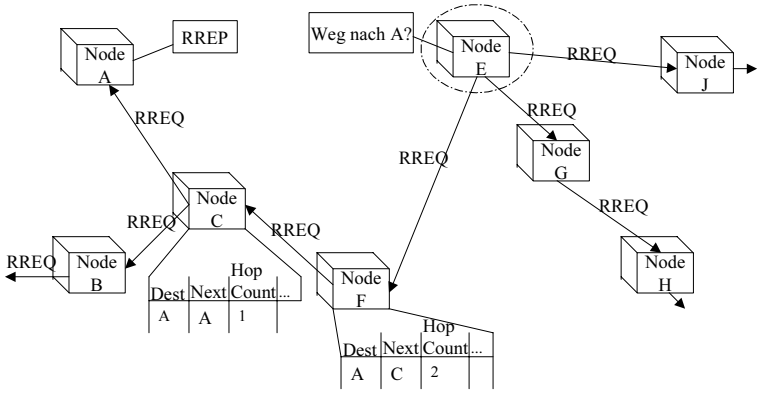

Fig. 14. AODV [1]

Der AODV Algorithmus speichert in jedem Knoten die Informationen verschiedener Routen. Im Bild 14 ist ein Beispiel dafür dargestellt. Hier benötigt der Knoten E den Weg zum Knoten A und sendet daher ein RREQ an alle erreichbaren Knoten aus. Falls der Knoten A diese Nachricht erhält, sendet er ein RREP zurück. Alle Knoten, die die Nachricht erhalten, vergleichen sie mit ihrem Cache. Falls ein Eintrag für diese Route existiert, wird eine Nachricht in Richtung Quelle weitergeleitet bis die Verbindung hergestellt ist und eine Kommunikation stattfinden kann.
Dieser Algorithmus ist zwar skalierbar, jedoch bei sehr großen Netzwerken kann keine Kommunikation zwischen sehr weit entfernten Knoten stattfinden.
Um dieses Problem zu beseitigen, hat man eine Vielzahl hybrider Ansätze entwickelt, auf die hier nicht näher eingegangen wird. Bisher funktioniert jedoch keiner von ihnen optimal.

3.4 MediaCup

Media Cup ist ein einfaches Beispiel dafür, wie smarte Dinge im Sinne des UbiComp eingesetzt werden können.
Media Cup ist eine Kaffeetasse, ausgestattet mit Sensoren und Kommunikationseinrichtungen, die im Tassenboden Platz finden. Sie sammelt Informationen über ihre Umwelt und leitet diese weiter. Aus dieser Tasse kann zusätzlich auch noch getrunken werden.
Die Tasse ist im Rahmen des RAUM-Projekts seit September 1999 im Einsatz [15].

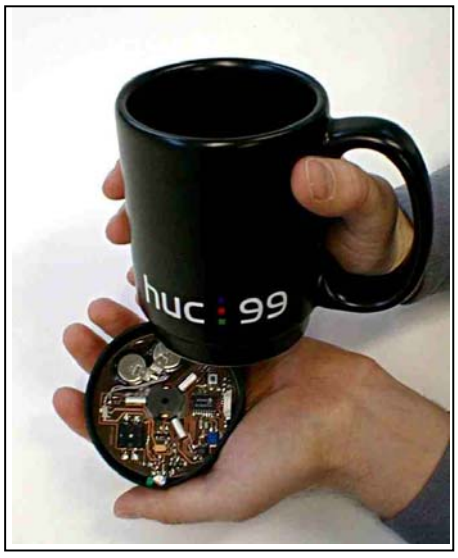

Fig. 15. Media Cup [15]

3.4.1 Anwendungen der MediaCup Umgebung

Nachfolgend werden einige der MediaCup zugeordnete Geräte kurz beschrieben. Man unterscheidet dabei grundsätzlich zwei Klassen von Anwendungen: Benutzeranwendungen und Software für die Netzwerk-Infrastruktur.

HotClock

HotClock ist eine Armbanduhr, die Temperatur und Status der MediaCup anzeigen kann. Zusätzlich warnt sie, wenn der Kaffee zu heiß ist, ihre nähere Umgebung durch einen Piepston. Um das zu ermöglichen, enthält die onhandpc Armbanduhr eine IrDA Schnittstelle, über die Daten empfangen werden können. Die Software der Uhr muss jedoch separat gestartet werden.

Smart DoorPlate

Smart DoorPlate baut auf der MediaCup und dem RAUM System auf. Sie ist eine Art elektronisches Türschild und kann die Situation „Besprechung“ anhand der von den Tassen gesendeter Daten, z.B. die Tassenaufstellung oder der gleichzeitigen Benutzung mehrerer Tassen in einem Raum, erkennen. Wird diese Situation erkannt, so wird als Warnung „Meeting“ auf dem LCD Display ausgegeben. Die derzeitige Version wird auf einem Windows-Rechner betrieben, wobei das Display seriell mit diesem Rechner verbunden ist.

CoffeePump

CoffeePump ist eine Kaffeemaschine mit erweiterter Funktionalität. Sie brüht neuen Kaffee auf, falls der Kaffee alle ist und alle Tassen ausgetrunken sind.

3.4.2 Technische Details

Der Kern der MediaCup Umgebung besteht aus der MediaCup selbst, der Netzwerkinfrastruktur und der Aufladeelektronik.
Die Elektronik der MediaCup ist in einem Gummisockel im Tassenboden integriert und kann so vor dem Spülen entfernt werden. Das Aufladen der integrierten Batterie geschieht durch das Platzieren der Tasse in einer extra entwickelten Untertasse, wobei schon 15 Minuten reichen, um die Tasse 10 Stunden lang mit Energie zu versorgen.

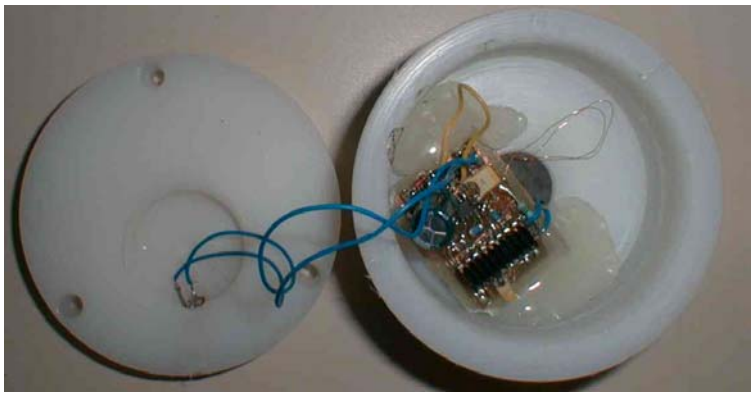

Fig. 16. Ladegerät: Untertasse [15]

Die Elektronik spürt, ob die Tasse benutzt wird und misst laufend die Getränktemperatur. Die Tasse kennt also ihren eigenen Zustand. Diese Informationen werden dann andere Smarte Dinge im Raum (z.B. Kaffeemaschine) weitergeleitet.
Im RAUM System werden drei verschiedene Arten von technischen Systemen unterschieden: Netzwerk-Systeme, Objekte und das Lokalisationssystem.
Im Netzwerk wurden als Verbindungen IrDA, ASK (kabellos) und Ethernet, CAN (kabelgebunden) ausgewählt.
Objekte haben verschiedene Kommunikationsbedürfnisse. Man unterscheidet hier zwischen Nur-Sendenden (z.B. MediaCup), Nur-Empfangenden (z.B. im RAUM System SmartDoorplate, HotClock, WebVis) und Sendenden-und-Empfangenden (z.B. AIDE) Objekten.
Im Location System wird momentan nur Infrarot-Technologie zur Bestimmung der Objektposition benutzt.

4 Probleme des UbiComp

Es gibt im Bereich des UbiComp noch einige Probleme, die zu lösen sind, damit sich diese neue Ära richtig durchsetzten kann.
Beispiele für solche Probleme sind:

- Sicherheitsaspekte wie Datenschutz, Abwehr von Angriffen, Schutz vor Viren, etc.
- Schutz der Persönlichkeitsrechte des Menschen
- Management begrenzter Ressourcen (z.B. Speicherkapazität, Energie)
- Synchronisierung der Daten
- Einfache Bedienbarkeit für größere Akzeptanz
- Gesetze an neue Technologien anpassen, bzw. neu entwickeln (z.B. Verbraucherschutz)

Im folgenden werden einige dieser Punkte etwas genauer beschrieben.

4.1 Sicherheit

Allgemein kann man zwischen der IT-Sicherheit (security) und der Funktionssicherheit (safety) unterscheiden [2, 6, 27].

Die IT-Sicherheit beschäftigt sich damit, wie Bedrohungen oder Angriffe von außen abgewehrt werden können. Die Funktionssicherheit dagegen befasst sich mit dem Fehlerverhalten des IT- Systems und Möglichkeiten zur Einschränkung (z.B. die Ausfallsicherheit steigern, oder die Zuverlässigkeit erhöhen). In dieser Arbeit möchten wir uns nur mit der IT-Sicherheit befassen.

4.1.1 Aufgaben der IT-Sicherheit:

Zentrales Ziel der IT-Sicherheit ist es, Informationen und Daten vor unautorisierten Zugriffen und Manipulationen zu schützen.

Um das garantieren zu können, muss als erstes die Identität des Nutzers bzw. des Gerätes, mit dem Daten ausgetauscht werden sollen, geprüft werden. Das geschieht durch Authentisierungsverfahren in denen nach einem Passwort oder einer PIN gefragt wird oder durch Verwendung von besonderen Protokollen wie beispielsweise SSL. Auf die Problematik, wie beide Kommunikationspartner ein geheimes Passwort austauschen können, kommen wir später zu sprechen (s.h. auch Skript Verteilte Systeme).

Nachdem sich der Kommunikationspartner korrekt authentifiziert hat, muss vor dem Zugriff auf Daten noch geprüft werden, ob er dafür autorisiert ist.

Eigenschaften /Forderungen an die IT-Sicherheit

- **Vertraulichkeit**
  Es muss sichergestellt werden, dass vertrauliche Informationen nur an berechtigte Empfänger weitergegeben werden. Beispiel hierfür wäre eine Flugbuchung über das Internet; Informationen wie die Kreditkartennummer und Gültigkeit sollen nur der Fluggesellschaft bekannt werden und keiner dritten Partei.
- **Integrität**
  Hier geht es um die Datenintegrität, d.h. Daten sollen nur von autorisierten Personen oder Geräten verändert oder gelöscht werden können.
- **Verfügbarkeit**
  Es soll gewährleistet sein, dass nach korrekter Authentifizierung und Autorisierung, der Zugriff auf die Daten auch möglich ist.
- **Verbindlichkeit**
  Nachdem Daten verändert wurden, soll es im Nachhinein möglich sein festzustellen, wer diese Änderungen vorgenommen hat. Bei einem Aktienkauf soll später nicht behauptet werden können, man wollte zu diesem Preis nie kaufen.

- **Privatsphäre**

Auf Grund der Vielzahl an Informationen über Handlungen eines einzelnen Menschen ist es leicht möglich, detaillierte Profile über ihn zu erstellen und so sein Kommunikationsverhalten, besuchte Websites oder besuchte Orte genau wiederzuspiegeln. Zum Schutz der Privatsphäre sollen diese Informationen jeweils nur zweckgebunden und ausschließlich an den Kommunikationspartner weitergegeben werden.

4.1.2 Bedrohungen:

Fast an der Tagesordnung sind Angriffe auf die Identität eines Partners. Bei diesen *Maskierungs-Angriffen*, Spoofing genannt, werden falsche Absender-Adressen bei Emails oder Datenpaketen und Signalnachrichten angegeben um beispielsweise Viren zu versenden oder den Empfänger dazu zu verleiten, falsche Daten von einem vermeintlich bekannten Absender zu verarbeiten.

Bekannt sind auch *Man-in-the-Middle-Attacken* bei denen der Angreifer komplett den Part eines der Kommunikationspartners übernimmt, seine Identität fälscht und so die Forderung nach der Verbindlichkeit von Handlungen unterläuft. Hierbei kann auch die Datenintegrität gefährdet werden, wenn Datenpakete abgefangen und dann verändert werden.

Das Abhören von Daten (*sniffen*) wie z.B. Passwörtern zählt zu den häufigsten Angriffen auf Daten. Es gibt hierfür sogar Tools zum Download im Internet.

Bei *Denial-of-Service-Angriffen* wird versucht, einen Server durch eine große Anzahl von Anfragen so zu überlasten, dass es ihm nicht mehr möglich ist, seine Dienste anzubieten. Eine solche Attacke wird bei einer kleinen Firma nicht die Existenz gefährden, kann einen kommerziellen Web-Server wie amazon.com aber durchaus in Gefahr bringen.

Um sich gegen solche Angriffe zu schützen, wurden unterschiedliche Verfahren entwickelt. Zur Absicherung bei der Authentifizierung können Chipkarten verwendet werden, die Zugangs- und Authentifizierungsdaten speichern. Für die Vertraulichkeit wurden eine Vielzahl an Verschlüsselungsverfahren entwickelt, ebenso wie für die Integritätsprüfung.

Schwierig ist es immer noch sich gegen Denial-of-Service-Angriffe zu wehren. Meistens wird der Datenverkehr über das Netz beobachtet, Muster erstellt und Abweichungen von diesen Mustern werden als Angriff gedeutet. Durch das Abbrechen der Verbindung zu dem Rechner der diese Abweichung verursacht hat, versucht man den Angriff abzuwehren.

Digitale Signaturen werden an Nachrichten angefügt um den Anforderungen nach Verbindlichkeit nachzukommen, allerdings ergibt sich hier wiederum das Problem, die Signaturen verifizieren zu können

4.1.3 Spezielle Risiken und Probleme bei Nutzung mobiler Technologien:

Bei der Nutzung von drahtlosen Technologien zur Kommunikation muss man immer berücksichtigen, dass Daten, die über die Luftschnittstelle übertragen werden, im Prinzip von jedem abgehört werden können. Wie weiter oben bereits erläutert, ist es mit WLAN möglich, Entfernungen von über 300 m zu überbrücken, was bedeutet, dass potentielle Angreifer sich nur in der Nähe aufhalten müssen, um an die Daten

heranzukommen. Im Internet gibt es eine Reihe von frei verfügbaren Programmen, mit denen ganz einfach nach Access Points gesucht werden kann, indem die Signalisierungsnachrichten abgehört werden. Diese Tools zeigen häufig eine Vielzahl von Informationen über die Access Points an, wie beispielsweise ihren Namen und den Hersteller. Da viele Benutzer die voreingestellten Werte (z.B. für Passwörter zur Konfigurierung oder Schlüssel zur Verschlüsselung) der Hersteller nicht abändern, ist es sehr leicht, Zugriff auf ihre Daten zu bekommen.

Die Bildung von Ad-hoc-Netzen stellt eine wichtige Basis in der Welt des UbiComp dar. Dadurch entstehen aber auch viele Probleme. Wie kann man, ohne vorab schon mal Kontakt gehabt zu haben, eine Vertrauensbeziehung aufbauen? Woher weis man, dass man mit dem richtigen Kommunikationspartner verbunden ist? Wie kann zur Abrechnung für in Anspruch genommene Dienste eine Rechnung gestellt, bzw. im Zweifelsfall die Benutzung nachgewiesen werden?

Da die mobilen Endgeräte alle mittels GSM, UMTS, GPRS oder WLAN miteinander verbunden sind, kann es ab und zu passieren, dass in einem Funkloch keine Verbindung zu bekommen ist. Die Verfügbarkeit einer Ressource oder eines Dienstes kann also nicht durchgehend garantiert werden, was wiederum Angriffsfläche für Eindringlinge bietet.

Auf Grund der geringen Größe der Geräte ist die Gefahr natürlich sehr groß, dass sie irgendwo vergessen, liegengelassen oder gestohlen werden. In einem Artikel des BBC heißt es, dass innerhalb von nur sechs Monaten allein in Londoner Taxen 1300 PDAs, 2900 Laptops und 62.000 Handys liegen geblieben sind. Während die Wiederbeschaffung des Gerätes oftmals durch Versicherungen abgedeckt ist, sind die gespeicherten Daten, deren Wert meistens viel höher als der der Hardware ist, verloren, und keine Versicherung zahlt dafür.

Außerdem besteht die Gefahr, dass der Benutzer bei der Eingabe seiner PIN oder von einem Passwort beobachtet werden kann und so eine dritte Person in den Besitz dieser Informationen kommt.

4.1.3.1 GSM/ GPRS:

Wie wir bereits wissen, wird bei GSM und GPRS die Identifikation des Gerätes durch die SIM- Karte vorgenommen, auf der die IMSI, der geheime Schlüssel, sowie weitere Informationen zur Verschlüsselung der Daten gespeichert ist. Auf die Sicherheitsprobleme wie z.B. die nur einseitige Authentifizierung oder die Sicherung der Datenintegrität möchten wir hier nicht erneut eingehen, sondern auf die Vorlesungen Mobilkommunikation I + II verweisen.

4.1.3.2 WLAN:

Die einfachste Möglichkeit seinen Access Point (AP) vor unberechtigten Zugriffen zu schützen ist die, eine Zugriffsliste zu erstellen und darin alle Rechner und Devices mit ihrer Media Access Control Adresse (MAC) aufzuführen, die berechtigt sind im Funknetz zu arbeiten [2]. Allerdings ist hier eine manuelle Verwaltung notwendig, was je nach Netzumfang sehr aufwendig werden kann.

Durch das Wired Equivalent Privacy Protokoll (WEP) [27] soll eine sichere Punkt-zu-Punkt Kommunikation ermöglicht werden. Das WEP ist ein optionaler Bestandteil

des IEEE Standards 802.11 und ist in den AP integriert. Die Geräte müssen, um mit einem AP kommunizieren zu können, nachweisen, dass sie im Besitz eines geheimen Schlüssels S (40 Bit, 104 Bit, in 802.11a 152-Bit) sind, welcher vorab durch einen Administrator sowohl im AP als auch bei allen Endgeräten einzutragen ist.

Die Abbildung 17 auf der nächsten Seite veranschaulicht den Ablauf der Verschlüsselung mit dem WEP Protokoll.

Zur Verschlüsselung der Daten werden die Datenpakte mittels des RC4 Verfahrens codiert. Hierbei wird, basierend auf dem bekannten Schlüssel S und einem zufällig gewählten 24 Bit- Wert, dem Initialisierungsvektor (IV), ein Bitstrom erzeugt, mit dem die zu sendenden Daten mittels XOR verknüpft werden (Stromchiffre). Der Empfänger erhält, zusammen mit den verschlüsselten Daten den IV (unverschlüsselt mitgesendet) und kann die Nachricht entschlüsseln.

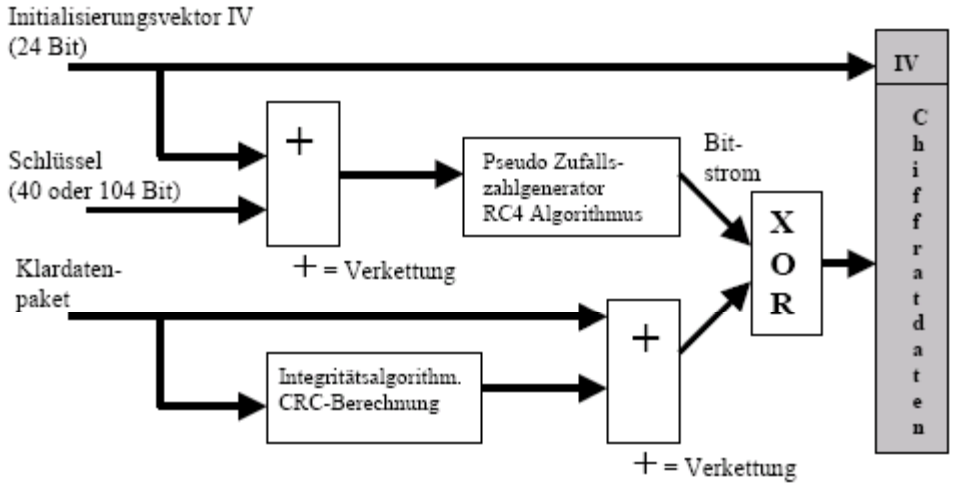

Fig. 17. WEP Protokoll [27]

Zur Prüfung der Datenintegrität wird über jedes Datenpaket eine Prüfsumme (CRC) berechnet und mitgeschickt.

Probleme des WEP

Da alle Geräte eines Funknetzes den selben geheimen Schlüssel S verwenden, ist es in einem großen Netzwerk unmöglich auf diese Art einen Rechner oder gar Nutzer zu authentifizieren. Hinzu kommt, dass wegen der Art und Weise wie der Schlüssel S in die Geräte eingetragen wird es ab einer gewissen Anzahl von Netzwerkteilnehmern unmöglich ist, ihn abzuändern, da das bei jedem Gerät manuell zu machen ist.
Als Standard sieht das WEP die Verwendung eines 40-Bit-Schlüssels vor. Diesen zu berechnen dauert heutzutage allerdings nur 15 Minuten; für den 104 Bit langen Schlüssel braucht man immerhin rund 40 Minuten.

Wie auch beim GSM, muss sich der AP nicht gegenüber den Geräten authentifizieren, was wieder die Möglichkeit zum AP Spoofing (falscher AP sendet mit hoher Signalstärke und überlagert so den echten AP) einräumt.
Hinzu kommt, dass die Verschlüsselung der Daten auch von diesem Schlüssel abhängig ist. Auf Grund der geringen Länge des IV von 24 Bit ist die Wahrscheinlichkeit, dass er sich innerhalb einer kurzen Zeitspanne wiederholt, sehr groß. Zeichnet ein Angreifer über einen Zeitraum alle Datenströme auf, ist er schnell in der Lage, den Schlüssel zu knacken und die Daten zu lesen oder zu manipulieren. Auch hierfür gibt es im Internet bereits Programme zum Herunterladen.

Um die Integritätsprüfung zu umgehen, muss von dem Angreifer nur nach Änderung der Daten die Prüfsumme angepasst werden. Hier stellt das WEP also gar keinen Schutz dar.

Der WEP Standard sieht derzeit keine Unterstützung für erweiterte Authentifizierung, wie z.B. Zertifikate, Smartcards oder biometrische Sicherheitsvorrichtungen vor.

Ausblick

Um diese Probleme zu lösen, wird Ende diesen Jahres mit IEEE 802.11i ein neuer Standard eingeführt werden, der mehr Sicherheit bieten soll.

- Sicherung der Vertraulichkeit und Integrität
  Hier wird ein neues auf AES (Advanced Encryption Standard) basierendes Protokoll, sowie das TKIP (Temporal Key Integrity Protokoll), welches eine Kompatibilitätslösung zu WEP darstellt, benutzt.
- Benutzerauthentisierung und Schlüsselmanagement
  Protokolle basierend auf IEEE 802.1X

Der AES [30], entwickelt vom National Institute of Standards and Technology (NIST), ist ein symmetrischer Block Cipher zur Ver- und Entschlüsselung von Daten. Er basiert auf dem Rijndael Algorithmus und kann 128 Bit lange Datenblöcke mit einem 128, 192, oder 256 Bit Schlüssel verschlüsseln. Mehr zu AES ist nachzulesen im Vorlesungsskript zu „IT- Sicherheit - Sicherheit vernetzter Systeme“ von Prof. Dr. H.G. Hegering, oder unter http://csrc.nist.gov/CryptoToolkit/aes/.

WPA (Wi-Fi Protected Access) als Zwischenlösung zu IEEE 802.11i:

IEEE 802.1X ist hier optional für die Benutzerauthentisierung und das Schlüsselmanagement vorgesehen. TKIP basiert weiterhin auf WEP, ermöglicht aber eine dynamische Erneuerung des Schlüssels für jedes Datenpaket, erweitert den IV und setzt zusätzlich zum CRC einen kryptographischen Message Integrity Check (MIC), genannt „Michael“ ein.

Ein kritischer Punkt von WPA ist der Kompatibilitätsbetrieb eines Access- Points, in dem er sowohl mit WPA als auch mit WEP arbeiten kann. Prinzipiell kommunizieren

zwar alle WPA- fähigen Clients mit dem AP über WPA; Multicast- und Broadcast-Nachrichten werden aber grundsätzlich mit WEP verschlüsselt. Außerdem sind Clients, die nicht WPA-fähig sind, zumeist auch nicht kompatibel mit 802.1X, wodurch die Authentisierung und der dynamische Schlüsselwechsel umgangen werden können.

4.2 Ressourcenknappheit und Umweltbelastung

Die meisten Gegenstände in der Welt des UbiComp sollen klein, leicht und einfach mitzunehmen sein. Auf Grund dieser Eigenschaften, die in engem Zusammenhang mit der Mobilität stehen, sind die Möglichkeiten beispielsweise für Speicherkapazität und Energie/ Akkus sehr beschränkt. Um die zur Verfügung stehenden Ressourcen so sinnvoll wie möglich einzusetzen wurden verschiedene Ansätze entwickelt, auf die nun kurz eingegangen wird.

4.2.1 Energiemanagement

Eine Möglichkeit besteht darin, Applikationen in einen Energiesparmodus wechseln zu lassen, eine andere ist, dem Betriebssystem die Kontrolle über das Energiemanagement zu übertragen, so dass es dynamisch auf die sich ändernden Anforderungen reagieren kann[19, 4, 5]. Dabei müssen vor allem 2 Probleme berücksichtigt werden. Es muss ein Ressourcenmanagement entwickelt werden, dass Verschwendung und Overhead minimiert, bzw. ganz verhindert und gleichzeitig eine effiziente Nutzung der Energie sicherstellt.

Ein Beispiel hierfür ist das ECOSystem, das Energie als eine „first class system resource“ versteht [19], die genau wie alle anderen Ressource von den Applikationen angefordert werden muss.
Wie auf dem folgenden Bild zu sehen, ist es durch Einsatz periodischer Korrekturmaßnahmen gelungen, die prognostizierte Lebenszeit einer Batterie tatsächlich zu erreichen, während ohne Beeinflussung das Ziel um ca. 10% unterschritten wurde.

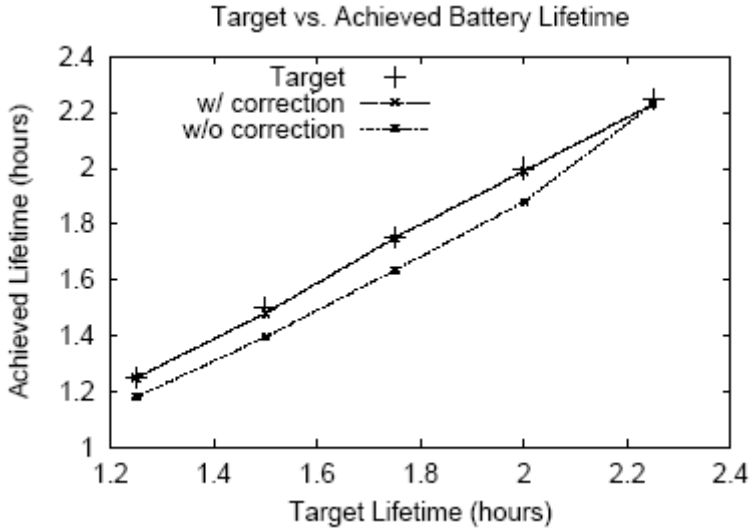

Fig. 18. Erreichen der prognostizierten Lebenszeit einer Batterie [19]

Das folgende Bild veranschaulicht, wie sich der Energieverbrauch beim Abspielen eines Videos in Abhängigkeit vom eingesetzten Energiemanagement verändert.

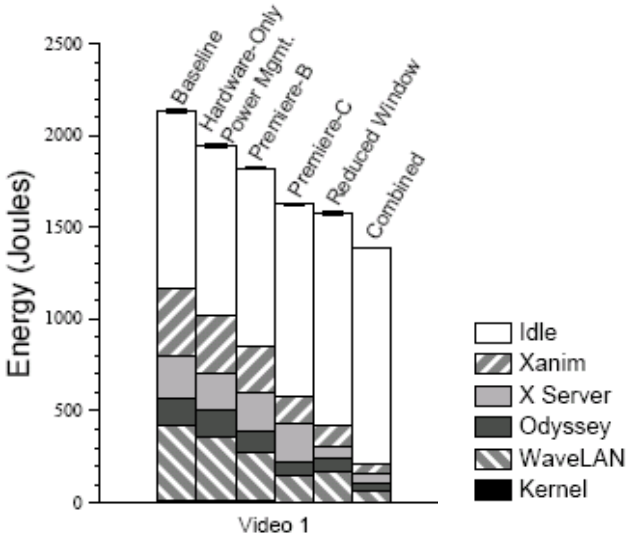

Fig. 19. Energieverbrauch beim Abspielen eines Videos [4]

Der erste Balken zeigt den Energieverbrauch ganz ohne jedes Management, im zweiten wird ein Hardware Power Management eingesetzt. Im 3. und 4. werden die Daten komprimiert, im 5. die Fenstergröße verkleinert und der letzte Balken kombiniert diese beiden Aspekte, wodurch eine Energieersparnis von 30% erreicht werden kann.

Allgemein lässt sich sagen, dass mit dem richtigen Management viel Energie eingespart werden kann. Allerdings kommt es bei der Entscheidung für ein System zum Energiesparen immer auf den Kontext an, d.h. es muss berücksichtigt werden, welches Gerät vorliegt, welche Applikationen ausgeführt werden sollen und letzten Endes muss der Nutzer entscheiden, ob er bestimmte Einschränkungen (z.B. schlechtere Auflösung) in Kauf nehmen möchte.

4.2.2 Umweltbelastung

Unumstritten sind die Gesundheitsgefahren, die durch Elektrosmog verursacht werden. Bereits jetzt werden Benutzer mobiler Telefone davor gewarnt, ihre Geräte zu nahe am Körper zu tragen. Allgegenwärtige Computer in Miniaturform vervielfachen alleine durch ihre Anzahl die möglichen Risiken.
Auch die Energiebilanz, besonders bei der Fertigung, minituarisierter Geräte ist sehr hoch. Wenn also auf jeden Menschen viele Computer bzw. Geräte kommen und diese die gleichen, nur mit hohem Energieaufwand produzierbaren Bestandteile enthalten, ist zu überlegen, wie das Recycling vonstatten gehen soll, vor allem da die Lebensdauer solcher Geräte meistens nicht sehr hoch ist.

5. Ubiquitous Computing aus betriebswirtschaftlicher Sicht

Mittels UbiComp können die meisten physischen Dinge von „dumm“ zu „intelligent“ umgewandelt werden. Jedes Produkt bzw. Produktionsmittel enthält einen Mikrochip und wird damit zu einem denkenden Ding. Solche Dinge können, selbstständig Umgebungsinformationen (Temperatur, Lagerort) aufnehmen, verarbeiten (zu hohe Temperatur, falscher Lagerort), versenden (Achtung! Warnung!) und somit ohne menschliche Hilfe und Medienbruch untereinander und mit der Welt der IT kommunizieren.

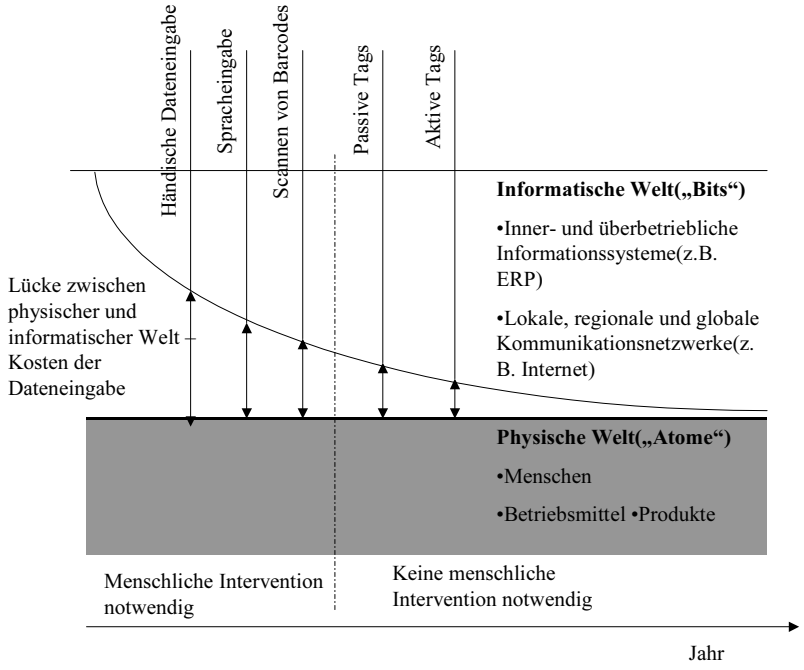

Fig. 20. Medienbruch [3]

Ein Medienbruch ist vergleichbar mit einem fehlenden Kettenglied innerhalb einer Informationskette und ist mitunter die Ursache für viele Probleme inner- und überbetrieblicher Prozesse. Ein Beispiel ist die mehrfache Erfassung eines Auftrags in unterschiedlichen betrieblichen Informationssystemen innerhalb einer Wertschöpfungskette. Das Ziel der Vermeidung von Medienbrüchen bedingt, dass die Lücke zwischen der physischen und der informatischen Welt geschlossen wird und der Mensch als Mediator zwischen diesen zwei Welten nicht mehr gebraucht wird.
Die Folge der Veränderungen durch UbiComp sind neue Geschäftsprozesse, die sowohl Kunden als auch Lieferanten hohen Nutzen bieten. Sie helfen durch niedrige Durchlaufzeiten und Lagerbestände, die Risiken und Kosten zu reduzieren und ermöglichen viele neue Services und die Individualisierung bzw. Personalisierung von Gütern während ihrer gesamten Lebensdauer.
Ähnlich wie bei eBusiness werden sich bei UbiComp wohl nur die Anwendungen und Szenarien durchsetzen, die den Wert und Gewinn von Unternehmen (Shareholder Value) nachhaltig erhöhen [3, 18].

5.1 Thesen zu den Auswirkungen des Ubiquitous Computing

Es lassen sich zwei Thesen über die Auswirkungen des UbiComp aufstellen:

- UbiComp hilft, die Lücken zwischen realer und informatischer Welt zu schliessen. Es verhindert so Medienbrüche im großen Rahmen und führt zu einer neuen Ebene der Automatisierung.

- UbiComp ermöglicht mittelfristig dem physischen Objekt das autonome Sammeln, Verarbeiten und Senden von Informationen und fördert damit die dezentrale Informationsverarbeitung.

5.2 Automatisierung und Verteilung von Intelligenz

Die derzeitige Forschung und Praxis konzentriert sich primär auf die Vernetzung von Unternehmen, Prozessen, Informationssystemen und Menschen. UbiComp adressiert dabei das größte Problem der Informationsverarbeitung: den Medienbruch bei der Dateneingabe.
Mit den heutigen Mitteln z.B. manuelle Eingabe per Tastatur, Spracheingabe oder Barcode scannen ist die Vermeidung dieses Medienbruches noch nicht möglich. Jedoch zeigen aktuelle Entwicklungen wie z.B. im Bereich von passiven und aktiven Tags, die auf der Radio Frequency Identification Technologie (RFID) basieren, einen möglichen Entwicklungspfad auf.
Passive Tags sind kleine mit Antennen ausgestattete Mikroprozessoren ohne eigene Energiequelle, aktive Tags dagegen besitzen eine Batterie. Tags ermöglichen neue Szenarien in denen Unternehmen ihre Produkte animieren (statten Sie beispielsweise mit Intelligenz aus und verknüpfen sie automatisch mit internen und externen Informationssystemen). Dies ermöglicht wiederum eine neue Qualität an zentral und dezentral gesteuerten Prozessen, die zu Preisvorteilen und Vorteilen bei inner- und überbetrieblicher Logistik führt.
UbiComp ermöglicht die Verteilung von Wissen an die Orte, an denen das Wissen verwendet oder erzeugt wird. Das kann sowohl ein globales Informationssystem als auch eine lokale Gruppe intelligenter Dinge sein. Dazu schreibt K. Kelly :

> *„Numerous small things connected together into a network generate tremendous power. But this swarm power will need some kind of minimal governance for the top to maximize its usefullness.[…] With the invention of a few distributed systems. Such as the ingernet, we have merely probed the potential of what minimally centralized networks can do…" [8]*

UbiComp kann durch die Verwendung intelligenter Dinge die Steuerung komplexer Systeme in einem ganz anderen Licht erscheinen lassen. Diese Fähigkeit zur Komplexitätsbewältigung wirkt sich natürlich auch auf die betriebliche Informationsverarbeitung aus, denn derzeit können aufgrund der kostenintensiven Architekturen und des Medienbruches Dateneingabe nur die teueren (A-)Ressourcen zeitnah in den Informationssystemen abgebildet werden. Die massenhaft vorkommenden billigen (C-)Ressourcen dagegen bleiben dabei aufgrund der mangelnden Wirtschaftlichkeit außen vor.

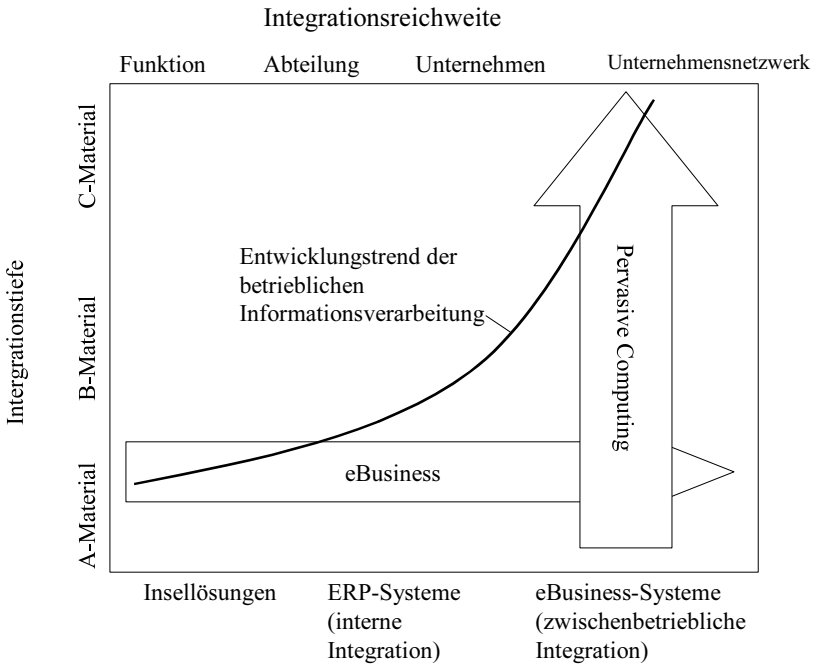

Fig. 21. Ubiquitous Computing und eBusiness Entwicklungstrend [3]

Genau diese Integrationstiefen, nämlich die Einbindung der B- und C-Ressourcen, kann UbiComp durch den Einsatz intelligenter Geräte und Dinge bewirken, ohne eine Kostenexplosion zu verursachen. Es wird sich aber noch in der Praxis zeigen müssen, ob diese Annahme ihre Richtigkeit hat.
E-Business dagegen beschreibt den Trend zur Ausdehnung der Integrationsreichweite auf Organisationseinheiten, wie Portale oder eCommerce-Systeme. Diese Einheiten integrieren einzelne Prozesse über Unternehmensgrenzen hinweg.
Sowohl UbiComp als auch eBusiness, bauen auf dem Internet auf und müssen durch die vielen Überschneidungen ihre Lösungen aufeinander abstimmen.

5.3 Selbstbestimmung

Die Geräte im Pervasive Computing Konzept sind zwar unsichtbar, aber durch die Verbindung ihrer Applikationen zur Geschäftswelt wahrscheinlich nicht besonders leise, denn sie wissen ja um einiges besser was der Benutzer will und meistens schon bevor er das überhaupt weiß. Wenn also über den Benutzer Daten gesammelt werden, um den Kontext besser erkennen zu können, ist die Frage, wie diese verwendet werden. Nicht nur die Speicherung und Vorhaltung dieser Daten ist aufwendig, es besteht auch noch die Gefahr, das der Mensch zu einem „gläsernen“ Menschen wird

über dessen Verhalten und Gewohnheiten jeder Auskunft bekommt, der Zugriff auf die Systeme hat.
Die für den Verkäufer besonders interessante Frage „Wo bekomme ich das Produkt XY, schnell und billig?“ wird so zu einer Farce, denn wohl selten wird der Informationsversorger unabhängig vom Hersteller und Betreiber des Systems agieren.

6. Schlussbetrachtung

Ob und in welchem Ausmaß sich die neuen Technologien in unseren Alltag integrieren, lässt sich nur schwer abschätzen.
Wie wir gesehen haben, sind in einigen Bereichen, wie z.B. in den Autos oder in Museen mit virtuellen Führern bereits einige Ideen umgesetzt, auf anderen Gebieten gibt es bislang nur Forschungsprojekte oder wenige Prototypen.
Die Akzeptanz bei den Endnutzern hängt dabei von einer Vielzahl von Bedingungen ab, wie der Einfachheit in der Bedienung, dem Preis für die Geräte, der Verlässlichkeit und der Funktionalität - um nur ein paar zu nennen.
Einige wenige Ideen werden sich letzten Endes durchsetzen und von vielen Menschen genutzt werden (wie mit Handys schon geschehen), viele andere werden aber über den Status eines Prototyps nicht hinauskommen.

Literaturverzeichnis:

[1] Bogenberger, Richard; Kosch, Timo (2002): Ad-hoc Peer-to-peer Communication-webs on the Street. 9th World Congress on Intelligent Transport Systems (ITS 2002). Chicago, USA 2002.

[2] Eckert, Claudia (2003): Mobil, aber sicher! In: Mattern, Friedemann: Total vernetzt. Szenarien einer informatisierten Welt. Springer-Berlin Heidelberg New York. S.85-121.

[3] Fleisch, Elgar (2001): Betriebswirtschaftliche Perspektiven des Ubiquitous Computing. In: Buhl, H.U.; Huther, A.; Reitwiesner, B.: Information Age Economy, Heidelberg, S. 177-191.

[4] Flinn, Jason; Satyanarayanan, M.(1999): Energy-aware adaptation for mobile applications. In: ACM Symposium on Operating Systems Principles, Charleston, USA, S. 48 - 63

[5] Gupta, S. K. S.; Lee, W.-C.; Purakayastha, A.; Srimani, P.K.(2001): Pervasive Computing: Vision and Challenges. In: IEEE Personal Communications, Vol. 8, Nr. 4, August 2001, S. 8-17.

[6] Hansmann, Uwe ; Merk, Lothar; Nicklous, Martin S.; Stober, Thomas (2000): Pervasive Computing Handbook. Springer Verlag Berlin Heidelberg.

[7] Herrtwich, Ralf G.(2003): Fahrzeuge am Netz. In: Mattern, Friedemann: Total vernetzt. Szenarien einer informatisierten Welt. Springer-Berlin Heidelberg New York. S.63-83.

[8] Kelly, K. (1998): New Rules for the New Economy. New York.

[9] Kosch, Timo; Michel, Hans-Ulrich; Steinberg, Karl-Ernst; Bonenberger, Hermann (2001): Multimediatechnologie im Automobil. In: Tagungsband Informationstage „Mobile Computing“ 2001; Universität Regensburg.

[10] Mattern, Friedemann (2003):Vom Verschwinden des Computers – Die Vision des Ubiquitous Computing. In: Mattern, Friedemann: Total vernetzt. Szenarien einer informatisierten Welt. Springer-Berlin Heidelberg New York. S.1-42.

[11] Schmidt, Albrecht; Laerhoven, Kristof van (2001): How to Build Smart Appliances? In: IEEE Personal Communications, Vo. 8, Nr.4, August 2001, S 66-71.

[12] Weiser, Marc (1991): The Computer for the 21st Century. In: Scientific American, 09-1991, S. 99-104.

[13] Want, Roy (2000): Calm Technologie and Pervasive Connectivity. In: IEEE Personal Communications, Vol.7, Nr. 1, February 2000, S. 8 – 10.

Internetquellen:

[14] http://www.ubiq.com/hypertext/weiser/UbiHome.html vom 21.07.2003

[15] http://mediacup.teco.edu vom 21.11.2003 und 27.11.2003

[16] http://www.informatik.tu-darmstadt.de/BS/Lehre/Sem00_01/Ausarbeitungen/ Christopher-Huhn-Ubicomp.pdf vom 18.08.2003

[17] http://www.ecommerce.wiwi.uni-frankfurt.de/pfaff/publikationen/ beitrag_liechtenstein.pdf vom 21.07.2003:
Pfaff, Donovan; Skiera, Bernd (2002): Ubiquitous Computing – Abgrenzung, Merkmale und Auswirkungen aus betriebswirtschaftlicher Sicht. In: Britzelmaier, Bernd (Hrsg): „Wirtschaftsinformatik: Der Mensch im Netz – Ubiquitous Computing, 4. Liechtensteinisches Wirtschaftsinformatik-Symposium an der Fachhochschule Liechtenstein“, Teubner-Reihe Wirtschaftsinformatik, Leipzig.

[18] http://www.m-lab.ch/pubs/publications.html vom 21.07.2003: **Fleisch**, Elgar; Christ, Oliver: Ubiquitous Computing: Von der Vernetzung von Computern zur Vernetzung von Dingen.

[19] http://www.informatik.uni-trier.de/~ley/db/indices/a-tree/v/Vahdat:Amin.html:

Zeng, Hang; Ellis, Carla S.; Lebeck, Alvin R.; Vahdat, Amin (2002) :ECOSystem: Managing Energy as a First Class Operating System Ressource, Department of Computer Science, Duke University 2002.

[20] http://www.jini.org/nonav/standards/davis/doc/specs/html/jiniTOC.html

[21] http://www.ednmag.com, September 2001, S. 65 – 70

[22] http://www.upnp.org/

[23] http://www-3.ibm.com/software/pervasive/index.shtml

[24] http://www.gwdg.de/forschung/publikationen/gwdg-nr/GN0209/gn0209_03.html

[25] http://msdn.microsoft.com/msdnmag/issues/0300/soap/default.aspx

[26] http://www.teco.edu/~michael/publication/mediacup_full.pdf

[27] http://www.bsi.bund.de/literat/doc/wlan/wlan.pdf - Sicherheit im Funk- LAN, Bundesamt für Sicherheit in der Informationstechnik

[28] http://w4.siemens.de/FuI/en/archiv/pof/heft2_02/artikel13/
Internet – Ubiquitous Computing, Inside the All-Inclusive Network

[29] http://www.dfki.de/%7Ekrueger/iiu/iiu05112001.pdf
Krüger, Antonio, Unversität des Saarlandes, Vorlesung "Intelligente Instrumentierte Umgebungen", Kommunikationsstrukturen, Positionierungstechnologien

[30] http://csrc.nist.gov/CryptoToolkit/aes/
AES – Advanced Encryption Standard