Mobile Systems II

Burkhard STILLER
Oliver BRAUN
Arnd HEURSCH
Peter RACZ
(Hrsg.)

Institut für Informationstechnische Systeme, IIS

Bericht Nr. 2003-04
October 2003

Universität der Bundeswehr München

Fakultät für

INFORMATIK

Werner-Heisenberg-Weg 39 • D-85577 Neubiberg

B. Stiller, O. Braun, A. Heursch, P. Racz (edts.): Mobile Systems II
Technical Report No. 2003-04, September 2003
Information Systems Laboratory IIS, Departement of Computer Science
University of the Federal Armed Forces Munich
Werner-Heisenberg-Weg 39, D-85577 Neubiberg, Germany

Introduction

The Information System Laboratory (Institut für Informationstechnische Systeme, IIS) of the Department of Computer Science, University of the Federal Armed Forces Munich, Germany offered its students again a seminar on Mobile Systems during the spring term 2003 (FT03).

While today's mobile system require protocol as well as technology support, only a variety of underlying services will complement the pure systems view point toward a complete communication network. Therefore, this year's seminar addressed two services in wireless networks and focussed on one technology comparison. In consequence, a review of several challenges and weaknesses of those technologies and services for a mobile world is required. The talks in this seminar are providing an approach to judge their dedicated suitability.

Content

This second edition of the seminar – entitled "Mobile Systems II" – discusses in the first section a service called positioning. The required systems for such a task as well as the techniques to be applied in the world are being discussed. While the satellite-based positioning based on GPS and GALILEO are introduced, cell-based telecommunication systems and their positioning techniques are addressed as well. The second section addresses the access of directories in mobile environments. Following the presentation of the X.500 directory service the LDAP (Light-weight Directory Access Protocol) is summarized. By combining those two parts a model for accounting WLAN (Wireless Local Area Network) has been developed and the suitability of the LDAP protocol in wireless accesses is discussed. Finally, the third section worked on two technologies in the wireless domain: WAP (Wireless Application Protocol) and i-mode. The protocol architecture of WAP 1.x and 2.x are outlined and applications for such a model are described. This part is complemented by the summary of the i-mode architecture and its sample applications. This section concludes with a comparison of both approaches.

Seminar Operation

All interested students worked on an initially offered set of papers and book chapters, relating to the topic titles as presented in the Table of Content below. They prepared a

written essay as a focussed presentation, an evaluation, and a summary of those topics of interest. Each of these essays is included in this technical report and allows for an overview on important areas of concern, business models in operation, and problems encountered. In addition, every student prepared a slide presentation of approximately 45 minutes to present his findings and summaries to a varying audience of students attending the seminar and other interested students or research assistants. Following a general question and answer part, a student-lead discussion debated lively open issues and critical statements with the audience.

Local IIS support for preparing talks, reports, and their preparation by students had been granted Peter Racz, Arnd Heursch, Oliver Braun, and Burkhard Stiller. A larger number of pre-presentation discussions have provided valuable insights in the emerging and moving field of Mobile Systems, both for students and supervisors. Many thanks to all people contributing to the success of this event, which has happened in a small group of highly motivated and technically qualified students and people.

Inhaltsverzeichnis

Kapitel 1

Positioning Systems and Techniques

Stefan Burkhard

Kabellose Kommunikationssysteme sind zur Zeit sehr populär. Sie nehmen in der heutigen Zeit immer mehr Dienste wahr und ermöglichen uns, an fast jedem Ort, mobil und von Kabelnetzen unabhängig, das Internet und andere Dienstleistungen in Anspruch zu nehmen. Viele dieser Dienste sind von der Position des Mobilgerätes und der Position des Nutzers abhängig. Ist die Position des Nutzers bekannt, kann der Anbieter gezielt für den Anwender weitere Dienste, wie Routenplanung oder das Anzeigen von Freizeitmöglichkeiten in der Umgebung, anbieten. Vieles davon ist schon in Betrieb und weitere Möglichkeiten werden sich eröffnen, wenn die Genauigkeit der Standortbestimmung zunimmt, oder die Systeme miteinander gekoppelt werden.
Diese Arbeit beschäftigt sich mit den Möglichkeiten der Positionsbestimmung in heutigen und in einigen zukünftigen Systemen. Dazu wird zwischen Navigation und Mobilfunk unterschieden.
Im ersten Abschnitt wird auf die Navigation eingegangen, bei der Satellitensysteme die grundlegende Technik sind. Wie funktioniert Satellitennavigation? Was für Systeme sind in Betrieb und welche werden in der Zukunft unseren Alltag bereichern? Diese Fragen werden, wie gesagt, im ersten Abschnitt beantwortet.
Der zweite Abschnitt klärt Fragen zur derzeitigen Mobilfunktechnik. Wie wird die Position in heutigen Netzen bestimmt? Welche Verfahren gibt es? Und wie genau sind diese? Hierbei wird der Schwerpunkt bei GSM liegen, da dies das hier in Europa meist genutzte System im Mobilfunkbereich ist.
*Was wird die Zukunft in der Mobilfunktechnik bringen? Und wie ist Positionsbestimmung in WLAN's (*Wireless Local Area Network*) machbar? Mit diesen Themen beschäftigt sich der dritte Abschnitt.*
Der vierte Abschnitt schließlich bildet eine Zusammenfassung und einen Vergleich der Systeme mit Blick auf den Anwender.

Inhaltsverzeichnis

1.1 Satellitengestützte Positionierungsverfahren

Die genauesten Positionierungsverfahren sind zur Zeit Verfahren, die auf Satelliten beruhen. Schon in den 1960'er Jahren wurden von den USA und der damaligen Sowjetunion Systeme zu militärischen Zwecken entwickelt.
Das System der USA hieß TRANSIT und bestand aus 4 Satelliten. Doch die Ungenauigkeit der Messungen und die grossen Zeitabstände zwischen 2 Messungen veranlassten das Department of Defence (*Verteidigungsministerium der USA*, DoD), ein neues System zu entwickeln. Dieses System wurde 1993 unter dem Namen NAVSTAR-GPS in Betrieb genommen und löste damit TRANSIT ab. Dieses ist das zur Zeit modernste und genaueste Satellitennavigationssystem.
Das Äquivalent der SU zu TRANSIT hieß TSIKADA und zu NAVSTAR-GPS wurde später GLONASS als Konkurrent eingeführt.

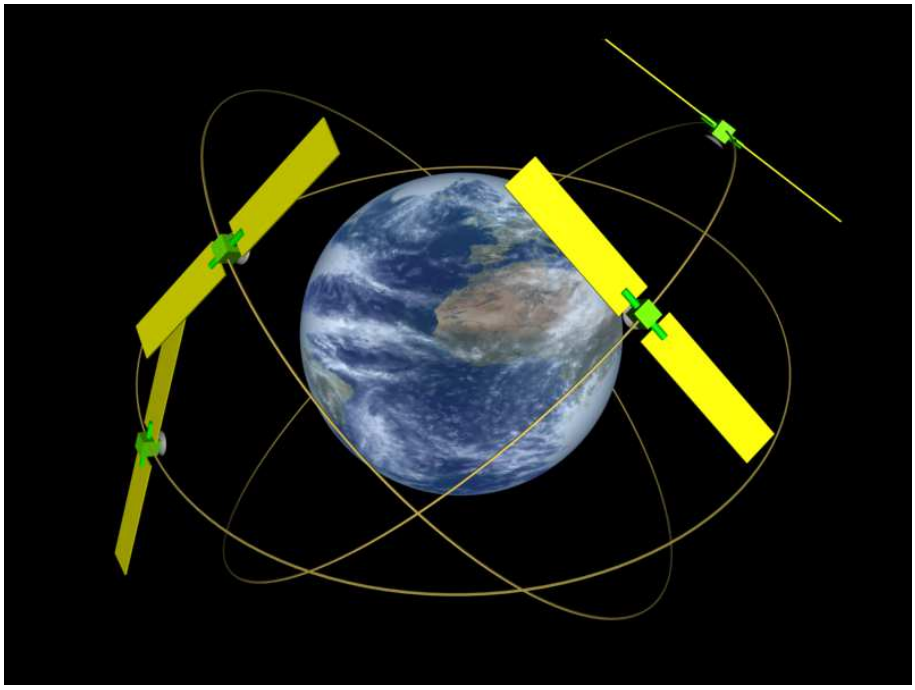

Abbildung 1.1: Anordnung der Satelliten bei Satellitennavigationssystemen (nicht maßstabsgetreu)

Da alle bisher genannten Systeme hauptsächlich der militärischen Nutzung dienen oder dienten und nur eingeschränkt zur zivilen Verwendung freigegeben sind (inwieweit, wird später erläutert), hat sich die Europäische Union entschlossen, ein Satellitennavigationssystem mit dem Namen GALILEO bis 2010 in Betrieb zu nehmen. GALILEO ist rein zur zivilen Nutzung konzipiert.

1.1.1 Grundlegende Technik

Alle bisher in Betrieb genommen und auch das zukünftige europäischen System nutzen die gleiche grundlegende Technik der Positionsbestimmung.

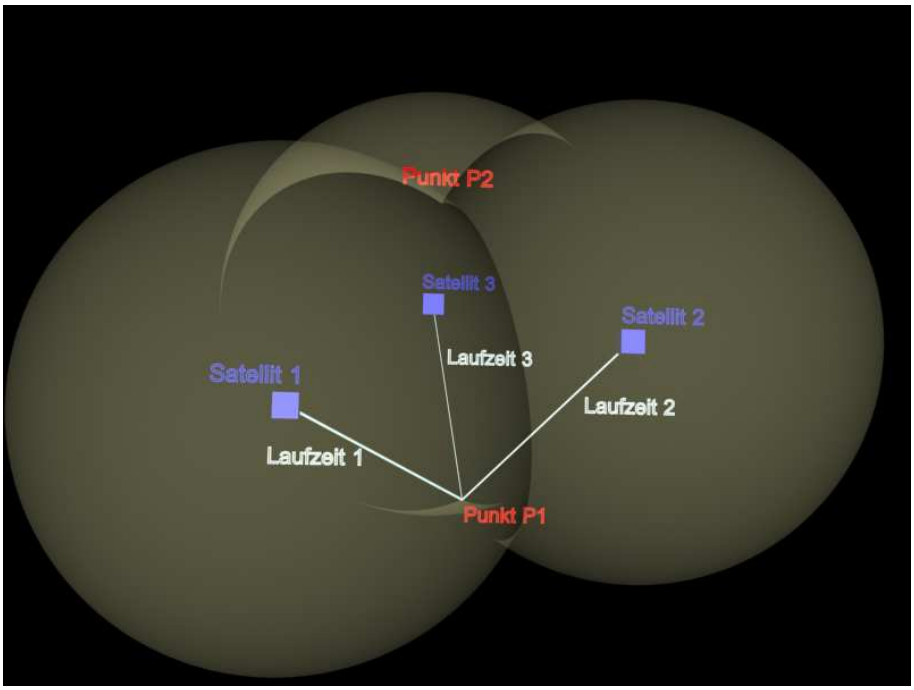

Abbildung 1.2: Technische Umsetzung der Positionsbestimmung

Bei den Systemen kommt ein Verfahren zum Einsatz, welches die Laufzeitunterschiede zu bekannten Positionen misst und daraus die gesuchte Position berechnet. Bei den Satellitensystemen sind die Satelliten die bekannten Orte, deren Position exakt bekannt ist. Gewährleistet wird dies durch Kontrollstationen am Boden, die Kursabweichungen oder Verschiebungen auf der Bahn der Satelliten durch Steueranweisungen an die Satelliten beheben.
In Abbildung 1.2 wird eine schematische Darstellung gezeigt. Gesucht ist die Position des Punktes P1. Der Empfänger empfängt die Informationen vom Satelliten 1 und misst daraus die Laufzeit. Der Punkt P1 muss also auf der Kugeloberfläche um den Satelliten 1 liegen. Nun wird die Laufzeit zum Satelliten 2 gemessen. Die Kugel des Satelliten 2 schneidet sich in einem Kreis mit der Kugel des Satelliten 1. Der Punkt P1 beschränkt sich also auf diesen Kreis. Durch Hinzunahme der Laufzeit vom Satelliten 3 lässt sich die Position des gesuchten Ortes auf 2 Schnittpunkte beschränken. Der Empfänger am Punkt P1 errechnet nun also aus den 3 Laufzeiten 2 mögliche Positionen. Allerdings scheidet der Punkt P2 aufgrund seiner „unmöglichen“ Lage weit im All aus.
Die Entfernung wird bestimmt, indem der Empfänger sich die Zeit seiner internen Uhr „merkt“ und den Zeitstempel der Satelliten empfängt. Dieser Zeitstempel beinhaltet die Uhrzeit, zu dem das Signal den Satelliten verlassen hat. Aus der Differenz der beiden Zeiten und der Lichtgeschwindigkeit wird dann die Entfernung zum Satelliten errechnet.
Eine zweite Möglichkeit ist die Verschiebung im C/A-Code (Coarse/Aquisition-Code) als Laufzeit zu interpretieren. Dieser wird vom Satelliten ständig ausgestrahlt und ist auch dem Empfänger bekannt. Wenn der Empfänger den Beginn dieses Codes erkennt, fängt er an, eine von ihm erzeugte Kopie zu synchronisieren. Die entstehende Phasenverschiebung kann dann zur Laufzeitbestimmung genutzt werden.
Zur Positionsbestimmung sind also 3 Satelliten notwendig. Da im Normalfall der Empfän-

ger keine Atomuhr besitzt, ist zur Synchronisierung der Uhr ein vierter Satellit notwendig. Damit werden auch Fehler, welche durch die Brechung an der Ionosphäre entstehen, minimiert.
Um die Höhe des Empfängers von der Erdoberfläche zu bestimmen, wird davon ausgegangen, dass die Erde eine flache Ebene ist und fest im Raum steht. Der Empfänger kann nun aufgrund der Kenntnis der Entfernung der Satelliten seine Höhe berechnen. Auch hier wird der vierte Satellit zur Bestätigung herangezogen.

1.1.2 Global Positioning System - GPS

Seit 1993 ist das GPS in Betrieb. Zu diesem System gehören 24 Satelliten, von denen 3 Reserve sind und auf einer Höhe von 20183 km um die Erde kreisen. Die Bahnen der Satelliten sind genau berechnet, damit im Idealfall zu jeder Zeit an jedem Ort der Erde mindestens vier Satelliten zu „sehen“ sind. Jeder Satellit besitzt 2 Sender und 4 Atomuhren. Die Sender senden auf den Frequenzen L1=1575,42 MHz und L2=1227,60 MHz, welche nötig sind, um Brechungsfehler an der Ionosphäre zu vermindern und 2 Genauigkeiten der Messung zu ermöglichen. Die Frequenz L1 ist dabei für die zivile und L2 für die militärische Nutzung bestimmt. Die 4 Atomuhren verringern Messfehler und verbessern Kurz- und Langzeitkonstanz. [1],[2]
Jeder Satellit sendet, wie gesagt, auf 2 Frequenzen. Auf jeder der beiden wird ein unterschiedliches Signal abgestrahlt. Auf der Frequenz L1 wird der so genannte PRN-Code (*Pseudo Random Noise*) (oder auch C/A - Code, Coarse/Acquisition-Code) moduliert und hat eine Wiederholrate von 1 MHz. Dieser Code wird von jedem handelsüblichen GPS-Empfänger genutzt und ermöglicht eine Genauigkeit von ca. 30 m. Der zweite Code, P-Code (*Precision*) genannt, ist der für das amerikanische Militär bestimmte und wird mit einer Rate von 10 MHz wiederholt. Durch die höhere Wiederholfrequenz ist die Übertragung von mehr Signalen im gleichen Zeitraum möglich. Dieser Code ist geheim und lässt Messungen auf drei bis fünf Meter genau zu.
Die Satelliten senden mit niedriger Leistung den PRN-Code und dadurch sind die Signale im Allgemeinen vom athmosphärischen Rauschen nicht zu unterscheiden. Die Empfänger allerdings kennen Teile, eben den C/A-Code, des gesuchten Code ja und „hören“ den Äther nach diesem Code ab. Dieser ist fest in die Geräte implementiert. Ist eine Übereinstimmung gefunden, empfängt der Empfänger die Informationen vom Satelliten und sucht nach weiteren Satelliten. Sind genug für eine Positionsbestimmung gefunden, wird diese durchgeführt.
Der PRN-Code ist bei jedem Satelliten unterschiedlich. Weiterhin senden alle Satelliten Informationen über die Ephemeriden (die Bahndaten der Satelliten), allgemeine Korrekturdaten, Statusinformationen des Satelliten, die GPS-Zeit und Korrekturdaten für die Uhr sowie die Flugbahn des Satelliten.
Wird ein Empfänger zum ersten Mal in Betrieb genommen, führt er eine Initialisierung durch. Hier werden alle Daten der verfügbaren Satelliten empfangen und gespeichert. Diese Daten werden danach ständig aktualisiert. Der Initialisierungsvorgang kann unter Umständen bis zu 20 Minuten dauern. Der Empfänger berechnet nun seine erste Position und speichert diese. Sie wird dann durch die interne Quarzuhr und den bekannten Ephemeriden ständig aktualisiert.

Doch nun zu den Nachteilen von GPS. Der größte ist mit Sicherheit die Unzuverlässigkeit im Dienstbetrieb, da das amerikanische Militär jederzeit von der Möglichkeit Gebrauch machen kann, die angebotenen Dienste einzuschränken, oder gar für die zivile Nutzung ganz abzuschalten.
Bis zum Jahr 2000 war der zivile Bereich der GPS-Dienste durch ein System namens *„selective availability“* eingeschränkt. Hierbei wurde die Modulation der Uhrzeit künstlich verlängert und damit kam eine Ungenauigkeit von ca. 200m in Nord-Süd Richtung und ca. 100m in Ost-West-Richtung in die Messungen. Dieses System wurde zwar abgeschaltet, kann aber jeder Zeit wieder in Betrieb genommen werden. Dies ist allerdings bisher nicht geschehen.
Ein weiterer Nachteil ist die Ungenauigkeit der Messungen in höheren Breitengraden. Hier stehen die Satelliten zu dicht über dem Horizont oder einfach nur „zu dicht“ beieinander. Auch hat hier das Militär die Möglichkeit, noch weitere Ungenauigkeit durch Bewegung der Satelliten herbeizuführen. Das ist zum Beispiel während des Golfkriegs dieses Jahr passiert.

1.1.3 GALILEO - Das europäische Satellitennavigationssystem

Die oben genannten Nachteile des GPS haben die Europäische Union veranlasst, in Zusammenarbeit mit der ESA (Europäische Weltraumorganisation) ein eigenes Satellitensystem zur Positionsbestimmung zu entwickeln.
Dieses System wird aus 30 Satelliten in Umlaufbahnen von 23616 km Höhe bestehen. Jeweils 10 Satelliten auf 3 Bahnen mit einer Neigung von 56° zum Äquator. Jeweils ein Satellit pro Bahn ist als Reserve gedacht.
Das Projekt ist in 3 Phasen geteilt. Zur Zeit und bis 2005 wird die Infrastruktur mit 3-4 Satelliten in der Umlaufbahn und einer Bodenkontrollstation getestet. Bis 2007 sollen dann die restlichen 27-28 Satelliten in die Umlaufbahn gebracht werden und das restliche Bodensegment fertiggestellt werden. Ab 2008 beginnt dann die kommerzielle Nutzung.[4]

Anders als GPS ist GALILEO rein zur zivilen Nutzung gedacht. Diese Nutzung teilt sich in 3 Bereiche. Der offene Dienst (*Open Service*, OS) ist der zur kostenlosen Nutzung gedachte Service, der jedem Empfänger auf der Erde zur Verfügung steht und die Positionsbestimmung ermöglicht und ein Signal zur Zeitsteuerung bereit stellt. Allerdings wird die Betreibergesellschaft keine Garantie für die Verfügbarkeit geben und eine Haftung ausschließen.
Der zweite Dienst ist der sicherheitskritische Dienst (*Safety-of-Life*, SoL). Dieser Dienst soll hauptsächlich den verkehrsbezogenen Nutzern dienen. Hierzu sind spezielle Empfänger nötig, da die Informationen auf 2 getrennten Frequenzen übermittelt werden. Dadurch will die GALILEO-Betreibergesellschaft den Empfang des Dienstes garantieren. Die Genauigkeit der Messungen haben die gleichen Werte wie beim offenen Dienst.
Der dritte Dienst stellt einen der größten Unterschiede zum GPS dar. Dieser kommerzielle Dienst (*Commercial Service*, CS) wird eine anwendungsabhängige Leistung zur Verfügung stellen und ist für Anwendungen mit hohen Transferraten gedacht. Durch die Kombination von 2 Frequenzen, welche dann verschlüsselt werden, sollen höhere Transferraten erreicht

werden, als bei den beiden o.a. anderen Diensten. Die Nutzer bekommen dann Empfänger, denen der Schlüssel bekannt ist. Zur Zeit werden Transferraten zwischen 50 und 1000 Zeichen pro Sekunde geprüft. Die niedrige Rate stört das Navigationssignal nur wenig, während höhere Raten für die kommerzielle Nutzung von Vorteil wären.
Zum Teilbereich der kommerziellen Nutzung gehören auch noch der öffentlich regulierte Dienst (*Public Regulated Service*, PRS), welcher von Polizei und Zoll genutzt wird und von einer zivilen Bodenstation kontrolliert wird, sowie der Such- und Rettungsdienst (*SAR*), welcher ein bestehendes System aus vier erdnahen Satelliten unterstützt und so die Positionsbestimmung von bisher 5 km auf wenige Meter reduziert.

Zu den o.a. 30 Satelliten kommt noch weitere Infrastruktur auf dem Boden. Dazu zählen 2 Kontrollstationen in Europa und einige Kontrollsegmente auf der Erde verteilt. Die Kontrollzentren steuern die Satelliten, überwachen die Genauigkeit der Messungen und gleichen die Atomuhren in den Satelliten ab. Die Kontrollsegmente messen ständig die Navigationsdaten der Satelliten und übermitteln diese Daten an die Kontrollzentren. Diese Teile sind über ein eigenes Kommunikationsnetzwerk miteinander verbunden.
Jeder Satellit wird 10 Signale aussenden. Sechs Signale für die offenen und die sicherheitskritischen Dienste, zwei für die kommerzielle Nutzung und zwei für die PRN-Dienste. Als Frequenzbänder sind folgende bereits reserviert:

- 1164-1215 MHz
- 1260-1300 MHz
- 1559-1591 MHz (wird auch von GPS genutzt, ermöglicht den gleichzeitigen Empfang beider Signale)

1.2 Positionierungsverfahren der Mobilen Telekommunikation

1.2.1 Technik der zellbasierten Funksysteme

Die Mobilfunksysteme in der heutigen Zeit benutzen alle ein Funksystem das auf einzelnen Zellen beruht. Dazu betreiben die Anbieter ein Netz aus Basisstationen. Die Stationen decken einen Bereich ab, der von der Sendeleistung abhängt. Die Zellen haben Radien zwischen 20 m innerhalb von Gebäuden, mehreren 100 m in Städten und bis zu 50 km auf dem Land. Die Form der Zellen ist dabei nicht ideal, sondern richtet sich nach Geländeform, Bebauung oder dem aktuellen Wetter. Bei manchen Systemen kann sogar die Anzahl der aktiven Teilnehmer Einfluss auf die Größe der Zelle haben.[5]
Diese Art der Abdeckung hat Vor- und Nachteile. Zuerst zu den Vorteilen:

- *Höhere Gesamtkapazität*: Durch den Einsatz von Sendern mit geringerer Leistung kann der Anbieter die gleiche Frequenz in verschiedenen, von einander getrennten

Gebieten, einsetzen und damit die Kapazität des Gesamtsystems erhöhen. Da jeder Teilnehmer für die Dauer seiner Nutzung eine Frequenz belegt, ist es so möglich, mehreren Teilnehmern die gleiche Frequenz zur gleichen Zeit in unterschiedlichen Gebieten zur Verfügung zu stellen, da im allgemeinen nur begrenzte Frequenzbereiche genutzt werden können.

- *Geringere Sendeleistung*: Das größte Manko heutiger mobiler Geräte ist die Größe und damit die Laufzeit der Akkumulatoren. Um dieses Problem ein wenig zu mindern, reichen durch den Einsatz von kleineren Zellen Sender mit geringerer Leistung, denn auch die Mobilgeräte müssen ihrerseits an die Basisstationen senden. Durch kleinere Zellen ist die Strecke, die das Mobilteil zu überwinden hat, kleiner und die Sendeleistung muss nicht so groß sein.

- *Nur lokale Störungen*: Durch den geringeren Abstand zwischen Sendern und Empfängern beschränken sich die möglicherweise auftretenden Fehler nur auf einen lokalen Bereich.

- *Robustheit*: Da die Zellen kleiner sind, wirkt sich ein Ausfall eines einzelnen Senders nicht gleich systemweit aus, sondern die Chance, das ein benachbarter Sender noch zur Kommunikation ausreicht, ist größer. Der Grund dafür ist der dezentrale Aufbau der Systeme.

Aber der Aufbau mit kleineren Zellen hat auch Nachteile:

- *Infrastruktur*: Kleinere Zellen benötigen natürlich auch mehr Sender. Aber ebenso sind auch mehr Zwischenstationen zur Weiterleitung der Daten und mehr Datenbanken für Lokalisierungsdatenspeicherung nötig. Dieses Mehr an Hardware erhöht natürlich auch die Kosten der Dienste.

- *Häufige Übergabe*: Der Empfänger bewegt sich in vielen Mobilsystemen von Zelle zu Zelle. Bei jedem dieser Übergänge muss ein so genannter *Handover* durchgeführt werden. Werden kleine Zellen benutzt, sind solche Übergaben, bedingt durch das Bewegungsmuster des Empfängers, evtl. sehr häufig durchzuführen. Das bedeutet eine zusätzliche Belastung der Infrastruktur.

- *Frequenzplanung*: Da nur eine begrenzte Anzahl von Frequenzen zur Verfügung steht. ist es nötig, schon im Voraus eine genaue Planung der Nutzung in den einzelnen Zellen durchzuführen, um Interferenzen zu vermeiden. Hierbei ist zwischen diesen beiden Punkten, der Frequenzanzahl und der Inferferenz, abzuwägen.

1.2.2 Positionierungsverfahren

GSM ist die zweite Generation der mobilen Kommunikation. Zu Beginn war auch dieses System nur zum Telefonieren gedacht. Doch die Entwicklung zeigte, das das System zu weit mehr in der Lage ist.

Mobile Terminated Call

Dies ist das Verfahren, wenn jemand versucht, den mobilen Empfänger zu erreichen. Hierzu sind mehrere Schritte nötig. Zu Beginn wählt man die Telefonnummer des gewünschten Teilnehmers. Diese Nummer ist weltweit einmalig. Nachdem die Nummer gewählt wurde, stellt die „Vermittlung“ (*Public Switched Telephone Network, PSTN*) fest, das es sich um eine Nummer eines Mobilgerätes handelt und gibt den Verbindungswunsch an den Gateway zum Mobilnetz weiter. Der Gateway erkennt anhand der gewählten Nummer das zuständige Heimatregister (*Home Location Register, HLR*). Dieses überprüft, ob der gewünschte Teilnehmer die nötigen Berechtigungen hat, den Verbindungswunsch entgegen zu nehmen. Hat er die Rechte, erfragt das HLR beim Besucherregister (*Visitor Location Register, VLR* eine MSRN (*Mobile Station Roaming Number*). Diese enthält unter anderem den Aufenthaltsort des Teilnehmers. Nachdem das HLR die MSRN ausgewertet und die Informationen an den Gateway weitergegeben hat, wird der Wunsch an die zuständige Dienstvermittlungsstellen (*Mobile (Services) Switching Center, MSC*) weitergegeben. Dieser veranlasst alle Basisstationen seines Netzes, einen Rundruf zu starten. Der mobile Empfänger reagiert darauf und die zuständige Basisstation gibt diese Information an die MSC zurück und diese stellt die gewünschte Verbindung her.
Näheres zu diesem und dem folgenden Unterabschnitt in [5].

Mobile Originated Call

Hier handelt es sich um den Wunsch, als Teilnehmer eines Mobilkommunikationssystems, eine Verbindung aufzubauen. Hierbei entfällt die Suche nach dem Mobilempfänger, der diese Verbindung wünscht. Der Teilnehmer wählt die gewünschte Nummer. Diese wird über die Basisstation an die MSC gesandt, welche prüft, ob es sich um eine Nummer eines Mobilfunkteilnehmers handelt, oder ein Festnetzanschluss gewählt wurde. Ist dem so, wird der Ruf an die nächste Vermittlung im Festnetz weitergeleitet. Ansonsten wird wie im oberen Unterabschnitt beschrieben, verfahren.

Positionsbestimmung innerhalb einer Zelle

Hierzu gibt es verschiedene Verfahren, welche im Folgenden kurz erläutert werden.[6]

COO - Cell of Origin
Jeder Mobilempfänger befindet sich im Betrieb in einer Zelle, welche er bei Bewegung evtl. verlässt. Sobald er sich in einer anderen Zelle anmeldet, muss er die Basisstation wechseln. Mit diesen Informationen ist es möglich, wenigstens die Zelle zu bestimmen, in der sich das Gerät befindet. Wenn die Zelle auch noch in Teilbereiche untergliedert ist, lässt sich die Genauigkeit noch erhöhen. Allerdings ist die Genauigkeit auch von der Größe der Zelle abhängig und wie o.a. schwankt diese sehr stark. Für eine Bestimmung in Notfallsitutationen ist dieses Verfahren nur bedingt einsetzbar, ebenso für die Navigation. Der Vorteil ist, dass für diese Technik keine Änderungen im System vorgenommen werden müssen, da alles Notwendige aufgrund der Struktur des Systems schon vorhanden ist.

TOA - Time of Arrival
Hier wird die Technik der Triangulierung angewendet. Der Mobilempfänger meldet sich nicht nur an einer Basisstation, sondern an 3 Stationen an. Dadurch kann, wie bei GPS, die Position des Empfängers berechnet werden. Allerdings ist es dazu notwendig, das die Basisstationen über eine synchronisierte Uhr verfügen, oder das GPS-Signal nutzen. Da dies im asynchronen GSM-Netz nicht der Fall ist, müsste die notwendige Technik nachgerüstet werden. Weiterhin ist eine stärkere Sendeleistung der Mobilgeräte nötig, um auch in Gebieten mit großen Zellen, 3 Stationen zu erreichen, welches sich wieder auf die Laufzeit der Akkumulatoren der Geräte auswirkt. Der Vorteil ist, das an den Empfängern nichts geändert werden müsste.

AOA - Angle of Arrival
Beim AOA-Verfahren meldet sich das Mobilgerät nicht an einer einzelnen Basisstation an, sondern in jeder Zelle existiert ein Array von Antennen. Alle Antennen dieses Arrays können untereinander kommunizieren. Jede Antenne berechnet den Winkel, aus dem die Anmeldeinformationen aufgenommen werden und teilt dies den anderen Antennen mit. Daraus lässt sich dann die Position des Senders berechnen. Aus dieser Form der Berechnung ist zu erkennen, das in jeder Zelle mehrere Antennen notwendig sind, welches auf der einen Seite sehr teuer ist, auf der anderen Seite auch die Kommunen nicht gewillt sind, überall Antennen aufstellen zu lassen. Weiterhin kann die Berechnung des Winkels auch von äußeren Faktoren, wie Gebäude oder Geländeformationen, an denen die Signale reflektiert werden, gestört werden.

E-OTD - Enhanced Observed Time Difference.
Diese Technik funktioniert ähnlich der TOA. Allerdings werden hier noch weitere Einrichtungen notwendig, so genannte *location measurement units, LMU*. Diese werden zellübergreifend aufgestellt und besitzen ein synchronisiertes Zeitsignal. Wenn der Empfänger nun von mindestens 3 Basisstationen und einer LMU die Zeit empfängt, kann er aus diesen Informationen seine Position berechnen. Die Nachteile sind die gleichen wie bei TOA. Hinzu kommt noch die Notwendigkeit, die Software der Empfänger anzupassen. Das macht das System für die Provider sehr teuer.

AGPS - Assisted Global Positioning System
Das AGPS basiert auf der im Abschnitt 1 erklärten GPS-Technik. Die Empfänger müssten dann in der Lage sein, auch das GPS-Signal zu verarbeiten. Dies würde neue Mobilgeräte notwendig machen. Weitere Nachteile sind im Abschnitt 1 erläutert worden.

Zusammenfassend ist zu sagen, dass keine der genannten Techniken die Genauigkeit der Satellitensysteme erreicht. Während diese eine Bestimmung bis auf wenige Meter genau ermöglicht, sind Messungen im GSM nur auf einige hundert Meter bis maximal 20 m machbar.

1.3 Ausblick auf zukünftige Techniken

Wie im vorhergehenden Abschnitt schon erwähnt, reicht die Genauigkeit in Mobilfunknetzen nicht aus, um einen vernünftigen Service zur Positionsbestimmung zur Verfügung

zu stellen. Dies will die Europäische Union allerdings in Zukunft von den Providern verlangen, so dass bei Wahl einer Notrufnummer die Position des Anrufenden auf wenige Meter genau bestimmt werden kann. Die Provider versuchen allerdings unter Angabe der notwendigen Umbauten und der damit anfallenden Kosten dies zu verhindern. Außerdem wird mit der Einführung der UMTS (*Universal Mobile Telecommunications System*) und der damit verbundenen Infrastruktur die Forderung der EU nach genauerer Lokalisierung im Notfall erfüllt.
Auch die Positionsbestimmung in drahtlosen Netzwerken soll kurz beleuchtet werden.

1.3.1 Positionsbestimmung im UMTS

Auf eine generelle Beschreibung der Technik von UMTS (*Universal Mobile Telecommunication System*) wird an dieser Stelle verzichtet und auf [7] verwiesen. Hier sollen nur kurz die 3 Methoden erklärt werden, welche in UMTS verwendet werden sollen. Allen dient das UTRAN (*Universal Terrestrial Radio Access Network*) als Grundlage. Die folgende Aufzählung soll die Verfahren nur kurz umreißen. Genaueres in [8].

- *Cell ID*: Dieses Verfahren ist dem COO beim GSM sehr ähnlich. Der Empfänger meldet sich bei der Bodenstation an und kann dann, wenn er eine Positionsbestimmung benötigt, die für diese Zelle gültige Zell-ID „erfragen“. In einer dem CN (*Core Network*) bekannten Datenbank sind diese Zell-ID's so genannten SAI (*Service Area Identifier*) zugeordnet, welche wiederum geographische Positionen darstellen. Dabei gibt es nicht für jede Zelle eine SAI, sondern diese sind zellübergreifend aufgeteilt. Genauer wird dieses Verfahren gegenüber GSM deshalb, da bei UMTS die Zellen viel kleiner sind und auch in ländlichen Gebieten nicht die Ausdehnung der GSM-Zellen erreichen. Dies macht eine genauere Lokalisierung im Notfall auch schon mit diesem relativ einfachen Verfahren möglich.

- *OTDOA - Observed Time Difference of Arrival*: Hier wird die Technik von TOA bei GSM verwandt. Da die Zellen im UMTS bedeutend kleiner sind, ist es dem Empfänger meist möglich, 3 oder mehr Basisstationen zu erreichen. Aus den Laufzeiten der Zeitsignale ist dann die Positionsbestimmung recht einfach zu realisieren. Die Synchronität der Zeit ist durch den Rückgriff auf das Zeitsignal des CN realisiert.

- *AGPS - Assisted GPS*: Sollte der Empfänger mit einem GPS-Empfänger ausgestattet sein, ist auch die Nutzung des Global Positioning System möglich. Dazu kann das UTRAN mit GPS verbunden werden und dann die Informationen der Satelliten auch terrestrisch zur Verfügung stellen. Das macht die Positionsbestimmung auch in Situationen, in denen der Empfänger keine „Sichtverbindung“ zu den Satelliten hat, aber die zuständigen Basisstationen erreichen kann, möglich, ohne an Genauigkeit einzubüßen. Dazu übermitteln die Basisstationen die benötigten Daten an den Empfänger, welcher dann seine Position bestimmen kann.

1.3.2 Positionsbestimmung in WLAN's

Auch die Lokalisierung innerhalb von drahtlosen Netzwerken (*Wireless Lokal Area Network, WLAN*) gewinnt immer mehr an Bedeutung. Vor allem in Zusammenhang mit Mobilfunk ist eine genaue Positionsbestimmung in WLAN's wünschenswert, um Dienste der Provider sinnvoll einsetzen zu können.
Wie auch in den anderen Mobilen Systemen gibt es bei WLAN mehrere Ansätze. Es sollen im Folgenden 3 davon vorgestellt werden: zellbasiert, Triangulierung und tabellenorientiert. Näheres in [9].

- *Zellbasierte Ortung*: Wie auch schon in den zellbasierten Mobilfunksystemen besteht ein WLAN aus einzelnen Zellen mit AC's (*Access Point*) als Basisstationen. Da auch hier die Zellgröße zwischen 30 und 300 m schwankt, ist die Positionsbestimmung meist sehr ungenau. Wenn man die Signalstärke noch als Kriterium hinzunimmt, kommt man auf eine Genauigkeit von ca 20 m.

- *Triangulierung*: Während bei GSM und UMTS die Laufzeit als Messwert dient, ist dies in WLAN nicht möglich, da es sowas nicht gibt. Hier wird als Ersatz die Signalstärke genutzt, was aber auch Nachteile mit sich bringt. So ist die Stärke stark von den äußeren Bedingungen beeinflussbar. Um dies zu minimieren, werden vorher Messungen der Signalstärke an signifikanten Punkten durchgeführt und dann auf statistische Funktionen zurückgegriffen. So kann eine Funktion mit Signalstärken in Abhängigkeit von der Entfernung aufgestellt werden. Damit wird die Genauigkeit erhöht. Auch ist eine hohe Dichte von AC's notwendig, um dem Empfänger die Möglichkeit zu geben, sich an 3 oder mehr AC's gleichzeitig anzumelden und die Signalstärke zu messen. Trotz allem wird bei einem Abstand der AC's von 10 m nur eine Genauigkeit von 15 m erreicht.

- *tabellenorientierte Ortung*: Dieses Verfahren benötigt vor der eigentlichen Positionsbestimmung einen enormen Aufwand, der sich aber in den besten Messergebnissen der 3 Möglichkeiten niederschlägt. Wie bei der Triangulierung sind auch hier sehr viele AC's nötig. Sind Reflektionen und Dämpfung der Signalstärke bei der Triangulierung noch störend, werden sich diese Eigenschaften bei diesem Verfahren zu nutze gemacht. Zu Beginn werden an ausgesuchten Punkten Pegelmessungen durchgeführt. Die Ergebnisse werden in einer Tabelle gespeichert, aus der Einträge mit nur einem oder 2 AC's gestrichen werden. Bei den Messungen ist auf ausreichend grossen Abstand zwischen den Messpunkten zu achten, um auch signifikante Unterschiede in den Pegeln zu erhalten. Bei der Positionsbestimmung zu einem späteren Zeitpunkt werden dann die 3 Einträge aus der Tabelle genommen, die dem gemessenen Wert am nächsten kommen und dann mit Hilfe einer Formel der Standort berechnet. Hier kommt das Euklidische Distanzmaß zu Einsatz. Durch dieses Verfahren kann die Position bis auf 10 m genau bestimmt werden, welches in einem Gebäude meist den Rückschluss auf den Raum zulässt, in dem das Gerät genutzt wird.

Zusammenfassend gilt auch hier, dass die Werte der Satellitennavigation nicht erreicht werden, was aber weniger das Problem darstellt, da man ja auch immer beachten muss, was man mit der Positionsbestimmung erreichen will und welchen Dienst man nutzen möchte.

1.4 Zusammenfassung

Ziel dieser Arbeit, war es, die einzelnen Systeme der Positionsbestimmung mit Hilfe von Satelliten und in Mobilfunknetzen darzulegen. Hierzu wurden GPS und Galileo vorgestellt und die grundlegende Technik bei Satellitennavigatonssystemen erläutert. Weiterhin wurde anhand von GSM auf die Standortbestimmung in Mobilfunknetzen eingegangen. Hier wurden die verschiedenen Verfahren erklärt und auf die Unterschiede hingewiesen.

Doch nun ein kleiner Vergleich mit Sicht auf den Anwender. Welches System das für den Nutzer beste ist, lässt sich so ohne weiteres nicht beantworten. Hier ist ganz klar zu unterscheiden, welche Bedürfnisse der Nutzer hat. Will er eine möglichst genaue Bestimmung seines Standorts, oder will er keine zusätzlichen Kosten haben? Das sind nur 2 der vielen Möglichkeiten, das für den Anwender nützlichste System zu bestimmen. Für eine einfache und grobe Positionsbestimmung, um zum Beispiel das lokale Wetter zu erfragen, ist bestimmt keine Bestimmung auf 15 Meter genau notwendig. Soll er allerdings von einem Navigationssytem von Ort A zu Ort B geleitet werden, ist diese Genauigkeit schon wünschenswert. Hierin liegen auch die größten Unterschiede in den einzelnen Systemen. Die Genauigkeit schwankt zwischen drei Metern beim militärischen GPS und 50 km bei der einfachen Zellbestimmung in Mobilfunknetzen. Aufgrund dieser Tatsache ist der Nutzer gezwungen, das für ihn geeignetste System zu wählen und unter Umständen weitere Investitionen in zusätzliche Hardware zu tätigen. Bei Systemen wie GSM wird die Hardware in Form des Telefons schon mitgeliefert, während bei GPS und Galileo spezielle Empfänger nötig sind.

Zusammenfassend lässt sich sagen, das die Bestimmung des eigenen Standorts heutzutage schon recht genau möglich ist, wenn auch nicht mit jedem System die gleiche Genauigkeit erreicht wird. Doch auch die Bestimmung der Position in den heutigen Mobilfunknetzen wird mit Einführung von UMTS weiter steigen. Allerdings bleibt abzuwarten, ob der Nutzer von den Möglichkeiten dann auch Gebrauch machen wird. In Sachen Navigation muss sich erstmal Galileo gegen das derzeit übermächtige GPS behaupten. Und ob dann auch die Mobilfunkbetreiber in dieses Segment vorstoßen ist fraglich, da es auch immer eine Frage der Rentabilität bleibt. Die Betreiber werden hier wohl eher andere Alternativen anstreben, wie zum Beispiel Servicedienstleistungen im Bereich der Freizeitgestaltung oder dem Auffinden von Örtlichkeiten im näheren Bereich des Nutzers.

Literaturverzeichnis

[1] „c't Magazin für Computertechnik“ Grundlagen des GPS S.150 Ausgabe 1/2003, Heise Zeitschriften Verlag GmbH & Co. KG, 2002

[2] „c't Magazin für Computertechnik“ Wie genau ist GPS-Navigation in Kriegszeiten? S.82 Ausgabe 8/2003, Heise Zeitschriften Verlag GmbH & Co. KG, 2003

[3] „c't Magazin für Computertechnik“ Überwachung per Mobilfunk S.102 Ausgabe 10/2003, Heise Zeitschriften Verlag GmbH & Co. KG, 2003

[4] „Galileo - Das europäische System für weltweite Navigationsdienste“ Broschüre September 2002, ESA Publications Division, 2002

[5] „Mobilkommunikation“ Techniken für das allgegenwärtige Internet, Jochen Schiller, Addison-Wesley, 2000

[6] „Mobile Systems I“ Bericht Nummer 2002-08, Burkhard Stiller, Oliver Braun, Arnd Heursch (alle Hrsg.), Institut für Informationstechnische Systeme, Universität der Bundeswehr, Neubiberg, Dezember 2002

[7] http://www.3gpp.org

[8] 3GPP TS 25.305, 3rd Generation Partnership Project, Technical Specification Group Radio Access Network, Stage 2 functional specification of User Equipment (UE) positioning in UTRAN, Version 5.5.0, 2003

[9] „Realisierung von Positionsortungen in WLAN“, Peter Dornbusch, TU München, Max Zündt, CDTM, München, wwwbroy.informatik.tu-muenchen.de/~dornbusc/pubs/RvPiWLAN_final.pdf

Kapitel 2

Accessing Directories in Mobile Environments

Andreas Liehr

In der heutigen Zeit sind WLAN-Netze immer mehr auf dem Vormarsch. In größeren Unternehmen ist es bereits üblich, daß Laptops nicht nur im Büro, sondern auf dem gesamten Firmengelände mit dem Netzwerk verbunden sind. Universitäten gehen dazu über, ihre Campusgelände komplett mit einem WLAN-Netz abzudecken und somit den Studenten die Möglichkeit zu geben, mittels eines Laptops, der über eine WLAN-Karte verfügt, studienrelevante Informationen aus dem Internet zu ziehen. Neuerdings wird damit begonnen, Stadtkerne flächendeckend mit WLAN-Netzen zu versorgen, wie dies jetzt in Hamburg geschehen soll.[12]
Hier tut sich ein gewinnträchtiger und zukunftsweisender Markt auf. Über kurz oder lang wird es dazu kommen, daß verschiedene Provider den Zugang zum Internet von einem beliebigen Ort einer Stadt, einer Region oder sogar des ganzen Landes aus mittels einer Funknetzkarte anbieten.
In diesem Moment wird natürlich ein sicheres, leistungsfähiges und rentables Providermodell benötigt, das zum einen dem Kunden die Möglichkeit gibt, sich möglichst einfach für einen Tarif zu entscheiden und mittels diesem online zu gehen, zum Anderen aber auch dem Provider die Sicherheit vor Mißbrauch und eine einfache Möglichkeit der Abrechnung gibt.
Ziel dieser Seminararbeit soll es sein, ein solches Modell zu entwickeln, das seine Daten in einem X.500-Verzeichnis speichert und auf dieses mittels des LDAP-Protokolls zugreift.

Inhaltsverzeichnis

2.1 Einleitung

Um ein solches Accounting-Modell zu entwickeln, wird ein Speichermedium für den Nutzerbestand benötigt. Es müssen zum Beispiel persönliche Daten der Nutzer, wie Abrechnungskonten oder Anschriften gespeichert werden. Des Weiteren werden Informationen zu den vom Nutzer gewählten Tarifen, Nutzerkennung und Passwort benötigt. Außerdem müssen die Gebühren, die dem Nutzer in Rechnung gestellt werden, aufgezeichnet werden. Ein Teil dieser Daten sollte vom Nutzer veränderbar sein, ein anderer Teil nicht. So ist es zum Beispiel sinnvoll, wenn der Nutzer seinen eigenen Tarif und sein Kennwort ändern kann. Solche Daten, wie die Kosten, die er bereits verursacht hat oder die Kontonummer, von der die Rechnung abgebucht wird, müssen jedoch vor Änderungen durch den Nutzer geschützt sein.
Eine gute Möglichkeit, alle diese Daten unter den genannten Forderungen zu speichern, bietet ein sogenanntes Verzeichnis (Directory). Deshalb wird im Folgenden der X.500 Standard für Verzeichnisse und das LDAP-Protokoll, das zum Zugriff auf ein solches Verzeichnis nötig ist erläutert, bevor auf das eigentliche Abrechungsmodell eingegangen wird.

2.2 Das Konzept eines Verzeichnisses nach dem X.500 Standard

Ein Verzeichnis ist eine Ansammlung von offenen Systemen, die zusammenarbeiten, um eine Menge von Objekten der realen Welt in einer logischen Datenbank abzubilden. Die Nutzer des Verzeichnisses können Teile der Informationen, die gespeichert sind, lesen, ändern oder löschen, wenn sie über die entsprechenden Zugriffsrechte verfügen. Nutzer des Verzeichnisses können entweder Personen oder Computerprogramme sein. Dabei wird jeder Nutzer, der auf das Verzeichnis zugreift, durch einen DUA (Directory User Agent) repräsentiert, der als Schnittstelle zwischen Nutzer und Verzeichnis fungiert (Siehe Abbildung 1.1).[1]

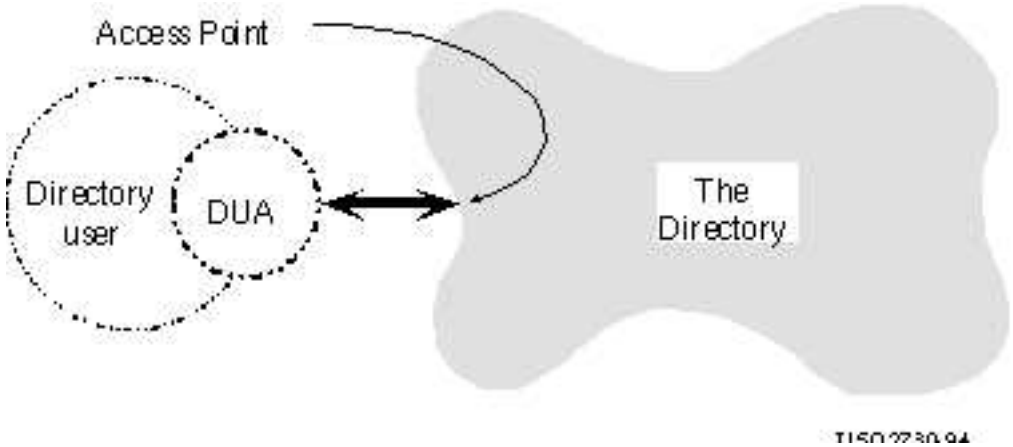

Abbildung 2.1: Zugriff auf das Verzeichnis [1]

Der Gedanke, der hinter einem solchen Verzeichnisdienst steht, ist, das viele Applikationen auf den gleichen Datenstamm zugreifen können und ein Nutzer in allen Applikationen durch das gleiche Objekt repräsentiert wird. Dadurch wird das Halten von redundanten Daten und das Überprüfen von Inkonsistenzen derselben überflüssig. Die gesamten Informationen, die in einem sochen Verzeichnis gespeichert sind, werden als DIB (Directory Information Base) bezeichnet. Auf diese wird im nächsten Unterkapitel eingegangen.

2.2.1 Die Verzeichnis-Informationsbasis (DIB)

Die DIB besteht aus Informationen, die Objekten zugeordnet sind. Dabei ist jedem Objekt ein Verzeichniseintrag zugeordnet, der die zum Objekt gehörigen Informationen enthält. Jeder dieser Einträge besteht aus einer Menge von Attributen, die jeweils über einen Typen und einen oder mehrere Werte verfügen. Dabei sind die Typen der Attribute von der Klasse des Objektes abhängig.
Die Einträge eines DIB sind dabei in einer Baumstruktur angeordnet, dem DIT (Directory Information Tree). Dabei repräsentiert jedes Blatt des Baums einen Verzeichniseintrag. So können zum Beispiel in einem Verzeichnis die Blätter nahe der Wurzel Länder oder Organisationen repräsentieren und die Blätter am unteren Ende des Baums einzelne Personen (siehe Abb. 1.2).[1]

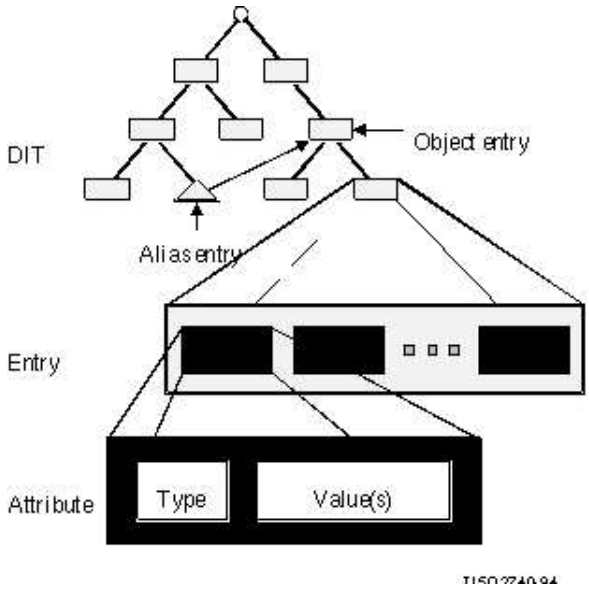

Abbildung 2.2: Struktur des DIT und der Einträge [1]

Dabei ist jeder Eintrag des Verzeichnisses über einen einmaligen Namen, den DN (Distinguished Name), eindeutig identifizierbar. Dieser Name setzt sich aus dem DN seines übergeordneten Eintrages und speziellen Werten eines Attributes des Eintrages (Distinguished Values) zusammen.
Es gibt drei Arten von Einträgen: Aliase (alias entries), Objekte (object entries) und zusammengesetzte Einträge (compound entries). Aliase zeigen auf andere Einträge und

ermöglichen somit die Vergabe von alternativen Namen für Objekte. Ein zusammengesetzter Eintrag ist eine Aggregation aus den Informationen mehrerer Einträge, wobei jeder dieser Einträge einen Teil der Information dieses Objektes bildet.
Damit die DIB im Laufe der Zeit auch nach Änderungen noch wohlgeformt bleibt, existieren Regeln, die die Typisierung der Attribute von Objekten bestimmen. Diese Regeln sind in einem Verzeichnisschema (Directory schema) definiert. Im Folgenden nun ein Beispiel für einen DIT:

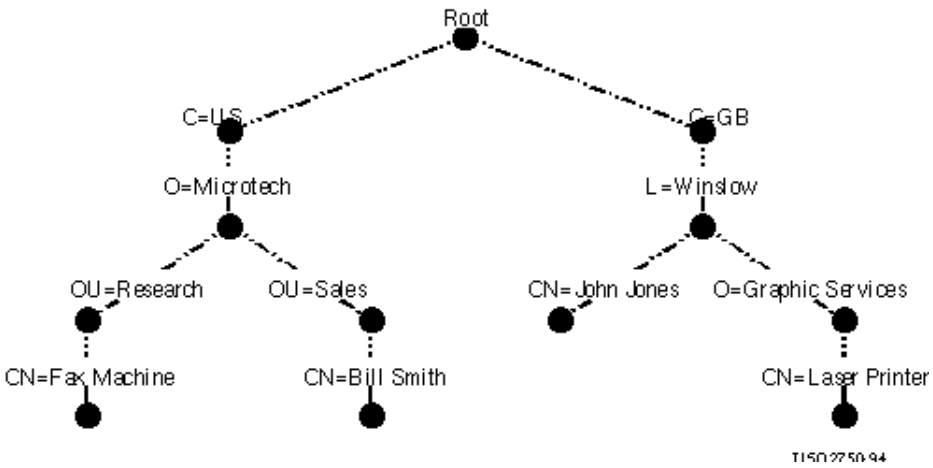

Abbildung 2.3: Beispiel eines Directory Information Tree [1]

Hier wird zum Beispiel durch den DN

$\{C = G,\ L = Winslow,\ O = GraphicServices,\ CN = LaserPrinter\}$

der Laserdrucker identifiziert. Dabei steht $C = GB$ für das Land (Großbritannien), $L = Winslow$ für die Örtlichkeit (Lokalitat Winslow), $O = GraphicServices$ für die Organisation (Grafikdienste) und $CN = LaserPrinter$ für den Namen des Eintrags (Common Name Laser Printer).

2.2.2 Die Dienste eines Verzeichnisses nach dem X.500 Standard

Hier soll ein Überblick über die vom X.500-Standart angebotenen Dienste gegeben werden, die den Nutzern (repräsentiert durch ihre DUAs) angeboten werden.

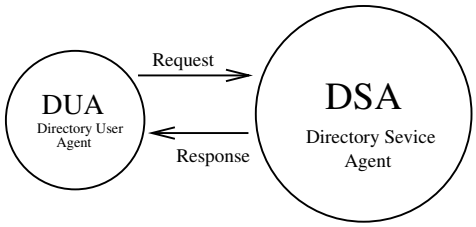

Abbildung 2.4: Request/Response Modell des X.500 Verzeichnisses

Alle Dienste liefern eine Antwort (Response) für eine mittels eines DUAs gestellte Anfrage (Request).(siehe Abb. 1.4)
Dabei wird zwischen Abfragediensten und Modifikationsdiensten unterschieden. Des Weiteren können die Anfragen konkretisiert werden um zum Beispiel ein Suchergebnis zu filtern. Weiterhin gibt es noch Fehlerausgaben und Verweise. Im Folgenden wird auf die Bestandteile dieser Dienste eingegangen.

Zusätzliche Parameter für Anfragen

Neben den Anfragen selber, wie zum Beispiel das Durchsuchen des Verzeichnisses oder das Anlegen von neuen Einträgen gibt es noch zusätzliche Parameter die entweder Anfragen präzisieren können oder dem Nutzer als Hilfestellung bei auftretenden Fehlern dienen. Hier werden drei Arten von zusätzlichen Parametern unterschieden:

- **Servicekontrollen** Durch diese Parameter können die zu nutzenden Resourcen eingegrenzt werden. Hierbei kann zum Beispiel die Zeit, die gesucht werden soll oder die Anzahl der Ergebnisse oder die Priorität der Anfrage festgelegt werden.
- **Sicherheitsparameter** Hiermit können Informationen übermittelt werden, wie die Informationen des Verzeichnisses zu schützen sind. Zum Beispiel kann hier eine digitale Signatur zusammen mit Informationen, die einen legalen Nutzer bei der korrekten Authentifizierung unterstützen, übergeben werden.
- **Filter** Hier kann ein Ausdruck übergeben werden, nach dem die Ergebnisse der Anfrage gefiltert werden sollen, um nur relevante Daten zu erhalten.

Abfragedienste

Es gibt fünf unterschiedliche Abfragedienste die im X.500-Standard implementiert sind.

- **Read** Eine Read-Operation bekommt einen DN übergeben und liefert die Attribute, die dem dadurch eindeutig definierten Objekt zugewiesen sind, als Antwort. Dabei kann man sich entweder alle Attribute zurückliefern lassen oder eine Vorauswahl treffen. Um eine Read-Anfrage durchzuführen, benötige ich den genauen DN des entsprechenden Objektes.
- **Compare** Compare wird hauptsächlich zum Vergleichen von Passwörtern genutzt. Hierbei übergibt der DUA in seinem Request einen DN, ein Attribut des DN und einen Wert vom Typ dieses Attributes. Nun wird verglichen, ob das Attribut des Objektes mit dem zugehörigen DN diesen Wert besitzt. Das ist deshalb notwendig, weil es möglich ist, Informationen aus Sicherheitsgründen gegen Lesezugriff zu schützen.
- **List** Diese Anfrage liefert eine Liste der DN's von Objekten, die einem Objekt, dessen DN im Request übergeben wurde, untergeordnet sind, zurück.

- **Search** Hierbei wird ein Teil des DIT, der mittels seines DN spezifiziert wird, nach Objekten durchsucht, die definierte Filterkriterien erfüllen. Als Ergebniss werden alle oder ausgewählte Attribute der entsprechenden Objekte geliefert. Hierbei ist der DN, der die obere Grenze der Suche im DIT festlegt, sorgfältig zu wählen, da eine Suche sonst extrem resourcenverschlingend werden kann oder eine dermaßen große Menge an Ergebnissen liefert, daß die Auswertung der Suche sich als sehr mühsam gestaltet.

- **Abandon** Diese Anfrage ist immer einer noch nicht beendeten Anfrage zugeordnet und informiert das Verzeichnis darüber, daß der Auftraggeber nicht länger an dem Ergebnis der Anfrage interessiert ist. Damit kann das Verzeichnis die laufende Anfrage beenden und bereits ermittelte Ergebnisse verwerfen.

Modifikationsdienste

Die folgenden Anfragen haben bei erfolgreicher Ausführung eine Veränderung des Datenbestandes des Verzeichnisses zur Folge.

- **Add Entry** Mit dieser Anfrage wird ein neues Blatt im DIT angelegt. Hierbei muss mindestens ein übergeordnetes Objekt und ein eigener Bestandteil des DN angegeben werden. Des weiteren muss das neue Objekt konform zum Verzeichnisschema sein, das zu diesem Verzeichnis gehört.

- **Remove Entry** Mit dieser Anfrage wird ein Blatt des DIT entfernt. Eventuell vorhandene Aliase und zusammengesetzte Einträge, die sich auf dieses Objekt beziehen, werden ebenfalls entfernt.

- **Modify Entry** Eine Modify-Anfrage bezieht sich auf einen einzelnen Verzeichniseintrag der DIB. Dabei ist es möglich, ein oder mehrere Attribute hinzuzufügen, zu entfernen oder deren Werte zu verändern. Dabei werden entweder alle Attribute, auf die sich die Anfrage bezieht, geändert, oder gar keins. Die Anfrage wird nur ausgeführt, wenn sich das entsprechende Objekt danach noch in einem Zustand befindet, den das zugehörige Schema erlaubt. Wenn sich die Änderung auf einen zusammengesetzten Verzeichniseintrag bezieht, können immer nur die Attribute eines Objektes dieses Eintrages modifiziert werden.

- **Modify DN** Mit dieser Anfrage kann der DN eines Eintrages geändert werden. Die DN aller Verzeichniseinträge, die im DIT unter diesem Eintrag eingeordnet sind, werden dementsprechend ebenfalls angepasst.

Fehlerausgaben und Verweise

Es gibt mehrere Möglichkeiten für das Auftreten von Fehlern. Das Einfachste wäre eine Verletzung der Syntax für Anfragen. Daraufhin erhält man mit der Fehlermeldung die Stelle der Anfrage zurück, bei der ein Fehler aufgetreten ist. Eine weitere Fehlerursache

ist das Übermitteln einer Anfrage, deren Ausführung eine Verletzung von Sicherheitsregeln, oder dem Schema des entsprechenden Verzeichnisses bedeuten würde. Das kommt zum Beispiel vor, wenn man ein Objekt verändern oder löschen will, ohne die benötigten Rechte zu besitzen. Eine andere Möglichkeit wäre der Versuch, einem Objekt ein Attribut zuzuweisen, das für dieses Objekt laut Verzeichnisschema nicht vorgesehen ist. Im Falle einer solchen Anfrage wird als Ergebnis eine entsprechende Fehlermeldung zurückgegeben. Diese bezieht sich immer nur auf den ersten gefundenen Fehler und versucht Informationen zurückzuliefern, die dem Nutzer die Beseitigung des Fehlers erleichtern.
Wenn ein DUA an einen Punkt angebunden ist, der für die Daten, mit denen er arbeiten will, ungeeigenet ist, zum Beispiel weil er logisch sehr weit von diesem Datenbestand entfernt ist, so kann der Verzeichnisdienst einen Verweis zurückgeben, der einen alternativen Zugriffspunkt auf das Verzeichnis empfiehlt, von dem aus der DUA seinen Request durchführen kann.[1]

2.2.3 Zugriff auf den Verzeichnisdienst

Der Zugriff auf die DIB erfolgt durch die Kommunikation eines DUA mit einem oder mehreren DSA (Directory System Agent). Dieser DSA, der Teil des Verzeichnisses ist, kann entweder die angeforderte Information aus seiner lokalen Datenbank beziehen, oder wenn dies nicht möglich ist, mit anderen DSA's kooperieren, um einen angeforderten Request auszuführen.
EinZusammenschluss mehrerer DSA's und einer beliebigen Menge DUA's, die auch leer sein kann, kann zu einer DMD (Directory Managment Domain) zusammengefasst werden. Je nachdem, wie das Verhalten der einzelnen Komponenten einer DMD spezifiziert wurde, kann eine DMD sich nach außen wie ein einzelner DSA verhalten. (siehe Abb 1.5)

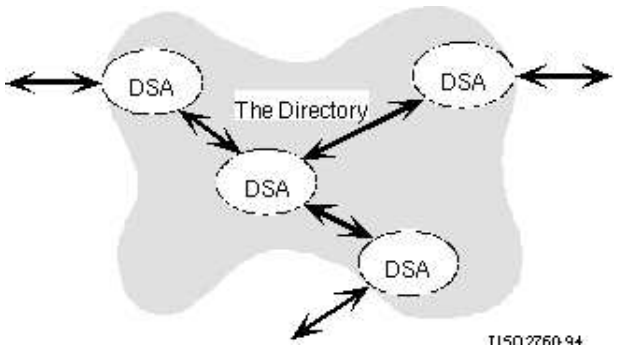

Abbildung 2.5: Funktionsmodell des Verzeichnisses [1]

Um eine Anfrage an ein Verzeichnis zu stellen, bindet sich ein DUA normalerweise an einen DSA und übermittelt diesem seine Anfrage. Nun kann es in einer solchen DMD vorkommen, daß der DSA, der an den DUA gebunden ist, die Anfrage nicht durch alleinige Nutzung seiner lokalen Datenbank ausführen kann. In diesem Falle ist es nötig, daß die einzelnen DSA einer DMD miteinander kommunizieren können. Nachdem ein DSA in Erfahrung gebracht hat, welcher DSA die Anfrage beantworten kann, kann er entweder die Anfrage auf diesem DSA ausführen und das Ergebniss an den entsprechenden DUA weiterleiten, oder den DUA an den entsprchenden DSA verweisen.[1]

2.2.4 Zugriffskontrolle im Verzeichnis

Die Zugriffskontrolle auf Verzeichnisse teilt sich in zwei Bereiche. Zum Einen in Prozeduren zur Authentifizierung eines Nutzers und zum Anderen das Schema das die Möglickeiten des Zugriffes durch Nutzer auf das Verzeichnis festlegt, das sogenannte access control scheme.
Methoden zur Authentifizierung beinhalten unter Anderm Möglichkeiten zur Verifizierung der Authentität von DSA's, Nutzern und Anfragen. Sie ermöglichen es, einen Nutzer am Verzeichnisdienst anzumelden und im Weiteren anhand seiner Identität zu entscheiden, ob er eine Anfrage ausführen darf oder nicht.
Bei dem access control scheme handelt es sich um eine Definition der Regeln die für die Zugriffskontrolle getroffen werden können. Hier kann festgelegt werden, wie fein die Zugriffsteuerung auf Dienste des Verzeichnisses oder Bestandteile des DIB granuliert werden kann.[1]

2.3 Das LDAP Protokoll (v3)

Der im Vorausgegangenen beschriebene X.500 Standard würden eigentlich für unsere Anforderungen genügen. Nun ist es aber sehr umständlich und mühsam, alle Anfragen an das Verzeichnis mittels DAP (Directory Access Protocoll) zu stellen. Deswegen wurde LDAP entwickelt.

2.3.1 Das Konzept des Protokoll-Modells

Hierbei handelt es sich um eine wesentlich nutzerfreundlichere Möglichkeit mit dem Verzeichnisdienst zu kommunizieren. Dabei arbeitet ein LDAP-Server als Gateway zwischen beliebig vielen LDAP-Clients und dem DSA des X.500 Verzeichnisses. (siehe Abb 1.6)

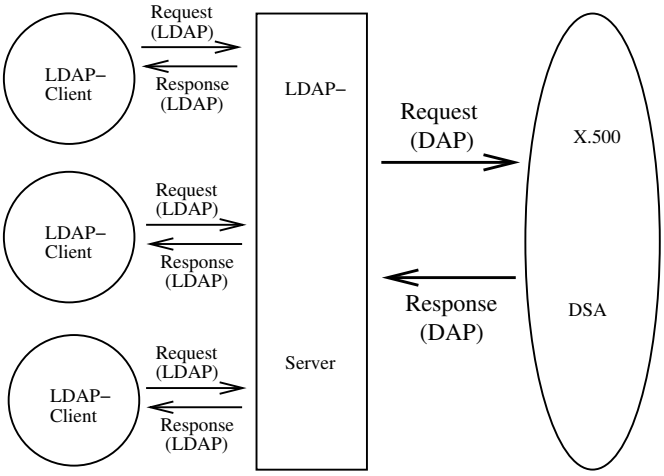

Abbildung 2.6: Funktionsmodell des LDAP-Servers

Der LDAP-Server übersetzt dann die Anfragen der LDAP-Clients, die er erhält in Anweisungen, die konform zum DAP sind, die er an den DSA weiterleitet. Für den DSA erscheint der LDAP-Server wie ein DUA. Dabei ist es oftmals notwendig, daß aus einer Anfrage des LDAP-Clients mehrere Anfragen an das X.500 Verzeichnis generiert werden, da sich eine Anfrage nach LDAP nicht immer auf genau eine Anfrage nach DAP abbilden läßt.[3]
Es existiert außerdem noch eine Version, die sich Open LDAP nennt. Hierbei handelt es sich auch um ein Cient-Server-Modell, allerdings arbeitet der Server nicht mehr als Gateway zu einem X.500-Verzeichnis, sondern ist selbst der Verzeichnisdienst. Damit wird die Notwendigkeit des Übersetzens von LDAP-Anfragen in DAP-Anfragen hinfällig. Es handelt sich dann jedoch nicht mehr um ein X.500-konformes Verzeichnis. Dies ist jedoch unproblematisch wenn das Verzeichnis ausschließlich über einen LDAP-Server genutzt werden soll.[5]

2.3.2 Die Elemente des Modells

Hier geht es um die Operationen, die das Modell dem Nutzer zur Verfügung stellt. Eine solche Operation besteht immer aus einem Request (der Anfrage an den Server) und einem Response (der Antwort des Servers auf die Anfrage), wie auch beim X.500 Standard für Verzeichnisse.

Bind-/ Unbind-Operation

Die Bind-Operation ermöglicht es dem Nutzer Authentifizierungsinformationen zu übertragen. Dementsprechend kann eine Bind-Operation entweder anonym oder mit einem Passwort und einem Nutzernamen ausgeführt werden. Dabei wird als Nutzer ein Objekt des Verzeichnisses vom Typ Person benutzt, der beim Request über seinen DN spezifiziert wird. Der Server antwortet auf einen Bind-Request mit einer Bind-Response. Wenn die Antwort 0 ist, so wurde die Bind-Operation erfolgreich durchgeführt. Andere Zahlen stehen für Fehlercodes.[3] (siehe Abb. 1.7)

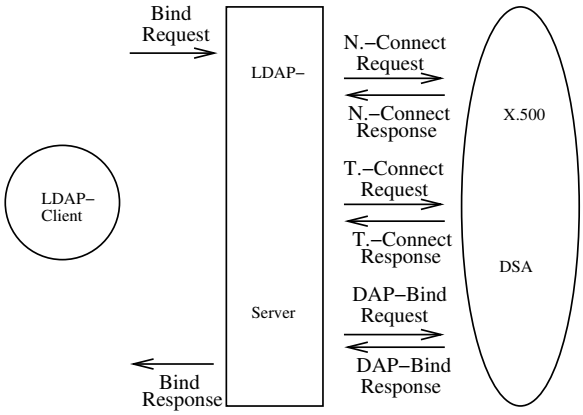

Abbildung 2.7: Ablauf eines Bind-Requests

An der Grafik ist die Umsetzung eines Befehls (des Bind-Requests) in mehrere Befehle an den DSA des Verzeichnisses durch den LDAP-Server gut ersichtlich. Nach DAP wird erst ein Network-Request und ein Transport-Request durchgeführt, bevor der DAP-Bind-Request durchgeführt werden kann.

Search-Operation

Mittels einer Search-Operation kann ein Client beim Server Attribute von Einträgen erfragen. Das kann entweder einzelne Einträge, Einträge unter einem bestimmten Eintrag oder einen gesamten Baum betreffen. Dabei wird im Request ein Basisobjekt übergeben, auf das sich die Suche bezieht, das kann auch eine Obergrenze sein (also alle Einträge, die in der Baumstruktur diesem untergeordnet sind, werden durchsucht). Des Weiteren wird ein Filter übergeben, nach dem einzelne Einträge aus der Suchmenge selektiert werden. Anschließend können noch Parameter, wie eine maximale Anzahl von Ergebnissen, ein Zeitlimit zum Suchen einer Auswahl der Attribute, die zurückgeliefert werden sollen und diverse andere Parameter in den Request eingearbeitet werden. Das Resultat der Suche wird in SearchResultEntrys unterteilt zurückgegeben. Dabei enthält ein Entry immer die ausgewählten Attribute eines Eintrags im Verzeichnis.
Bei einem Search-Request kann der LDAP-Server die Anfrage direkt in einen DAP-Search Request umwandeln, wie am Bild ersichtlich ist.[10] (siehe Abb. 1.8)

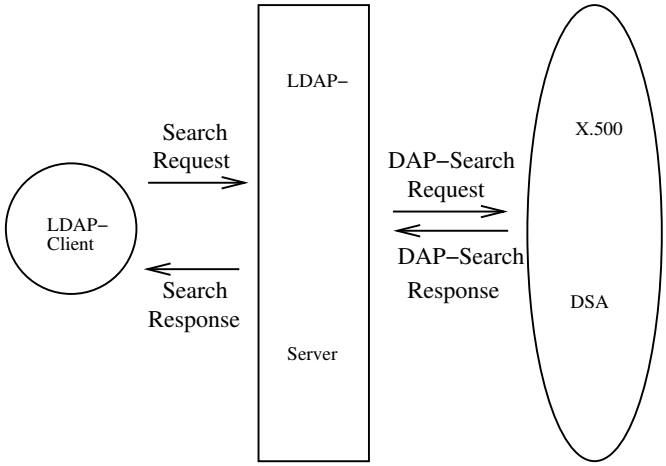

Abbildung 2.8: Ablauf einer Search-Operation

Modify-Operation

Die Modify-Operation erlaubt es einem Client an den Server eine Anfrage zum Verändern eines Eintrages des Verzeichnisses zu stellen. Dabei enthält der Request den DN des zu modifizierenden Objektes. Dieser DN darf nicht auf einen Alias-Eintrag zeigen, weil der Server bei einer Modify-Operation keine Referenzierungen durchführt. Weiterhin enthält der Request eine Liste von auszuführenden Änderungen. Diese wird entweder komplett

abgearbeitet oder der alte Zustand wird beibehalten. Das heißt, wenn eine dieser Operationen einen Fehler verursacht, werden alle Änderungen nicht durchgeführt. Als Response erhält der Client eine Erfolgsmeldung (Success) oder eine Fehlermeldung.[3]
Im Beispiel wird als neuer Wert für das Attribut *Phone* für das Objekt mit dem DN $L = Munich,\ O = UniBw,\ CN = AndreasLiehr$ ein Array mit 2 Werten übergeben und der alte Wert von *Phone* damit überschrieben.[10] (siehe Abb. 1.9)

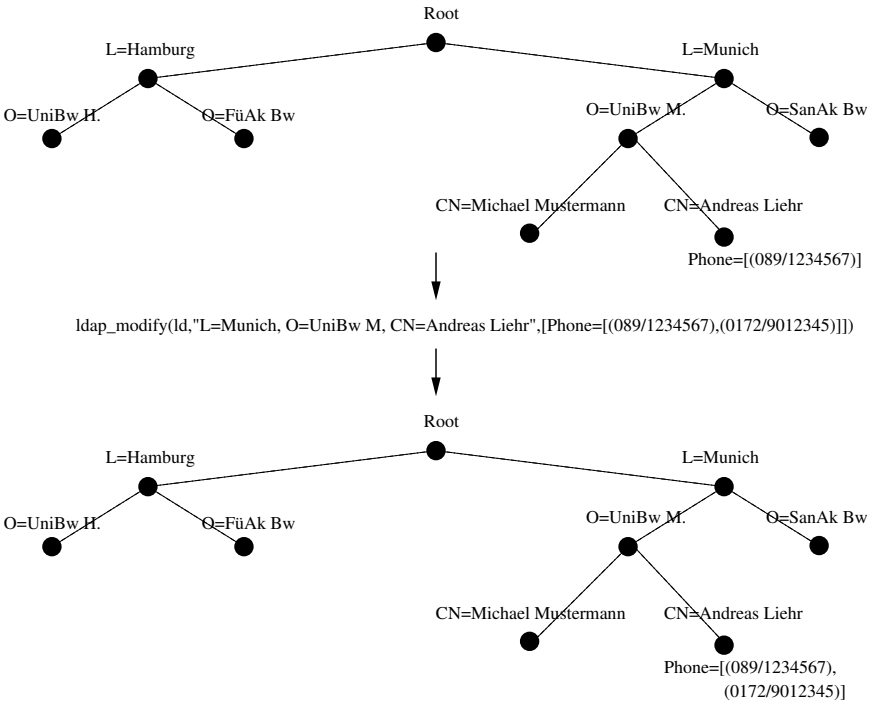

Abbildung 2.9: Auswirkungen einer Modify-Operation auf den DIT

Add-Operation

Mittels der Add-Operation wird einem Verzeichnis ein Eintrag hinzugefügt. Hierbei wird mittels des Requestes der DN des neuen Eintrages übergeben. Als weiterer Parameter werden die Attribute des Eintrages in einer Liste übergeben. In dieser Attributliste müssen mindestens die Werte des DN für diesen Eintrag enthalten sein. Des Weiteren muss der Eintrag durch diese Attribute konform zum Schema dieses Verzeichnisses gehalten werden. Auch hier erhält der Client als Response entweder eine Erfolgs- , oder eine Fehlermeldung.[3]
Im Beispiel wird ein neues Objekt, das der UniBw H. untergeordnet ist, angelegt. Dies würde nur funktionieren, wenn CN und Password die beiden einzigen benötigten Attribute für ein Objekt dieser Art wären, die im Schema als notwendig festgelegt wurden. (siehe Abb 1.10)

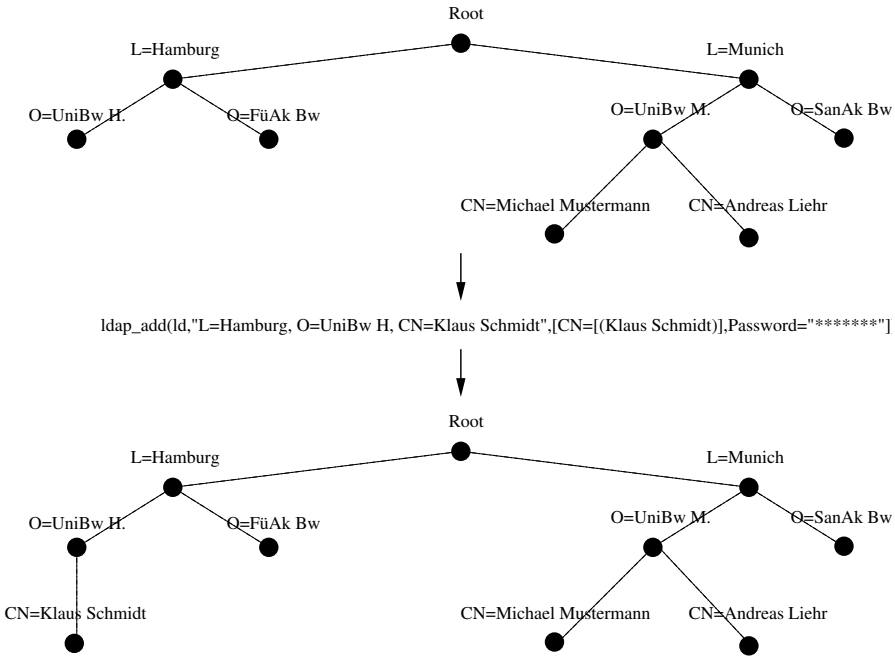

Abbildung 2.10: Auswirkungen einer Add-Operation auf den DIT

Delete-Operation

Hier wird dem Server mittels des Delete-Requestes der DN des zu entfernenden Eintrages übergeben. Der Server versucht den entsprechenden Eintrag zu entfernen und liefert dementsprechend als Response eine Fehlermeldung oder eine Erfolgsmeldung zurück.[3] Im Beispiel wird die Organisation UniBw M. gelöscht. Wie man sieht werden in diesem Fall auch alle Objekte gelöscht, die diesem Objekt untergeordnet sind. (siehe Abb. 1.11)

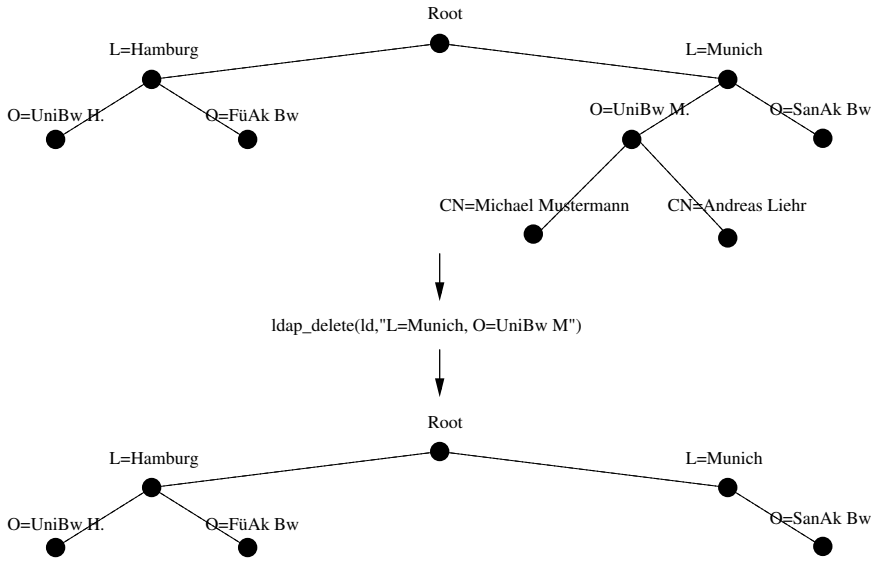

Abbildung 2.11: Auswirkungen einer Delete-Operation auf den DIT

Es existieren noch einige weitere Operationen, wie die Modify-DN-Operation oder die Compare-Operation. Näheres dazu kann in den Spezifikationen zum LDAP-Protokoll (siehe Literaturverzeichniss) nachgelesen werden.

2.3.3 Methoden zur Authentifizierung

Wie schon angesprochen, existieren verschiedene Möglickeiten der Authentifizierung eines Nutzers mittels des LDAP-Protokolls.

Anonyme Authentifizierung

Diese Methode wird normalerweise verwendet, wenn Nutzer ausschließlich lesend auf das Verzeichnis zugreifen wollen. Aus Sicherheitsaspekten sollte ein Server so konfiguriert sein, daß es anonymen Nutzern unmöglich ist, Veränderungen am Verzeichnis durchzuführen. Normalerweise wird ein Client, der einen Bind-Request nicht erfolgreich durchführen konnte anonym gebunden, wenn der Server anonyme Binds unterstützt. Ein Client kann jedoch auch in seinem Bind-Request sofort anonyme Bindung anfordern.[11]

Passwort-basierte Authentifizierung

Hier authentifiziert sich der Client mittels einer DN und dem Passwort, das in den Attributen des zugehörigen Eintrages gespeichert ist. Dabei ist zu beachten, daß die Übertragung von Anmeldeinformationen nur verschlüsselt durchgeführt werden sollte. Das LDAP Protokoll unterstützt zwar eine Authentifizierung ohne Verschlüsselung, davon ist jedoch dringend abzuraten. Standardmäßig wird zum Schutz von Passwörtern der DIGEST-MD5 SASL-Mechanismus verwendet.[11]

Zertifikat-basierte Authentifizierung

Ein Nutzer, der über ein Public/Private Schlüsselpaar verfügt, von dem der Public-Key von einer Zertifizierungsautorität signiert wurde, kann dieses Schlüsselpaar zum Authentifizieren verwenden. Dabei muss das Zertifikat im Betreff-Feld den DN des Nutzers enthalten. Der Nutzer sendet dann dem Server ein Zertifikat und der Server führt eine Private-Key basierte Verschlüsselung durch um die Zusammengehörigkeit von Zertifikat und Schlüssel zu prüfen. Ist dies erfolgreich, so wird der Nutzer an das Verzeichnis gebunden.[11]

2.4 Ein Accounting-Modell für WLAN-Verbindungen

Nachdem die Grundlagen des LDAP Protokolls erläutert wurden, wird nun ein Accounting-Modell für Internetprovider entwickelt, das mittels des LDAP-Protokolls realisiert werden

kann. Dazu muss der Vorgang vom Entschluss, einen Vertrag zur Nutzung des Internets abzuschließen, bis zur eigentlichen Verbindung in mehrere Schritte aufgespalten werden. Folgende Schritte sind im Einzelnen nötig:

- **Providerwahl** Der Kunde informiert sich über die unterschiedlichen Provider und ihre Tarife. Daraufhin wählt er den für seine Bedürfnisse am besten geeigneten Provider und schließt bei diesem einen Vertrag ab. Hierbei ist es jedoch noch möglich, innerhalb seines Vertrages unterschiedliche Pakete mit unterschiedlichen Leistungen und Preisen zu wählen. Dies geschieht erst im folgenden Schritt.

- **Tarifwahl** Der Kunde hat nun einen Account bei seinem Provider und kann selbst zwischen den einzelnen Tarifmodellen wählen und das für sich am besten Geeignete auswählen. Das von ihm gewählte Modell wird ihm bei der nächsten Einwahl automatisch zur Verfügung gestellt. Eine Änderung des Tarifes ist auch danach noch jederzeit möglich und erfordert nur die Trennung der Verbindung und eine erneute Einwahl.

- **Einwahl** Der Nutzer wählt nun den Server des Anbieters an, um eine Verbindung herzustellen. Nun muss sich der Nutzer mittels seines Accounts authentifizieren und bekommt dann automatisch seinen derzeit gewählten Tarif zugeteilt.

2.4.1 Providerwahl

Als Erstes muss der Kunde sich für einen Provider entscheiden und bei diesem einen Account beantragen. Dabei würde ein zentralisierter Server, auf dem man sich einwählen kann, ohne über einen Account zu verfügen und dessen einzige Funktionalität die Auswahl und der Vergleich von Providern darstellt, die beste Möglichkeit sein. Ob diese Möglichkeit praktisch umsetzbar ist (alle Provider müssen sich bereiterklären, an diesem Dienst teilzunehmen, bzw. ihn mit zu bezahlen), ist natürlich fraglich. Dies würde aber ein Modell erlauben, das gänzlich ohne eine bereits vorhandene Internetverbindung auskommt.

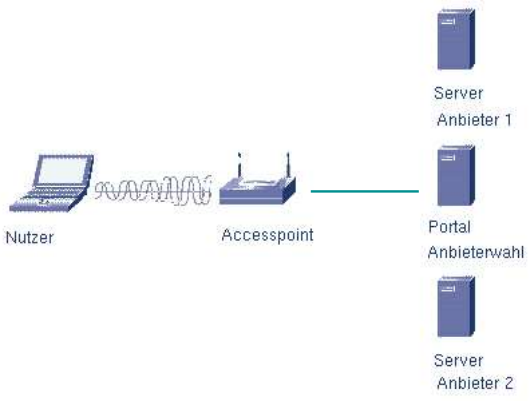

Abbildung 2.12: Herstellung der Verbindung zur Providerwahl

Ein potentieller Kunde wählt sich auf einem Portalserver ein und vergleicht die Angebote unterschiedlicher Anbieter. Anschließend hat er auf diesem Portal die Möglichkeit, Kunde bei einem Anbieter zu werden und eine Nutzerkennung zu erhalten. (siehe Abb. 1.12)
Die LDAP-spezifischen Anteile bei der Providerauswahl beschränken sich darauf, daß für den neuen Kunden ein Eintrag im Verzeichnis angelegt werden muss. Dies obliegt dem Provider selbst. Dabei wäre es empfehlenswert, den Kundenstamm zu gliedern (zum Beispiel nach regionalen Kriterien), um die Übersicht zu bewahren. So wäre es zum Beispiel möglich, einen Baum aufzuspannen, in dem Deutschland die Wurzel ist, und dann nach Bundesländern unterteilt wird, diese wieder nach Städten usw. Eine weitere Möglichkeit wäre die Unterteilung nach Kundennummern, Postleitzahlen oder Anfangbuchstabe des Nachnamen. (siehe Abb. 1.13)

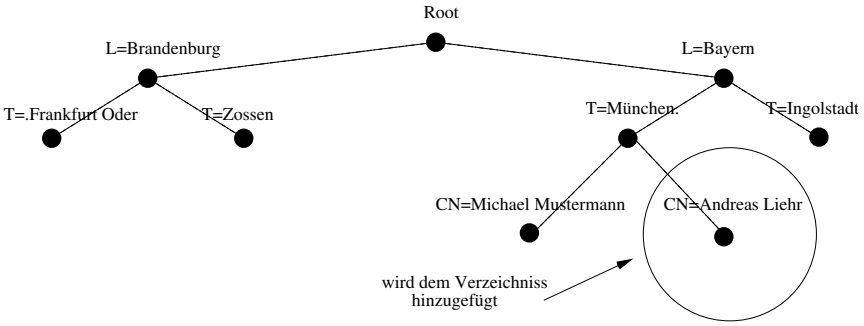

Abbildung 2.13: Hinzufügen eines neuen Nutzers zum Verzeichnis

Wenn sich ein Kunde für diesen Anbieter entscheidet, so tritt er mit diesem in Kontakt (Idealerweise über ein Formular für den Web-Browser) und erhält einen Nutzernamen und ein Passwort. Den Tarif, den er dann für seine Einwahl nutzen will, kann er daraufhin selbst festlegen.

2.4.2 Tarifwahl

Hier kann der Kunde eines Providers zwischen den Tarifen dieses Providers wählen. Idealerweise stellt hierfür der Anbieter ein kostenloses Portal zur Verfügung. (siehe Abb. 1.14)

Im Folgenden ein fiktives Tarifmodell eines solchen Providers. Dabei werden dem Kunden 3 Tarife (Small, Middle und Large) angeboten. Der Nutzer ist in der Lage, vor jeder Einwahl den Tarif zu wechseln und dadurch zu entscheiden, zu welchen Kosten und zu welchen Gebühren er bei der nächsten Einwahl online geht.
Somit kann der Kunde sich dann auf diesem Portal mittels seines Nutzernamen und seines Passwortes einwählen und dann seine Tarifauswahl treffen. Im Beispiel hätte er die Auswahl zwischen Paket S, M und L.

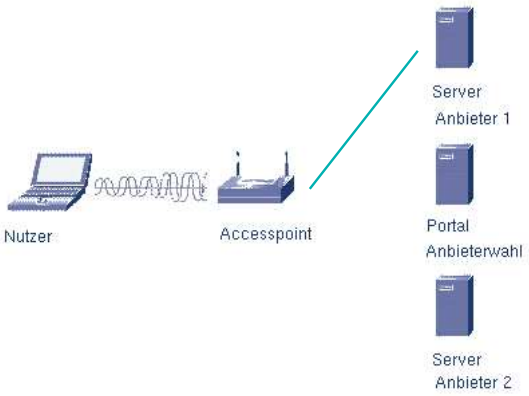

Abbildung 2.14: Herstellung der Verbindung zur Tarifwahl

	Paket S	Paket M	Paket L
HTTP Upload	5 k/s	50 k/s	500 k/s
HTTP Download	10 k/s	100 k/s	1000 k/s
FTP Upload	10 k/s	100 k/s	1000 k/s
FTP Download	15 k/s	150 k/s	1500 k/s
Preis	1 Cent/min	2 Cent/min	4 Cent/min

Der Nutzer wählt sich auf einem Server seines Providers ein und authentifiziert sich mit dem Nutzernamen und dem Passwort, das er bei der Providerauswahl erhalten hat. Er kann nun seine aktuelle Rechnung und seinen derzeitigen Tarif anzeigen lassen. Außerdem kann er seinen Tarif ändern.

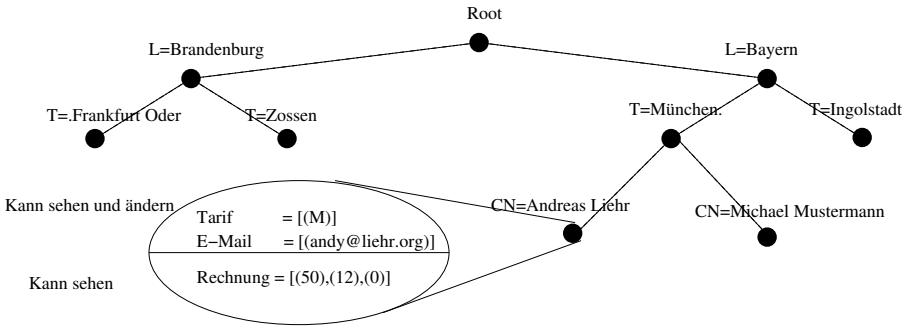

Abbildung 2.15: Struktur der Tarifinformationen im DIT

Hierbei arbeitet der Nutzer direkt auf dem Datenbestand des Verzeichnisses seines Anbieters. Da es die Möglichkeit gibt, die Rechte zum Ändern von Einträgen bis auf die Ebene einzelner Attribute herunter zu granulieren, ist es möglich, daß sich der Nutzer mit der eigenen DN an den LDAP-Server anbindet und die Berechtigung hat, seinenTarif zu ändern. Dadurch ist es nicht mehr notwendig, daß das Portal zur Tarifwahl sich mit einem administrativen Nutzer an den LDAP-Server bindet. Dadurch entfallen einige Sicherheitsrisiken und eine Prüfung auf Zulässigkeit von Operationen ist nicht mehr nötig, weil der Nutzer durch seine Rechte auf dem LDAP-Server ausreichend eingeschränkt wird. Eine unerwünschte Änderung am Verzeichnis wird somit ausgeschlossen. (siehe Abb. 1.15)

2.4.3 Einwahl

Nachdem der Kunde nunmehr einen vollwertigen Account bei einem Anbieter hat, kann er sich über den Server des Anbieters einwählen. Dazu benötigt er die Adresse des Einwahlservers des Anbieters und seine Nutzerdaten (Nutzername, Passwort). Nachdem er sich eingewählt hat, stehen ihm die Dienste seines Tarifs zu den jeweiligen Bandbreiten zur Verfügung. Außerdem werden die Gebühren verbucht, die er für seinen Tarif zu zahlen hat, bis er die Verbindung wieder trennt. (siehe Abb. 1.16)

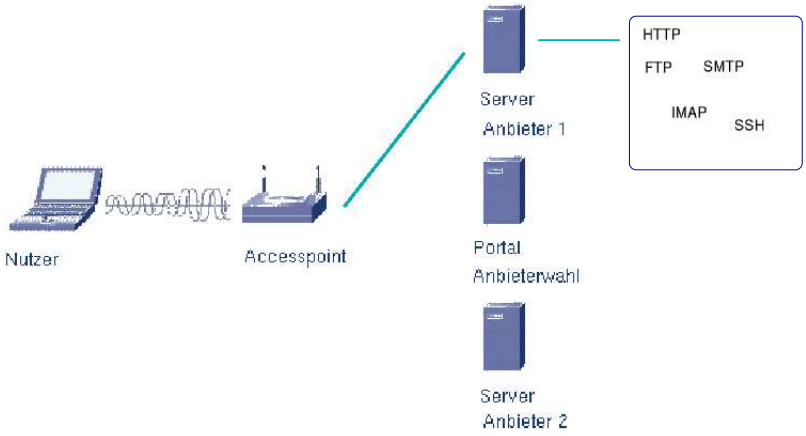

Abbildung 2.16: Einwahl auf dem Dial-In Server

Bei der Einwahl selber wird der Nutzer direkt anhand seiner DN und seines Passwortes authentifiziert. Eine Authentifizierung über Zertifikat macht wenig Sinn, weil man dann von jedem Nutzer verlangen müsste, daß er ein zertifiziertes Public/Private Schlüsselpaar besitzt. Darunter würde natürlich unweigerlich die Nutzerfreundlichkeit leiden. Es wäre jedoch aus sicherheitstechnischen Aspekten sinnvoll, sicherheitsbewußten Nutzern diese Möglichkeit trotzdem anzubieten. Das Abrechnungssystem kann nun die Informationen über den Tarif des Nutzers direkt aus dem Verzeichniseintrag des Nutzers übernehmen. Des Weiteren können dadurch die Dienste und zur Verfügung gestellten Bandbreiten des Nutzers festgelegt werden. Die Summe der zu zahlenden Gebühren kann dann auch wieder direkt in ein Attribut des Verzeichniseintrages des Nutzers geschrieben werden.

2.4.4 Zusätzliche Möglichkeiten des Accountingmodells mit LDAP-Protokoll

Die Lösung mittels LDAP-Protokoll eröffnet noch einige weitere interessante Möglichkeiten. Da hier ein Nutzeraccount existiert, dem in Form von Attributen beliebige weitere Informationen zugeordnet werden können, ist es möglich, dieses Nutzerkonto zur Authentifizierung für beliebige andere Anwendungen zu nutzen. Denkbar wäre zum Beispiel eine Authentifizierung für Administrationsdienste von Webseiten oder E-Mail-Konten. Ein anderes Einsatzgebiet wäre zur Authentifizierung für E-Commerce Anwendungen. So können entweder gekaufte Dienstleistungen und Waren mit über den Provider abgerechnet

werden, oder aber mit dem Einverständnis des Nutzers Kreditkarten oder Kontoinformationen übermittelt werden. Eine weitere Möglichkeit wäre das Speichern von Adressinformationen, da diverse Mail-Programme die Möglichkeit besitzen, ihre Adressbücher in LDAP-Verzeichnissen zu speichern. Auch hier ist es wieder möglich, daß der Nutzer selbst einige über ihn gespeicherte Informationen im Verzeichnis ändern kann, indem er sich mit seinem DN an das Verzeichnis bindet. Diese Informationen könnten dann für beliebige Anwendungen benutzt werden.

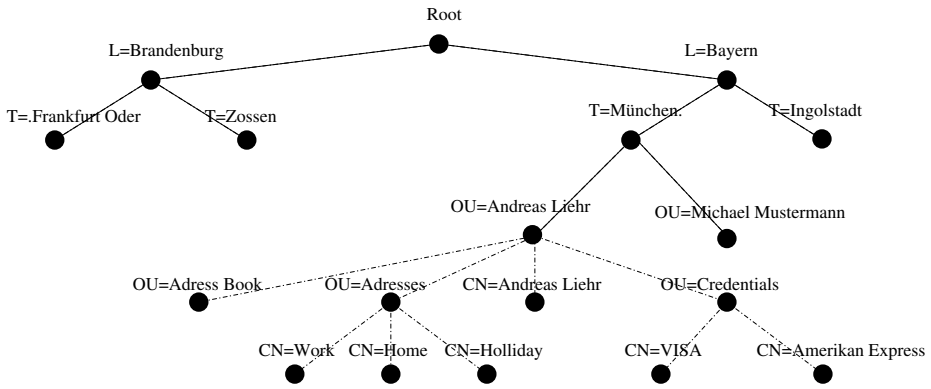

Abbildung 2.17: Mögliche Struktur eines Nutzereintrags mit Zusätzlichen Features

In dem dargestellten Beispiel wird für jeden Kunden eine eigene Organisationseinheit erstellt, die außer ihm als Person noch Angaben über Wohnsitze, Konten, persönliche Daten und ein Adressbuch für Mail-Programme und andere Anwendungen enthält. Es wäre auch denkbar, für ein Nutzerkonto mehrere Personen anzulegen, zum Beispiel für eine Familie. Dementsprechend könnten dann auch die Kosten die einzelne Familienmitglieder verursacht haben, nachvollzogen werden. (siehe Abb. 1.17)

2.5 Betrachtungen zum Accounting-Modell mittels LDAP-Protokoll

Im folgenden soll auf den praktischen Nutzen der hier skizzierten Lösung eingegangen werden und ein kurzer Überblick über sicherheitstechnische Aspekte der Lösung gegeben werden. Zuvor jedoch wird die Möglichkeit untersucht, das Modell mit einem AAA-Server zu kombinieren.

2.5.1 Versuch der Kombination mit einer AAA-Lösung

Ursprünglich sollte hier ein Vergleich des aufgestellten Modells mit einem AAA-Server gezogen werden. Als AAA-Server wurde der reeRadius-Server[6] herangezogen. Hierbei handelt es sich um ein Projekt, das unter der GPL steht und für jeden kostenlos nutzbar ist. Es stellte sich jedoch heraus das gerade dieser Server die Möglichkeit bietet, auf einem Verzeichnisdienst zu arbeiten. Somit wurde daraus vielmehr ein Versuch, den freeRadius-Server in das Modell zu integrieren.

Das Konzept des freeRadius-Servers

Hierbei handelt es sich unter Anderem um eine Komplettlösung zum Herstellen von PPP-Verbindungen. Zum Einen können Nutzer mit unterschiedlichen Rechten verwaltet werden und zum Anderen ist eine komplette Abrechnungsmöglichkeit enthalten, indem zum Beispiel die Zeit der Verbindungsnutzung festgehalten wird. Dabei können die Informationen des Servers (Nutzer, Onlinezeiten, Rechte etc.) entweder in Dateien, Datenbanken oder Verzeichnissen abgelegt werden. Was besonders im Rahmen dieser Arbeit interessant ist, ist die Möglichkeit mittels des LDAP-Protokolls zu arbeiten.[6]
Die Authentifizierung eines Nutzers wird hier in zwei Schritten durchgeführt:

- **Authorisation** Hierbei werden aus einer externen Datenquelle Informationen über den Nutzer eingeholt und geprüft, ob der von ihm angeforderte Dienst für ihn erlaubt ist. Zum Beispiel beim Versuch eines Dial-In würde hier geprüft werden, ob diesem Nutzer eine Einwahl erlaubt ist. Die für die Authorisation nötigen Informationen können in unterschiedlichen Datenquellen gespeichert sein. Üblich sind Dateien, SQL-Datenbanken und LDAP-Server.
- **Authentifizierung** Bei der Authentifizierung wird die Identität des Nutzers überprüft. Dies kann über Abfrage eines Passworts oder ein Zertifikat erfolgen. Auch hier besteht wieder die Möglichkeit, einen LDAP-Server zu nutzen. In diesem Fall wird ein Bind-Request mit den Credentials des Nutzers ausgeführt. Ist dieser erfolgreich, so ist auch die Authentifizierung erfolgreich. Authentifizierung mittels eines SQL-Servers ist wenig sinnvoll, da normalerweise nicht jedem Nutzer, der einen Einwahldiest nutzen will, ein Nutzer auf einem SQL-Server angelegt wird.

Als reiner Einwahlserver ist der freeRadius-Server dem hier entwickelten Modell überlegen. Er kann auf unterschiedliche Datenquellen zugreifen und besitzt somit eine höhere Flexibilität.
Im Bereich der Abrechnung ergibt sich hier jedoch der Mangel, daß der Nutzer nicht selbständig seinen Tarif ändern kann. Für einen Tarifwechsel wäre hier also immer eine Handlung seitens eines Administrators nötig. Außerdem sind hier die zusätzlichen Möglichkeiten, die unser Modell bietet, also Speichern von Adressbüchern etc., nicht vorhanden.
Was den freeRadius-Server jedoch sehr interessant macht, ist die Möglichkeit, ihn mit dem hier entwickelten Modell zu verbinden. Da sämtliche Informationen über Authorisierung, Authentifizierung und Abrechnung in einem Verzeichnis gespeichert werden können, auf das mittels LDAP-Protokoll zugegriffen wird, könnte man sämtliche Einwahl- und Abrechnungsvorgänge durch den freeRadius-Server abwickeln lassen. Trotzdem könnte man mittels eines Portals den Nutzer selbst seinen Tarif wählen lassen und im Verzeichnis andere Informationen speichern.

Das Beispiel zeigt die Möglichkeit des Eintrags für einen Nutzer. Da für den Nutzer eine eigene Organisationsuntereinheit angelegt wird, ist die Erweiterung um ein eigenes Adressbuch, Informationen zum Wohnsitz oder Kreditkarteninformationen problemlos machbar. Das eigentliche Objekt der Person beinhaltet zum einen die nötigen Attribute des

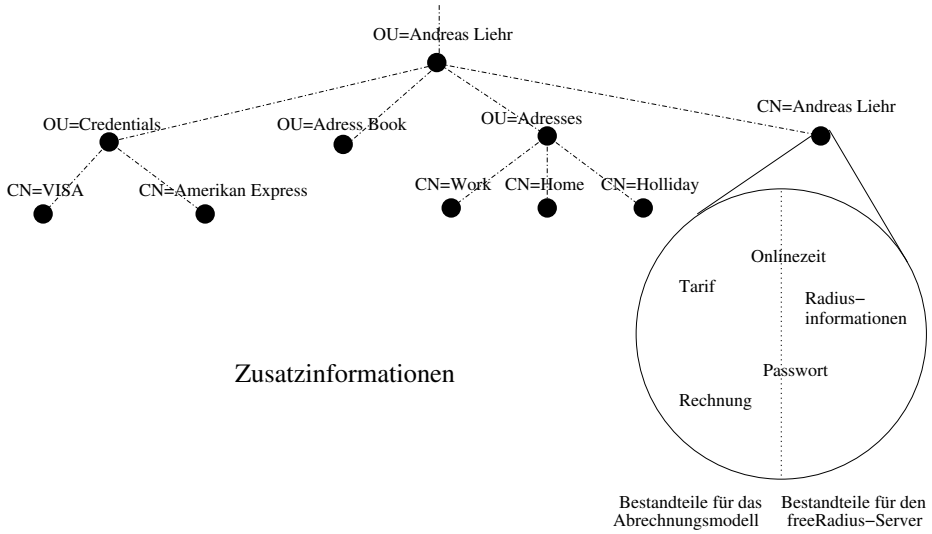

Abbildung 2.18: Eintrag für einen Nutzer mit Informationen für Zusätzliche Features und der Einwahl mittels eines freeRadius-Servers

freeRadius-Servers, aber auch die für das Modell nötigen Informationen. Dabei werden Attribute wie das Passwort und die Zeit, die der Nutzer online war, von beiden Seiten aus benötigt. (siehe Abb. 1.18)
Ein Tarifwechsel würde sich nun so darstellen:

- Der Nutzer stellt die Verbindung zum Portal (zum Beispiel einer Website) her und authentifiziert sich anhand seines Accounts. Im Beispiel müsste der Nutzer dazu Bundesland, Stadt und Namen, sowie sein Passwort angeben.
- Der Nutzer wählt seinen neuen Tarif. Daraufhin muss die Software die Onlinezeit auslesen und auf 0 setzen, dann die Onlinezeit mit den Kosten des Tarifs der zuvor gewählt war multiplizieren und auf die Rechnung schreiben. Anschließend wird der neue Tarif eingetragen.

Damit ist der Tarifwechsel vollzogen und der Nutzer kann sich zu seinem neuen Tarif einwählen. Dieses Modell funktioneiert jedoch nicht wenn die Tarifwahl erfolgt, während die Abrechnung des Nutzers läuft. Hierfür wäre eine komplexere Lösung vonnöten. Man könnte zum Beispiel ein extra Attribut für gewählten und aktuellen Tarif schaffen und bei jeder Einwahl den Wert für die Onlinezeit auf Null setzen und davor die bei der letzten Einwahl genutzte Zeit mit dem gewählten Tarif verrechnen und auf die Rechnung schreiben. Danach kann man in dem Attributfeld für den aktuellen Tarif den neu Gewählten setzen.

2.5.2 Gedanken zur Realisierbarkeit und praktischem Nutzen

Hierbei muss zwischen Aspekten der technischen Realisierung und Aspekten der praktischen Realisierung unterschieden werden.

Technische Realisierung

Von der technischen Seite her würde sich die Realisierung nicht sehr kompliziert gestalten. So stellt das Anlegen der entsprechenden Schemen und das Installieren der benötigten Server sicherlich kein großeres Problem dar. Ein großer Vorteil ist außerdem, daß die benötigte Software frei verfügbar ist. OpenLDAP fällt zum Beispiel unter die GPL (GNU General Publlic License) und wäre somit für dieses Modell ideal geeignet. Als Portal könnte eine leicht zu implementierende dynamische Webseite fungieren. Hier würde sich ein Apache-Webserver mit den entsprechenden Modulen für PHP und SSL eignen. PHP bietet sich deshalb an, weil es über ein sehr leistungsfähiges Modul für den Umgang mit LDAP-Verzeichnissen verfügt. Der Apache-Webserver ist deshalb sehr gut dafür geeignet, weil er über ein Modul (mod_auth_ldap) verfügt, das es ermöglicht, Nutzer, die auf Bereiche des Servers zugreifen wollen direkt über ein LDAP-Verzeichnis zu authentifizieren. Somit wäre also der Test eines solchen Modells nicht an großen Aufwand oder gravierende Kosten gebunden.

Praktische Realisierung

Die Praktische Realisierung gestaltet sich schon komplizierter. Zum Einen muss es möglich sein, daß ein Neukunde sich auf einem Server einwählen kann, um einen Vertrag mit einem Anbieter abzuschließen. Dazu muss er zum Einen die Möglichkeit haben, einen Accesspoint zu nutzen und zum Zweiten eine zentrale Anlaufstelle nutzen können, die ihm eben diesen Dienst anbietet. Dies wäre wohl nur realisierbar, wenn ein Providerübergreifendes Portal zur Anmeldung geschaffen werden würde.
Das nächste Hindernis bietet sich bei der Tarifwahl. Hier muss der Anbieter dem Kunden die Möglichkeit bieten, seinen Tarif festlegen zu können, ohne sich einzuwählen. Dies wäre über einen hierfür gesondert geschaffenen Server denkbar, den jeder Provider für seine Kunden anbieten würde. Allerdings würden bei dieser Version die Kosten für die Verbindung dem Provider zu Lasten fallen. Man könnte jedoch notfalls auf diesen Dienst verzichten und dem Nutzer vor der ersten Einwahl in den günstigsten Tarif einstufen und ihn nur dann die Mögklichkeit zur Tarifwahl geben, wenn er bereits eine kostenpflichtige Verbindung hergestellt hat.

2.5.3 Sicherheitstechnische Aspekte

Hier muss zwischen zwei Bereichen unterschieden werden. Zum Einen muss man sich Gedanken um die Sicherheit des Modells als solches machen, zum Anderen aber auch um die Sicherheit der Verbindung.

Sicherheit des Modells

Um das Modell möglichst sicher zu gestalten, ist es notwendig, daß die Sicherheitsschemen des Verzeichnisses sehr sorgfältig ausgearbeitet werden. Indem man die Rechte der einzel-

nen Nutzer im Verzeichnis klar und sauber absteckt, wird eine große Risikoquelle bereits beseitigt. Das kann man erreichen, indem man zum Beispiel jedem Benutzer sowohl Lese-, als auch Schreibrechte im Verzeichnis verwehrt und dann nur den Admin-Nutzern Rechte einräumt und zusätzlich auf den einzelnen Objekten nur dem Objekt selbst Leserechte für alle Attribute und Schreibrechte für die Attribute, die geändert werden dürfen, gibt:

```
access to *
        by self read
        by dn.children="dc=provider,ou=admins" write

access to attr=tarif,telefon
        by self write
```

(Jeder darf seine Daten lesen. Jeder, der in der Organisationseinheit *Admins* der Domäne *Provider* geführt wird darf alles ändern. Jeder darf seine eigene Telefonnummer und seinen eigenen Tarif ändern)
Dadurch wird das Auslesen fremder Daten und das unberechtigte Ändern von Verzeichnisinformationen schon mit dem Schema verhindert.[5]
Ein weiterer Punkt ist, daß man dafür Sorge tragen muß, daß nur dann eine Verbindung zum Internet durch einen Client hergestellt werden kann, wenn er sich auf dem Server korrekt eingewählt hat und sichergestellt ist, daß ihm seine Nutzung auch berechnet wird. Dies korrekt zu implementieren wäre Aufgabe des Providers.
Ein letzter Punkt ist die Absicherung der Portale zur Wahl von Provider und Tarif. Hier ist es notwendig, dafür Sorge zu tragen, daß kein potentieller Angreifer die Möglichkeit erhält, über diese eine Verbindung zum Internet herzustellen. Auch dies ist wieder eine Frage der anspruchsvollen Administration.

Sicherheit der Verbindung

Hier geht es darum, die Verbindung des Clients zum Server sicher zu gestalten. Da es sich hier um eine WLAN-Verbindung handelt, ist es natürlich für jeden möglich, die Übertragenen Daten mitzuempfangen. Demzufolge ist eine angemessene Verschlüsselung hier unerlässlich. Es genügt nicht, Passwörter verschlüsselt zu übertragen. Um die Privatsphäre der Nutzer zu wahren und eine ausreichende Sicherheit herzustellen, ist es unerlässlich, daß die gesamte WLAN-Kommunikation verschlüsselt erfolgt.[4]

2.6 Zusammenfassung

Die Möglichkeit, ein Providermodell zur Nutzung des Internets über WLAN-Netze zu betreiben, das seine Daten in Verzeichnisdiensten ablegt, besteht. Das Modell wäre ohne hohe Kosten oder Vorarbeiten realisierbar und bietet diverse Vorteile. Zum Einen kann der Verzeichnisdienst auch für andere Anwendungen, wie zum Beispiel Berechtigungsprüfungen von Webseiten oder Datenbanken für Mailprogramme genutzt werden. Zum Anderen

garantiert das LDAP-Protokoll hohe Sicherheitsstandards, die es ermöglichen, Zugriffsrechte bis auf Attributebene hinunter zu bestimmen und machen so eine einfache und übersichtliche Sicherung des Datenbestandes möglich. Auch die Möglichkeit das Modell mit einem freeRadiuss-Server zu kombinieren, bietet erfolgsversprechende Möglichkeiten. Dies hat außerdem den Vorteil, daß ein Großteil des selbst zu tätigenden Programmieraufwandes entfallen würde. Bislang fehlt jedoch die praktische Erprobung eines solchen Modells und bevor diese abgeschlossen ist, kann man keine endgültige Aussage über den praktischen Nutzen eines solchen Modells treffen.

Abkürzungsverzeichniss

AAA	Authentifizierung, Authorisierung, Abrechnung
DAP	Directory Access Protocoll
DIB	Directory Information Base
DIT	Directory Information Tree
DMD	Directory Managment Domain
DN	Distinguished Name
DSA	Directory System Agent
DUA	Directory User Agent
GPL	GNU General Public License
LDAP	Leightweight Directory Access Protocoll
WLAN	Wireless Local Area Network

Literaturverzeichnis

[1] ITU-T, Series X: Data Networks and open System Comunications, X.500 Directory

[2] LDAP (v3) Revision (ldapbis)
http : //www.ietf.org/html.charters/ldapbis - charter.html

[3] White Paper LDAP Version 3
http : //www.isode.com/whitepapers/ic - 6032.html

[4] IT Grundschutzhandbuch
http : //www.bsi.de/gshb/deutsch/menue.htm

[5] Homepage des OpenLDAP-Projektes
http : //openldap.org

[6] Homepage des freeRadius-Projektes
http://www.freeradius.org

[7] Understanding X.500 Abbreviations
http://www.isi.salford.ac.uk/staff/dwc/Version.Web/Abbreviations.htm

[8] LDAP: The Protocol
http://www.ietf.org/internet-drafts/draft-ietf-ldapbis-protocol-13.txt

[9] Lightweight Directory Access Protocol (v3): Technical Specification
http://www.ietf.org/rfc/rfc3377.txt?number=3377

[10] Connection-less Lightweight X.500 Directory Access Protocol
ftp://ftp.venaas.no/pub/rfc/rfc1798.txt

[11] LDAP: Authentication Methods and Connection Level Security Mechanisms
http://www.ietf.org/internet-drafts/draft-ietf-ldapbis-authmeth-05.txt

[12] Heise-Newsticker
http://www.heise.de

Kapitel 3

WAP versus i-mode

Michael Melchior

WAP und iMode sind auf den ersten Blick zwei völlig unterschiedliche Technologien, die sich damit befassen, das Internet für mobile Endgeräte verfügbar zu machen.
In dieser Arbeit wird zunächst die Architektur von WAP 1.x vorgestellt, sowie die Beschreibungssprache für die von WAP 1.x dargestellten Inhalte. Anschliessend wird auf die Übertragung zum Endgerät eingegangen und anhand einer Beispielanwendung die Fähigkeit von WAP 1.x umrissen.
Danach wird die Weiterentwicklung zu WAP 2.x anhand deren Architektur und Beschreibungssprache erläutert. Zudem sollen dessen Neuerungen anhand der Fortentwicklung der Beispielanwendung deutlich gemacht werden.
Anschliessend wird auch die Architektur von iMode beschrieben und auch hier die Möglichkeiten anhand der Beispielanwendung vorgestellt.
Zuletzt werden beide Techniken miteinander verglichen. Dabei werden vor allem Gemeinsamkeiten bis hin zur teilweisen Kompatibilität auffallen.
Im Fazit wird letztlich festgestellt werden, daß WAP und iMode gemeinsam den Weg zu UMTS ebnen sollen.

Inhaltsverzeichnis

3.1 Einleitung

Am Anfang war das Internet einem kleinen Personenkreis, der Zugang zu einem abgeschotteten Netzwerk hatte, vorbehalten. Das später daraus entstandene WorldWideWeb war dann schon für jeden verfügbar, der einen Telefonanschluß besaß. Doch inzwischen können Besitzer entsprechender Endgeräte Inhalte aus dem Internet überall da beziehen, wo es die Netzabdeckung und das Angebot des jeweiligen Mobilfunkbetreibers zulassen.
Diese Inhalte reichen von der Möglichkeit, E-Mails zu lesen und zu schreiben über kleine Spiele zum Zeitvertreib und den Abruf aktueller Veranstaltungskalender des Ortes, in dem sich der Nutzer gerade befindet, bis hin zu den Börsennachrichten, Wegbeschreibungen, Standortermittlungen oder gar kleinen Filmchen. Das Mobile Endgerät, meist ein Handy, ist jedoch in seiner Fähigkeit, Daten zu speichern, zu verarbeiten oder darzustellen bei weitem nicht mit einem multimediafähigen PC am heimischen Schreibtisch zu vergleichen. Ebenso waren die Mobilfunknetze ursprünglich dazu ausgelegt, das gesprochene Wort und allenfalls noch eine Kurznachricht zu übermitteln, nicht aber Peilmeldungen, Musik- oder Videodatenströme.
Es mussten also entweder neue Standards geschaffen oder die alten modifiziert werden. Das im Jahre 1997 von Nokia, Ericsson, Motorola und Phone.com gegründete WAP-Forum entschied sich dafür, zunächst das Internet für das in Europa weit verbreitete, verbindungsorientierte GSM-Netz mit einem speziellen Protokoll, dem Wireless Application Protocol, nutzbar zu machen. Anders als der japanische Mobilfunkbetreiber NTT DoCoMo, der iMode für das auf Paketvermittlung basierende Personal digital Cellular-Packet (PDC-P) entwickelt hat.
Während iMode sich in seiner Heimat grösster Beliebtheit erfreut, floppte WAP hierzulande. Für beides gibt es viele Ursachen, ebenso gibt es gute Gründe anzunehmen, daß sich iMode mit der Einführung von GPRS und später UMTS auch in Europa durchsetzen und WAP damit sogar verschmelzen könnte.

3.2 WAP

Auf einem WAP-fähigen Endgerät kann der Nutzer Internetseiten abrufen und über Hyperlinks zwischen den Seiten navigieren. Texteingaben sind ebenfalls möglich. Damit ähnelt WAP dem World Wide Web sehr, obgleich es noch weit davon entfernt ist, da die Endgeräte wegen der langsamen CPUs, dem fehlenden Massenspeicher, der kleinen Anzeige, schlechter Eingabemöglichkeiten und der geringen Bandbreite des Netzwerkes stark eingeschränkt sind.

3.2.1 WAP 1.x

WAP 1.x ist eine nahezu rein textbasierte Möglichkeit, mobil auf das WWW zu zugreifen.

Der WAP 1.x Protokollstapel

Das Wireless Application Protocol 1.x ist in eine Hierarchie von fünf Protokollschichten unterteilt (vgl. Abb. 3.1), die am ISO / OSI Referenzmodell ausgerichtet sind.

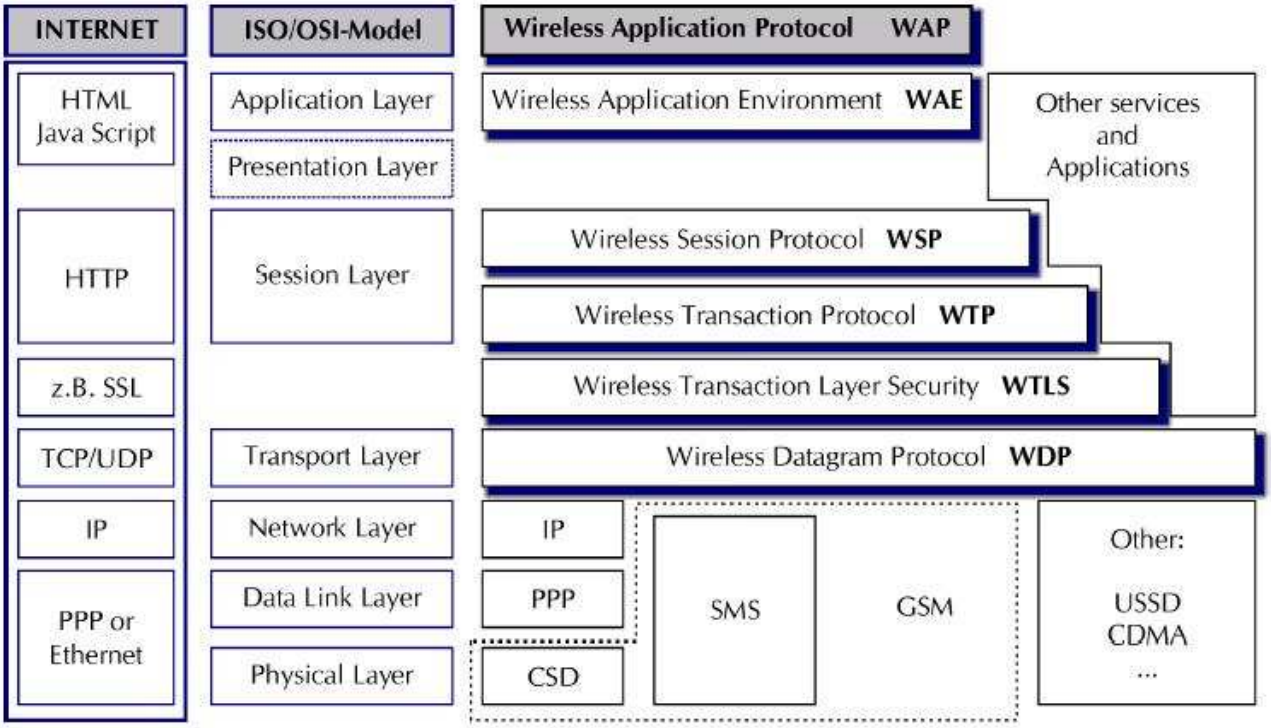

Abbildung 3.1: Der WAP 1.x Protokollstapel [3]

Die Schichten im Einzelnen:

WAE Diese Protokollschicht definiert, wie der Name Wireless Application Environment schon sagt, die Umgebung der Anwendungen. Im Vordergrund steht hierbei der WAP-Browser. Hier befindet sich ebenfalls die Definition der Wireless Markup Language (WML), der Scriptsprache WMLScript sowie Schnittstellen zu Sprachmehrwertdiensten, wie etwa der Verwaltung von Anrufumleitungen oder der persönlichen Mailbox.

WSP Das Wireless Session Protocol bietet Browsern des WAE die Schnittstelle zu zwei verschiedenen Session Services. Diese sind zum einen ein verbindungsorientierter Service, der weiter über die folgende WTP Schicht abgewickelt wird, zum anderen aber auch ein verbindungsloser Service, der die nächsten beiden Schichten überspringt und direkt zum Wireless Datagram Protocol (WDP) über geht.
Unterstützt werden hier in binärer Form HTTP, als auch Sitzungen, die ein Abschalten und erneutes Einschalten des Gerätes überdauern.

WTP Das Transaktionsprotokoll beinhaltet die Basisfunktionen zur Kommunikation zwischen dem Endgerät und dem Server. Dabei werden drei Arten der Kommunikation unterstützt:

- unsichere Einweg-Anforderung
- sichere Einweg-Anforderung
- sichere Zweiweg-Anforderung und -Antwort

Da das Übertragungsmedium, auf dem der Protokollstapel aufsetzt, ohne weiteres unterbrochen werden kann, sei es durch mangelnde Netzabdeckung oder durch einen

leeren Akku des Endgerätes, musste über diese Protokollschicht eine zuverlässige Verbindung gewährleistet werden. Sie basiert auf positive Quittungen, die auf jede Empfangene Nachricht folgen müssen. Ist dies nicht der Fall, wird die Nachricht erneut versandt. Eine eindeutige Nummerierung verhindert doppelte Nachrichten.

WTLS Das Sicherheitsprotokoll ist ebenfalls aus einem bereits etablierten Standard hervor gegangen: Dem im Internet bereits verbreiteten Transport Layer Security (TLS), das wiederrum von Secure Socket Layer (SSL) abstammt. Es stellt die Datenintegrität, den Schutz gegen Mithören, die Authentifizierung als auch den Schutz vor DOS-Angriffen sicher.

WDP Verglichen mit dem ISO / OSI Referenzmodell stellt das WDP die Funktionalität des Transport-Layers zur Verfügung. Es passt sich dem darunter liegenden Bearer an, der beispielsweise ein GPRS Netz sein kann, per SMS übertragen oder per GSM Cell Broadcast empfangen werden oder einfach über ein Drahtloses DECT Telefon. Sinn und Zweck dieses Protokolls ist es, für die darüber liegenden Schichten eine Unabhängigkeit vom jeweiligen Übertragungsmedium zu schaffen. Hier besteht nun auch die Möglichkeit, WAP in das UMTS Netz zu übertragen.

WML

Um Inhalte auf WAP 1.x-fähigen Geräten darstellen zu können, müssen sie in der auf XML basierenden WML (*Wireless Markup Language*) vorliegen. Die einzeln dargestellte Seite wird hierbei als Karte bezeichnet, wobei eine WML-Datei mehrere solcher Karten beeinhalten kann. Sie wird daher als Kartenstapel bezeichnet. Ein neuer Stapel wird so immer erst dann geladen, wenn der Benutzer zu einer Karte navigiert, die nicht in dem Stapel enthalten ist. Wie bei XML üblich, werden die Elemente des Dokumentes durch tags gekennzeichnet. Dabei wird beispielsweise der Kartenstapel mit <wml> Kartenstapel </wml> umschlossen. Eine Auswahl weiterer gültiger Elemente ist in der Tabelle 3.1 aufgeführt.

In dem in Abbildung 3.2 dargestellten Beispiel wird ein Kartenstapel beschrieben, bei dem der Nutzer die Möglichkeit hat, über eine Auswahlliste einen Namen auszuwählen und ein Passwort einzugeben. Das Beispiel ist sehr einfach gehalten und umfasst nicht etwa eine Prüfung der Eingabe auf ihre Richtigkeit oder gar Aspekte der Sicherheit bei Passworteingaben.
Der Stapel besteht aus drei, durch *card* Tags umgebene Karten: Der *Login* Karte, *Password* Karte und der *Results* Karte. Auf der ersten Karte befindet sich die Auswahlliste mit den Namen der Personen, die sich 'einloggen' können. Zu Beginn der Karte wird innerhalb des *do* Blocks ein Ereignis mit einer Aktion verknüpft. Eine Möglichkeit für ein Ereignis ist beispielsweise ein Druck auf eine Funktionstaste, meist mit *accept* oder *option* bezeichnet. Mit der Aktion *go* kann eine beliebige Karte angesprungen werden, mit *prev* die vorherige. Die Beschriftung der Taste wird mit *label* bestimmt. Im Beispiel handelt es sich um eine Karte, die eine Eingabe mit der *accept* Taste annimmt welche mit dem Label Passwort versehen ist. Weiter ist im *do* Block der Link zur Passwortkarte eingetragen und damit der Eingabe zugeordnet.
Die Liste mit den Namen wird durch den *select* Tag umgeben, der im Wert *name* den Namen der Variablen beschreibt, in die der Name des ausgewählten Elements gespeichert werden soll. Der *option* Tag beschreibt dabei innerhalb des *select* Blocks je ein Element

Element	Beschreibung	Element	Beschreibung
Karten / Kartenstapel		**Variablen**	
card	Karte	setvar	setzen einer Variablen
head	Überschrift		
meta	Metainformation	**Benutzereingaben**	
		input	Texteingabe
Ereigniselemente		select	Auswahlelement
do		option	Optionselement
onenterforward	Bei “Vorwärts”		
onenterbackward	Bei “Zurück”	**Anker und Timer**	
onpick	Bei Auswahl	a	Anker für einen Link
onevent	Bei Ereignis	anchor	Anker
		img	Bild
Textformat			
br	Neue Zeile	**Tasks**	
p	Abschnitt	go	Gehe zu
table	Tabelle	prev	Zurück
tr	Zeile	refresh	Neu laden
td	Spalte	noop	Leere Operation

Tabelle 3.1: Die wesentlichen Elemente der WML

der Liste. In der Beschreibung wird dem jeweiligen Element ein Wert zugeordnet, der unabhängig vom darzustellenden Text ist und der in der im *select* Tag festgelegten Variablen abgelegt wird, wenn das Element ausgewählt wurde. In dem Beispiel sind der Wert und der dargestellte Text gleich.
Die zweite Karte Trägt den Titel und die id ’Password’. Auch hier wird wieder ein Link auf die nächste Karte mit einem *do* Block gelegt. Das Passwort wird hinter dem Label ’Password’ eingetragen, was durch das *input* Tag beschrieben wird. Der eingegebene Wert wird in der Variablen ’password’ abgelegt. Die dritte Karte zeigt letztlich den Ausgewählten Namen und das eingegebene Passwort an. An dieser Stelle wird gezeigt, daß mit *$(variable)* auf die jeweilige Variable zugegriffen werden kann.

```
<?xml version='1.0'?>
<!DOCTYPE wml PUBLIC "-//WAPFORUM//DTD WML 1.1//EN"\\
"http://www.wapforum.org/DTD/wml_1.1.xml">
<wml>
    <card id="Login" title="Login">
        <do type="accept" label="Password">
            <go href="#Password"/>
        </do>
        <p>
            UserName:
            <select name="name" title="UserName:">
                <option value="John Doe">John Doe</option>
                <option value="Paul Smith">Paul Smith</option>
```

Abbildung 3.2: WML Quelltextbeispiel [1]

```
            </select>
        </p>
    </card>
    <card id="Password" title="Password:">
        <do type="accept" label="Results">
            <go href="#Results"/>
        </do>
        <p>
            Password: <input type="text" name="password"/>
        </p>
    </card>
    <card id="Results" title="Results:">
        <p>
            You entered:<br/>
            Name: $(name)<br/>
            Password: $(password)<br/>
        </p>
    </card>
</wml>
```

Grafik bei WAP 1.x

Auf einer WAP 1.x-Seite lässt sich neben reinem Text auch in eingeschränktem Maße Grafik darstellen. Diese müssen allerdings im wbmp Format vorliegen, das lediglich 1 Bit pro Pixel zulässt, also nur schwarz-weiß dargestellt wird (vgl. Abb 3.3). Eine weitere Einschränkung ist natürlich das sehr kleine Display der meisten Endgeräte mit einer Auflösung von etwa 100 x 60 Pixeln.

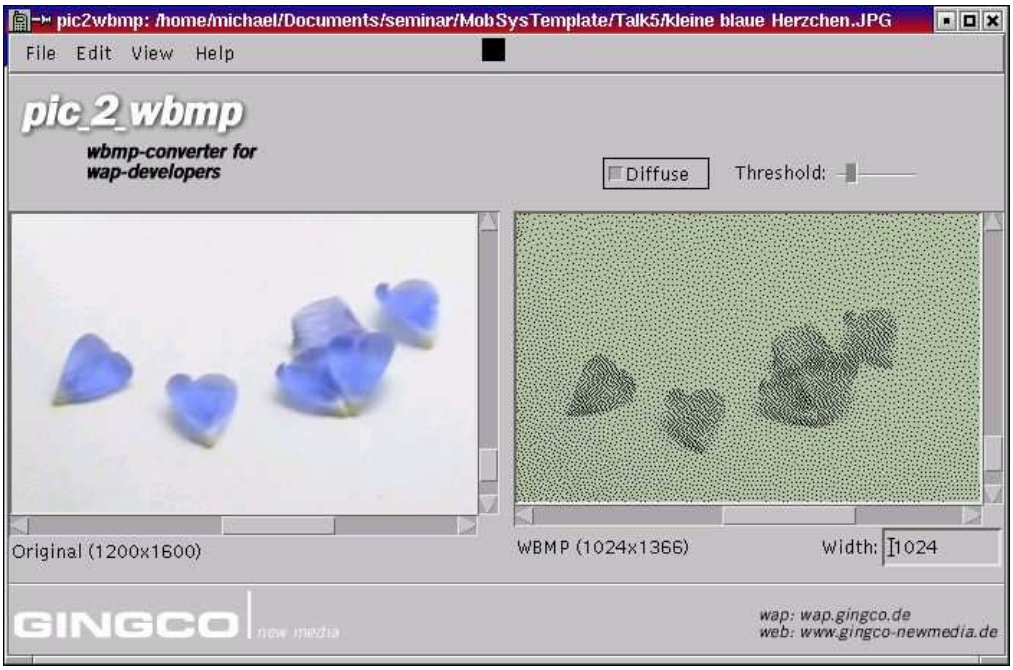

Abbildung 3.3: Ein .jpg Bild in .wbmp Format umgewandelt

Übertragung auf das Endgerät

Nicht immer machen sich Anbieter von Webinhalten die Mühe, neben der in HTML vorliegenden Seite auch eine Version in WML bereit zu stellen. Es existiert zwar die Möglichkeit, die Konvertierung automatisch vorzunehmen, doch bleibt dabei ein Großteil des im Normalfall auf multimediale Unterstützung aufgebauten Inhalts auf der Strecke.
Die Kommunikation des mobilen Gerätes mit einem Webserver geschieht über einen WAP-Proxy, während die Verwaltung von Sprachmehrwertdiensten auf einem Wireless Telephony Application (WTA) Server direkt geschieht (vgl Abb.3.4).

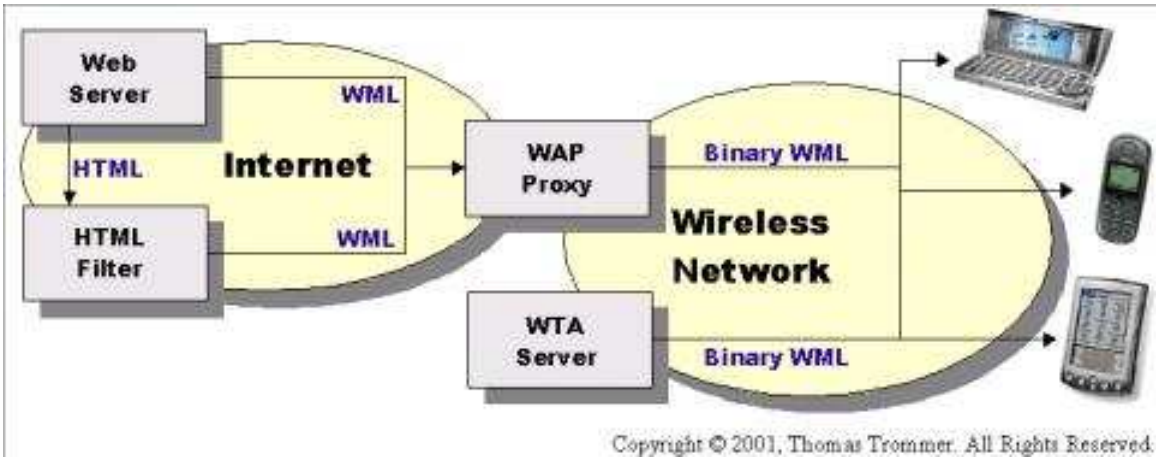

Abbildung 3.4: Der Übertragungsweg bei WAP 1.x [7]

Die Anfragen sendet das Endgerät in WAP binary XML (WBXML), binär kodiertem WML, das gegenüber dem normalen WML kompakter ist. Es nutzt alle acht Bits eines Datenwortes und verwendet mitunter auch Tokens: WML-Elemente, die statt durch lange Zeichenketten durch einzelne Bytes ausgedrückt werden (vgl. Abb. 3.5). Beispielsweise wird das BR Tag durch das Token 5 ersetzt.

```
<?xml version='1.0'?>
    <!DOCTYPE XYZ [
        <!ELEMENT XYZ (CARD)+>
        <!ELEMENT CARD (#PCDATA | BR)*>
        <!ELEMENT BR EMPTY>
        <!ENTITY nbsp ' '>
    ]>
    <XYZ>
        <CARD>
        X &amp; Y<BR/>
            X = 1
        </CARD>
    </XYZ>
```

02	01	03	00	47	46	03	' '	'X'	' '	'&'	' '	'Y'	00	05	03	' '
'X'	00	02	81	20	03	'='	00	02	81	20	03	'1'	' '	00	01	01

Abbildung 3.5: Die Hexadezimaldarstellung eines XML-Dokumentes [6]

Der WAP-Proxy konvertiert das WBXML in die entsprechende Anfrage an den Webserver, der diese dann seinerseits entweder mit einem WML-Dokument dem Proxy direkt beantwortet oder ein HTML-Dokument zu einem Filter sendet. Letzterer wandelt das Dokument um und übergibt es dem WAP-Proxy im WML-Format. Hier wird es wieder in WBXML umgewandelt und an das mobile Gerät versandt.

Beispielanwendung (1)

Die mobile Datenkommunikation und Anbindung an das WWW bietet ein ungeahntes Potential an Anwendungsmöglichkeiten. Von der bereits genannten Verwaltung von Sprachmehrwertdiensten angefangen, über die Bedienung von Getränke- und anderen Automaten an öffentlichen Plätzen und etwa dem Ersatz für Speisekarten in Restaurants bis hin zur Verwaltung von Licht, Jalousien, Garagentoren, Sprinkleranlagen, Mikrowellengeräten, Videorekordern usw. im eigenen Heim von einem beliebigen Ort aus, ist alles vorstellbar. Im Bezug auf das eigene Heim wäre es sicher auch recht angenehm, eine Art Sicherheitsanlage über mobile Datenkommunikation zu steuern und zu überwachen. Vorstellbar wäre hier, die Alarmanlage zu aktivieren bzw. zu deaktivieren, Alarmmeldungen zu empfangen und ihren Status abzufragen.
Mit WAP 1.x wäre dies zunächst rein textbasiert möglich. Der Benutzer wählt sich in das Netz ein, gibt die WAP-Seite seines Alarmanlagenverwaltungsservers ein und hat nun die Möglichkeit, über das Verfolgen von Links und die Auswahl von Optionen die Anlage ein- und abzuschalten, den Status und auch Alarmmeldungen abzufragen. Sollte insbesondere im letzteren Fall ein Alarm vorliegen, kann dieser mitunter schon so alt sein, wie die letzte

Einwahl auf den Server. Bilder, etwa von Überwachungskameras sind nur in so schlechter Qualität übertragbar, daß sie hier nicht sinnvoll nutzbar sind.

3.2.2 WAP 2.x

Das im Jahr 2001 veröffentlichte WAP 2.0 stellt eine grundlegende Änderung des bisherigen Standards dar. So werden beispielsweise IP-Verbindungen unterstützt und auch die Internetprotokolle TCP, TLS und HTTP, wenn auch in einer an WAP angepassten Form. Der Protokollstapel ist nun dem des Internet weitestgehend angepasst (vgl Abb.3.6).

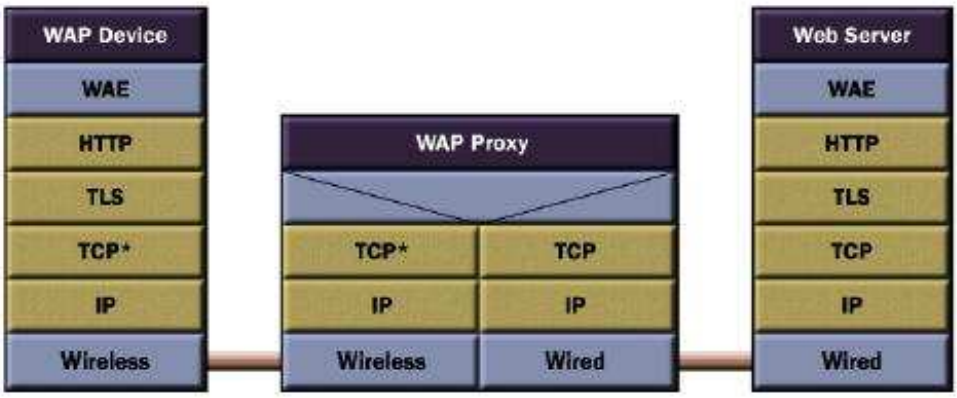

Abbildung 3.6: Der WAP 2.x Protokollstapel [4]

Die Schichten des neuen Stapels:

WP-HTTP Das Wireless Profiled Hypertext Transfer Protocol ist ein an die Bedürfnisse von WAP angepasstes HTTP und HTTP/1.1 kompatibel. Es unterstützt sowohl Kompression als auch Tunneling. Die Interaktion zwischen dem WAP-Gerät und dem Proxy basiert auf Request/Response Interaktionen.

WP-TLS Die Abkürzung steht für Wireless Profiled Transport Layer Security. Auch hier liegt eine an WAP angepasste Form des TLS vor. Die Besonderheit ist hier die Unterstützung von Zertifikaten, verschiedenen Verschlüsselungsverfahren und die Wiederaufnahme von Sitzungen. Es können sogar TLS-basierte Tunnel für gesicherte End-to-End Verbindungen erzeugt werden.

WP-TCP Eine speziell an Funkverbindungen angepasste Version des Transmission Control Protocol, das auch in der Performance verbessert wurde.

Eine weitere Besonderheit ist der Dual Stack: Eine Koexistenz des Wap 1.x und 2.x Protokollstapels im Endgerät, um eine Abwärtskompatibilität zu gewährleisten.

XHTML

Das WAP-Forum hat sich mit der Einführung des WAP 2.0 Standards auf XHTML als Content Authoring Sprache festgelegt. Damit wurde auch entschieden, daß zukünftige Inhalte für WAP-fähige Geräte nicht länger in WML zu formulieren sind.

XHTML stellt eine erweiterte Version von HTML 4.1 dar und enthält deren Gestaltungselemente, unterscheidet sich aber darin, daß es zum einen erweiterbar ist und zum anderen XML-Konform sein muß. Neben der zwingenden Einhaltung von Groß- und Kleinschreibung, können die Elemente auch nicht abgekürzt werden und unterliegen einer strengen Syntax.
Auf den mobilen Endgeräten kommt XHTML Basic zum Einsatz, das fast alle Standardelemente von XHTML beinhaltet. Dies sind beispielsweise einfache Formulare, Textformatierungen, Links, Tabellen, Bilder und Metainformationen. Frames werden ebensowenig unterstützt wie Stylesheets.

PUSH

Die meisten WWW Dienste sind Pull basiert, d.h. der Nutzer fordert Information an. Hier ist ein ständiges Wiederholen der Anfrage notwendig, wenn er immer die aktuellste Version einer Seite haben möchte, die ständigen Wechseln unterliegt, wie etwa bei Schlagzeilen, Wettermeldungen oder Börsendaten.
Beim Pushen hat ein Webserver die Möglichkeit, Daten an den mobilen Empfänger zu schicken, ohne daß diese immer wieder neu angefordert werden. Damit wird auch erreicht, daß die Daten immer dann beim Nutzer aktualisiert werden, wenn sich tatsächlich auch etwas geändert hat. Unnötige Abfragen und eine hohe Netzaktivität sowie auch Kosten werden damit vermieden.

GPRS

Mit WAP 2.0 ist es nun auch möglich, über die IP-Verbindung paketorientierte Dienste zu nutzen. Der General Packet Radio Service (GPRS) bietet das passende Netz dazu. Trotz der nach wie vor geringen Datenrate von etwa 53 kBit/s, je nach Anbieter und Netzauslastung, sind die Wartezeiten für ein Seitenaufbau vergleichbar mit denen am PC.
Die Angewählten Seiten erscheinen damit wesentlich schneller als beim verbindungsorientierten GSM, zudem entfällt das dauernde Einwählen in das Netz, da das Endgerät mit GPRS im Grunde immer online ist.

Beispielanwednung (2)

Zurück zu der Steuerung der Alarmanlage. Mit WAP 2.0 ist nun auch eine gesicherte TLS Verbindung zum Alarmanlagenserver möglich, sowie die Übertragung von Bildern der Überwachungskameras in guter Qualität. Beschränkt wird letzteres nur noch durch das Display und den Speicher des Endgerätes. Mit GPRS als Bearer ist es vor allem aber auch möglich, einen Alarm unmittelbar zu empfangen. Ohne GPRS geht dies hier zwar auch, ist aber kostspielig, weil das Endgerät ständig eingewählt sein muß.

3.3 iMode

Im Februar 1999 wurde dieser Dienst in Japan von dem Telekommunikationsunternehmen NTT DoCoMo (die Abkürzung steht für 'Nippon Telephone and Telegraph Cooperation Mobile Communication Network') eingeführt. Während WAP ursprünglich eher schlicht und nüchtern für Geschäftsanwendungen konzipiert war, zielte iMode auf Unterhaltung ab. Es war von Begin an auch wesentlich stärker an das Internet angelehnt, wurde paketvermittelt angeboten und erlaubte damit eine Abrechnung nach der übertragenen Datenmenge. Hierzulande wird iMode schon als UMTS im Kleinformat bezeichnet ([12]).

Architektur

Die im Protokollstapel von iMode verwandten Protokolle (vgl Abb. 3.7) gleichen prinzipiell denen des Internet. Es wurden lediglich Anpassungen an die besonderen Umstände der mobilen Datenübertragung vorgenommen.

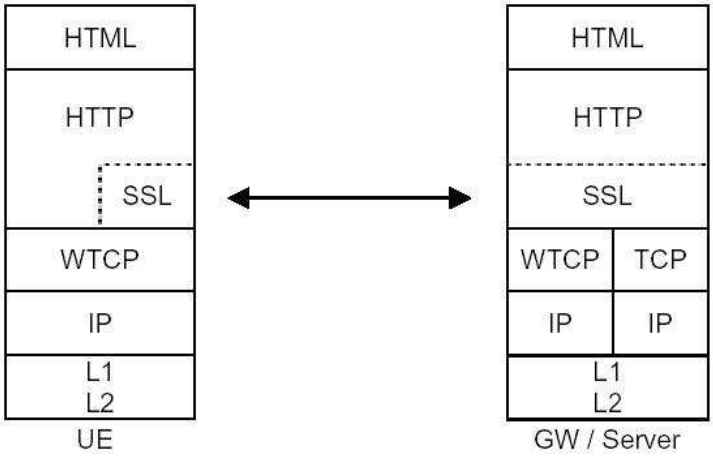

Abbildung 3.7: Der iMode Protokollstapel [8]

iHTML

iMode compatible HTML (iHTML) basiert auf dem von W3C spezifizierten compact HTML (cHTML), das wieder eine Untermenge von HTML darstellt.
Es wird zwischen den Entwicklungs- bzw. Gerätestufen 1.0, 2.0 und 3.0 unterschieden, die sich nach unten jeweils durch zusätzliche Tags abgrenzen. cHTML 1.0 ist auf allen iMode-fähigen Geräten, die immerhin auch Autonavigationsgeräte umfassen, einsetzbar. Die Version 2.0 beinhaltet zusätzlich die Tags MARQUEE (Scrollbarer Text), BLINK (Blinkender Text), SELECTOPTION (Option), BODY (Textkörper) und FONT um Displayeigenschaften zu verändern, sowie istyle, um den Eingabemodus zu bestimmen. Die Erweiterung der Version 3.0 umfasst Java-Tags, ID-Feststellung, Mailtags, sowie Telefonbuchregistrierung.

cHTML unterstützt keine Frames und auch keine Tabellen. Bilder werden nur im GIF Format unterstützt. Weiter kann Java-Script genutzt werden. iHTML ist durch die Ähnlichkeit der beiden Protokollstapel auch WAP 2.0 kompatibel.
cHTML bietet ausserdem noch die drei Dienste *mail to*, *phone to* und *web to*. Damit kann der Benutzer sich durch einen Tastendruck unmittelbar mit einer Telefonnummer oder Webseite verbinden oder eine Mail schreiben.

Java

iMode unterstützt die 'Connected Limited Device Configuration' (CLDC) der Java2 Platform Micro Edition (J2ME). Dies ist eine Minimalanforderung an die Klassenbibliotheken kleiner, netzwerkfähiger Endgeräte, um noch den Java virtual machine specifications zu genügen. Dabei steht vor allem die K Virtual Machine im Vordergrund, auf der CLDC basiert. Die KVM ist eine äusserst portable JVM, die besonders an Geräte mit geringer CPU-Leistung, Speicherkapazität und Akkulaufzeit angepasst ist.
Der von NTT DoCoMo hervorgehobene Vorteil von Java Applikationen ist eben die Portabilität, also die Möglichkeit, eine Vielzahl unterschiedlicher Geräte mit einer einzigen Version einer Applikation bedienen zu können. Neben der Anwendungsumgebung für Java bietet iMode noch das dynamische Erweitern der Programme und Inhalte auf einem Gerät, sowie den Java Application Manager (JAM) und Sicherheitseinrichtungen, wie etwa das 'simple sandbox model', bei dem nur eine Grundausstattung an nicht sicherheitsgefährdender Java-Klassen ausgeführt werden dürfen.

Die NTT DoCoMo iMode Netzstruktur

Herzstück des NTT DoCoMo iMode Netzwerkes ist das DoCoMo iMode Center (vgl Abb.3.8). An diesem müssen sich alle offiziellen Contentanbieter (iMode information service providers) anmelden, um im iMode Netz auch verfügbar sein zu können. Derzeit sind dies laut NTT DoCoMo etwa 3500 [9]. Zudem laufen die Verbindungen zu Banken über spezielle, von den Banken mietbare Leitungen. Der iMode-Nutzer kann aber auch iMode kompatible Internetseiten direkt nutzen. Bei NTT DoCoMo wird die Zahl dieser Seiten auf etwa 66500 geschätzt.

NTT DoCoMo Services

Die Angebotspalette von NTT DoCoMo scheint geradezu zu explodieren. Dabei wird sie nur den immensen Kundenzahlen gerecht, die in den letzten drei Jahren von 30 Mio. auf über 36 Mio gestiegen sind [10].
Die vier wichtigsten Servicebereiche sind i-@ppli, i-area. i-motion und i-shot.

i-@ppli Mit diesem Service kann der Nutzer Java Applikationen herunterladen und diese im weiteren Verlauf ständig nutzen, ohne weitere Kosten zu verursachen. Die von NTT DoCoMo hervorgehobenen Vorteile des Services sind die multimedialen Fähigkeiten der Anwendungen in Bild, Text und Ton.

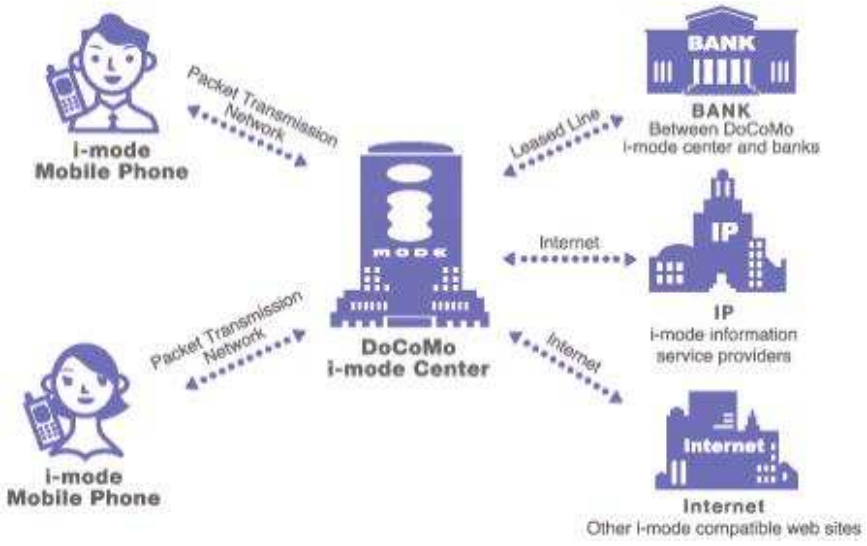

Abbildung 3.8: Die iMode Netzstruktur von NTT DoCoMo [11]

i-area Der Service ist dem Namen nach ein regionaler Service. Dabei ist das Japan in 482 verschiedene Regionen unterteilt, für die der Nutzer Kartenmaterial erhalten kann, Informationen über Hotels und Gastronomie, sowie Veranstaltungstipps und aktuelle Wetterinformationen

i-motion Bewegte Bilder auf dem Display des Endgerätes bietet dieser Service, darunter Torszenen und andere Highlights aus dem aktuellen Sportgeschehen, Nachrichten, Musikclips und Werbung. Die Länge der Videoclips und Musikstücke ist jedoch auf etwa 40 bis 100 Sekunden begrenzt.

i-shot Dieser Service ist mit MMS vergleichbar. Er bietet die Möglichkeit, mit mobilen Kameras aufgenommene Bilder über das Netzwerk entweder an andere Endgeräte oder als Anhang einer E-Mail zu verschicken

Weitere Angebote sind etwa

- **Cmode**, mit dem sich über das Endgerät Getränke- und Fahrkartenautomaten steuern lassen
- **Mobil GEO**, ein bargeldloses Zahlungssystem
- **Melo-Dam**, mit dem sich in Japan sehr beliebte Karaoke Geräte bedienen lassen
- **VF.NET**, mit dem der Nutzer in Spielhallen Automaten füttern kann
- **PlayStation**, durch das das Endgerät entweder zum Controller einer solchen wird, zur Playstation selbst, indem die heruntergeladenen Spiele auf dem Fernseher spielbar werden oder als Verbindungsstück zu einem Mehrspielernetzwerk
- **AOLi**, welches das Endgerät mit AOL verbindet
- **i-navi link**, durch den das Handy zum Navigationssystem avanciert
- **iLawson**, mit dem sich Rabatt-Coupons sammeln lassen

Daneben gibt es noch eine Reihe Handels- und Geschäftssyteme, die hier aber nicht näher beschrieben werden.

Beispielanwendung (3)

Nachdem das WAP-Forum versucht hat, mit WAP 2.x die Qualitäten von iMode zu erreichen, kann mit der alleingen Nutzung von iHTML nicht viel an der Anwendung verbessert werden. Mit der Javaunterstützung kann diese jedoch plattformübergreifend und umfassend neu gestaltet werden, sowohl in ihren Funktionen als auch in ihrem Erscheinungsbild. So könnte durch multimediale Unterstützung wie etwa Videostreams oder Ton die Kontrollmöglichkeit durch den Nutzer verbessert und über Scriptsprache noch die Möglichkeit geschaffen werden, automatisch die Polizei, oder bei einem Brand die Feuerwehr zu alamieren, Nachbarn automatisch anzurufen oder einfach das Licht im gesamten Haus samt der Stereoanlage einzuschalten, um etwaige Eindringlinge abzuschrecken.

3.4 Vergleich von WAP und iMode

An dieser Stelle ist allenfalls ein Vergleich zwischen dem älteren WAP 1.x und iMode möglich, der aber in den Unterschieden im Großen und Ganzen die Weiterentwicklung zu WAP 2.x umfasst und damit im Grunde hinfällig geworden ist.
Es muß an dieser Stelle auch immer vorausgeschickt werden, ob nun der Protokollstapel der beiden Techniken verglichen wird oder die Dienste, die auf diesen Techniken basieren. iMode hat vor allem in letzterem Punkt einen hohen Vorsprung, da die Anbieter in Japan über eine wesentlich höhere Abnehmerzahl verfügen und damit wesentlich näher am Bedarf der Kunden operieren können, während der Bedarf in Europa durch die erste WAP Generation abgeschreckt und durch die neue Generation noch nicht neu geweckt werden konnte. Die Protokollstapel von iMode und WAP 2.x unterscheiden sich in ihren Schichten nicht mehr, im Gegenteil, sie sind mitunter sogar kompatibel zueinander.
Einzig im Bearer und der Scriptfähigkeit lassen sich Unterschiede feststellen: Während WAP 2.x auch noch verbindungsorientiert arbeiten kann und Java-Script nicht unterstützt, ist iMode der etabliertere Standard, der, wie bereits erwähnt, über wesentlich mehr Anwendungen verfügt als WAP und vor allem Java-fähig ist.
WAP wird es sicher auch schwer haben, der Einführung von iMode in Europa stand halten zu können, denn die negativen Erfahrungen der WAP-Anfänge sitzen noch tief. Aber auch iMode läuft Gefahr, in die Mißgunst der Kunden zu geraten: Es herrscht nämlich noch eine eher undurchsichtigen Preispolitik (vgl. [12]). Zwar bietet gerade ein paketorientierter Dienst wie GPRS die Möglichkeit, Preise nach der übertragenen Datenmenge 'gerecht' zu erheben, doch wird dies beispielsweise von dem Anbieter E-Plus als auch von den Content-Anbietern wie etwa Spiegel.de nicht unbeding zum Vorteil der Kunden umgesetzt (vgl. 3.2. Neben dem recht hohen Preis für ein iMode-fähiges Handy verlangt der Netzanbieter zunächst eine zusätzliche Grundgebühr von 5,- Euro für iMode (iMode Datenpaket S). Hier kommen seitens der meisten Content-Anbieter nochmal zwischen 0,25 und 2,- Euro monatliche Grundgebühr hinzu, sowie seit Juni diesen Jahres 1Cent pro übertragenem KByte, was bei einem Klingelton von 12 KByte oder einem kleineren GIF-Bild von 3KByte den Preis recht schnell in die Höhe treiben kann. Eine i-Mail von bis zu 1000 Zeichen kostet bei E-Plus ebenfalls eine Grundgebühr von 19 Cent pro Mail plus übertragene Datenmenge. Im Vergleich dazu verlang NTT DoCoMo von seinen Kunden 300 JPY, also umgerechnet etwa 2,20 Euro Grundgebühr (vgl. [11]). Das übertragene

Paket kostet 0.3 JPY, was etwa 0.2 Eurocent entspricht. 400 Pakete sind dabei frei, wobei das in etwa 100 Emails mit 50 gesendeten oder 100 empfangenen Zeichen wären. Das Unternehemn bemüht sich ebenfalls auf seiner Seite, die Preise so transparent wie möglich zu halten und gibt sogar an, welche Menüaktionen in etwa welche Kosten verursachen.

	E-Plus	**NTT DoCoMo**
Grundgebühr Telefon	10,21 Euro / Monat	etwa 24 Euro
Grundgebühr iMode	5 Euro / Monat	etwa 1,10 Euro
content Abo	0,25 - 2,- Euro / Monat	meist Kostenfrei
iMode-Mail	0,19 Euro	keine
Datentransfer	1 EuroCent / KByte	0,2 EuroCent / Paket

Tabelle 3.2: Gebührenvergleich zwischen WAP und iMode [11], [13]

3.5 Schluß

An einem beliebigen Ort über eine Verbindung ins Internet zu verfügen, E-Mails schreiben und empfangen, Bilder austauschen, kleine Videos ansehen und beliebig Musikstücke herunterladen zu können, Automaten und mit dem Internet verbundene kleine Helfer fernzusteuern, den eigenen Standort feststellen und sich selbst von anderen finden zu lassen, Veranstaltungskalender beziehen und Fahrten mit öffentlichen Verkehrsmitteln über die Telefonrechnung bezahlen, all das ist längst nicht mehr nur Zukunftsmusik, sondern schon im Anfangsstadium. Es muß noch viel getestet werden, viele neue Standards müssen geschaffen und alte angepasst werden und die beteiligten Entwickler müssen strengstens vermeiden, das Rad neu zu erfinden.

WAP und iMode sind dabei in Japan und Europa die Grundsteine für die schöne neue Mobilfunkwelt. Von ihrem Erfolg hängt es aber vor allem ab, ob das eifrige Steigern um die UMTS-Frequenzen in Deutschland eine kluge Investition in eine Technologie der Zukunft war oder die vermeintlich erfolgreichen Unternehmen im Nachhinein noch in den Ruin treiben wird.

Mit der Version 2.0 hat das WAP-Forum eindeutig versucht, mit iMode gleich zu ziehen. Sowohl die Einbindungsmöglichkeit von Grafikobjekten und die Erweiterung der Textgestaltungsmöglichkeiten als auch die Unterstützung paketorientierter Übertragungsdienste bis hin zur Neugestaltung des Protokollstapels sollten WAP den gleichen Schub geben, den iMode dank dieser technologischen Grundlage in Japan hatte. Dies ist vor allem verständlich und war auch nötig, insbesondere wegen der Eigenschaft von WAP und iMode in Europa als Testballone für UMTS zu fungieren. Erreichen beide (wieder) nicht die gewünschte Akzeptanz beim Endkunden, wird es die neue Generation der mobilen Datenübertragung um so schwerer haben, sich zu etablieren und damit würde Europa wohl mehr auf dem Stand bleiben, das Handy nur zum Telefonieren und Kurznachrichten Verschicken zu nutzen.

Mit WAP und iMode stehen wir also an der Schwelle zur mobilen Datenkommunikation von Morgen. Die inzwischen recht enge Zusammenarbeit von WAP-Forum und NTT DoCoMo, die sogar hin zur Kompatibilität von beiden Diensten führen soll, machen es eher schwierig, sie gegeneinander aufzuwiegen und von 'WAP vs. iMode' zu sprechen. Vielmehr ist zu erwarten, daß beide miteinander verschmelzen werden, um so gemeinsam das Testfeld für und den Vorgeschmack auf UMTS zu bieten.

Literaturverzeichnis

[1] http://www.wirelessdevnet.com/channels/wap/training/wml.html, *The Wireless Markup Language (WML)*, Ein Tutorial

[2] http://www.iicm.edu/wrichter/thesis-final/, Wolfgang Richter: *Virtual Communities und Customer Relationship*, Diplomarbeit an der TU Graz

[3] Sven Thoenissen: *Das WAP-Protokoll: Aufbau, Anwendung und Infrastruktur*, Vortragsfolien zum Mobile Commerce am 19.06.2000

[4] PD Dr. Thomas Myrach: *Mobile Computing*, Vorlesungsfolien, RWTH AACHEN SS2002

[5] http://www.gingco.de/wap/ Software zur Umwandlung von .jpg zu .wbmp

[6] www.wapforum.org/ *WAP Binary XML Content Format Specification* Version 1.2 1999

[7] Christian Berger, Henry Trommer, Thomas Trommer: *Smartphones & Handys*, Dokumentation des Proseminars IBM-PC an der TU Chemnitz SS2001

[8] http://www.nttdocomo.com Eingangsseite von NTT DoCoMo

[9] http://www.nttdocomo.com/current_information/subscriber_growth.html iMode Statistiken von NTT DoCoMo

[10] http://www.nttdocomo.com/i-mode/evolution/index.html iMode Kundenzahlen von NTT DoCoMo

[11] http://www.nttdocomo.co.jp/english/p_s/imode/ Information rund um iMode von NTT DoCoMo

[12] http://www.tecchannel.de/internet/887/index.html Infoseite über iMode

[13] http://www.umts-report.com/index.php4?seite=i-mode-preise Preisübersicht für iMode bei E-Plus