Zusammenfassung 1679 – Mobile Computing

KE 1

1 Einleitung

- Was versteht man unter der Forschungsrichtung Mobile Computing?
- Umgang mit verschiedenen Begriffen im Umfeld

1.1 Forschungsrichtung Mobile Computing

Die Forschungsrichtung Mobile Computing befasst sich mit der Kommunikation von mobilen Benutzern (Mobilkommunikation), mit mobilen Endgeräten und den dazugehörigen Anwendungen.

1.2 Begriffe

1.2.1 Aus Benutzersicht

1.2.1.1 Allgegenwärtige Computer – Ubiquitous Computing

Drei Phasen:
1. Mainframes,
2. Personal Computer,
3. Ubiquitous Computing.

Mit fortschreitender Miniaturisierung kleine, weltweit vernetzte Systeme, die überall verfügbar sind und nicht mehr die volle Aufmerksamkeit des Benutzers beanspruchen. (Pervasive-, calm-, invisible-, disappearing Computing)

1.2.1.2 Nomadic Computing

Stärkere Schwerpunkt auf der Mobilität des Anwenders. ⇔ Mobile Computing behandelt auch Probleme am Zielort.

1.2.1.3 Personal Computing

Die Mobilen Geräte enthalten mehr persönliche Informationen und werden daher als persönlich betrachtet.

1.2.1.4 Tragbare Computer (Handheld-, Palm-, Wearable Computing; Augmented Reality)

Untersuchung der physischen Mobilität der Geräte, je nach Anwendungsform.

1.2.2 Aus Sicht der Netzwerke

1.2.2.1 Ad-hoc-Vernetzung und mobile Vernetzung

Kurzfristige Vernetzung von Geräten ohne aufwändige Konfiguration, vorwiegend die Vernetzung von mobilen Geräten untereinander.

1.2.2.2 Mobile Vernetzung – Mobile Networking

Vernetzung mobiler Rechner mit einem stationären Netzwerk.

1.2.2.3 Embedded Nedtworking

Vernetzung von Geräten der Haushalts-, Unterhaltungs- und Konsumelektronik, die von Embedded Systems gesteuert werden.

1.2.2.4 Mobilkommunikation ⇔ drahtlose Kommunikation

Betrachtung der reinen Kommunikation. Drahtlos heißt nur drahtlos und kann mobil oder stationär sein

1.2.3 Arten der Mobilität

1.2.3.1 Endgerätemobilität

Ein Endgerät bleibt vernetzt, obwohl es bewegt wird.

1.2.3.2 Benutzermobilität

Ein Benutzer kann beliebige Geräte verwenden, um Dienste zu nutzen, hierzu muss er sich identifizieren.

1.2.3.3 Dienstmobilität

Ein Benutzer kann von jedem Ort auf dieselben Dienste zugreifen.

1.3 Beispiele

1.3.1 M-Commerce

Sicherer An- und Verkauf mittels drahtloser Technologie.

1.3.1.1 Business to Consumer

- Mobile Banking
- Mobile Brokering
- Mobile Payment (Mikro/Makro)
- Mobile Shopping
- Ticketbestellung
- Unterhaltung

1.3.1.2 Business to Business

- Beschaffungswesen
- Vertrieb
- Service, technischer Kundendienst, Fertigung, Produktion, Montage
- Logistik

1.3.1.3 HP-CoolTown

Beispielinfrastrukur zur Übertragung von Infos über das WWW. Museum mit Führung und Konferenzraum.

2 Grundlagen der drahtlosen Kommunikation

- OSI-Referenzmodell erläutern
- Unterschiede zwischen drahtloser und drahtgebundener Kommunikation erläutern
- Verfahren zur Mehrfachausnutzung von Funkressourcen nennen

2.1 Das OSI-Referenzmodell

Schicht	**Übertragung von**	**Erläuterung**
1 Bitübertragungsschicht Physical Layer	Bits	Festlegung von mechanischen, elektrischen und elektromagnetischen Eigenschaften der Übermittlung
2 Sicherungsschicht Data Link Layer	Frames	Gesicherte Übertragung durch Redundanz durch CRC, ARQ oder Forward Error Correction
3 Vermittlungsschicht Network Layer	Pakete	Kommunikation zwischen nicht direkt verbundenen Rechnern über Routing-Verfahren
4 Transportschicht Transport Layer	Nachrichten	Entkopplung der höheren Schichten von der Kommunikation, auf Wunsch zuverlässige Übertragung.
5 Kommunikationsst. Session Layer	transparent	Synchronisation und Flussteuerung, Verwaltung logischer Verbindungen
6 Darstellungsschicht Presentation Layer	transparent	Einheitliche Darstellung der Übertragungsdaten
7 Anwendungsschicht Application Layer	transparent	Kommunikation zwischen Anwendern

IEEE 802 beschreibt die untersten beiden Schichten (Physical Layer und Data Link Layer, lezteres aus Media Access Control und Logical Link Control bestehend). TCP/IP faßt die unteren beiden Schichten zusammen, die dritte und vierte entsprechen dem OSI-Modell und die obersten drei werden wieder zusammengefasst:

2.2 Vergleich der Schichten verschiedener Modelle

OSI	**TCP/IP**	**Drahtlose Kommunikation**	**IEEE 802**
1 Bitübertragungsschicht Physical Layer	Netzwerkschicht	Bitübertragungsschicht und Sicherungsschicht: Bit- und Frameübertragung	Phy
2 Sicherungsschicht Data Link Layer		Mehrfachzugriff Sicherheit	MAC LLC
3 Vermittlungsschicht Network Layer	Internetschicht: (IP, ICMP, ARP, Multicast IP, Mobile IP)	Vermittlungsschicht: Handover & Roaming, Ad-hoc-Routing, Geografische Adressierung	
4 Transportschicht Transport Layer	Transportschicht: (TCP, UDP)	Transportschicht: Flusskontrolle, Dienstgüte	
5 Kommunikationsst. Session Layer	Anwendungsschicht: (FTP, HTTP, SMPT, Telnet, NNTP, DNS, DHCP)	Anwendungsschicht: Übertragung von Daten, Dienstvermittlung, Berücksichti-	

		gung der Endgeräte	
6 Darstellungs-schicht Presentation Layer			
7 Anwendungs-schicht Application Layer			

2.3 Besonderheiten der drahtlosen Kommunikation

2.3.1 Kategorien

Mobiltelefonie (GSM, UMTS), Drahtlose lokale Netze (WLAN, HIPERLAN, Wireless ATM, Home RF), Wireless personal Area Networks (WPAN: Bluetooth, IrDA), Satellitennetze, Rrichtfunk, Wireless local loop, Rundfunk, Bündel- und Betriebsfunk

2.3.2 Probleme

2.3.2.1 Sicherungsschicht und Bitübertragungsschicht

Anforderungen der Luftschnittstelle: Bitübertragung und Mehrfachzugriff.
Randbedingungen der drahtlosen Kommunikation in der Bitübertragungsschicht

- Störanfälligkeit
- Niedrigere Datenraten
- Abhörmöglichkeit
- Hoheitliche Restriktionen

2.3.2.2 Vermittlungsschicht

Behandelt die räumliche Mobilität, Handover, Roaming.

2.3.2.3 Transportschicht

Anpassung der existierenden Protokolle an die Besonderheiten der Luftschnittstelle, z. B. Fehlerkorrekturverfahren von den Gegebenheiten des Internet auf die drahtlose Umgebung anpassen.

2.3.2.4 Anwendungsschicht

- Dienstvermittlung in mobilen Umgebungen, d. h. insbesondere deren automatische Nutzung
- Datenübertragung zwischen heterogenen Systemen
- Berücksichtigung der eingeschränkten Fähigkeiten der Endgeräte.

2.4 Multiplexverfahren – Mehrfachausnutzung von Funkressourcen

Generell wird zwischen Duplex (bidirektionale Verbindung) und Multiple Access (Mehrfachausnutzung) unterschieden

2.4.1 Raummultiplex

Ausnutzung der beschränkten Ausbreitung elektromagnetischer Wellen durch Zellenbildung bzw. Richtantennen.

2.4.2 Frequenzmultiplex

Aufteilung des zur Verfügung stehenden Spektrums auf Kanäle.

2.4.3 Zeitmultiplex

Das zur Verfügung stehende Funkmedium wird jeweils nur für eine bestimmte Zeit verwendet.

2.4.4 Codemultiplex

Mehrfache Ausnutzung des Funkkanals durch Verwendung verschiedener Spreizcodes.

3 Mobiltelefonie

- Mobilfunkgenerationen
- Grundlagen der Mobiltelefonie auf Basis zellularer Netze
- Architektur und Eigenschaften von GSM-Netzen
- UMTS und DECT

3.1 Mobilfunkgenerationen mit Eigenschaften

Generation	**Betreiber**	**Netz**	**Zeitraum**	**Eigenschaften**	**Frequenzbereich**	**Nutzer (Jahr)**
Erste (analog)	Bundespost	A	1958-1977	Analog, handvermittelt	150 MHz	10000 (1970)
	Bundespost	B	1972-1994	Analog, Selbstwahl	150 MHz	27000 (1986)
	Bundespost	C	1986-2001	Analog, zellular	450 MHz	800000 (1992)
Zweite	Telekom	D1	Ab 1992	Digital GSM 900	900 MHz	13 Mio (2000)
	Vodafone	D2	Ab 1992			19 Mio (2000)
	E-Plus	E1	Ab 1994	Digital, DCS 1800	1800 MHz	5,8 Mio (2000)
	O2	E2	Ab 1998			3,2 Mio (2000)
Dritte	Verschiedene	UMTS	Ab 2004?	Digital UMTS	1900 MHz	?

3.2 Grundlagen zellularer Mobilfunknetze

3.2.1 Konzept

Ein Mobilfunknetz soll eine Fläche vollständig abdecken. In de Realität schwächt sich die Sendeleistung mit der vierten Potenz des Abstands, eine Isolation von Kanälen ist nicht möglich.
Daher wurde das Konzept zellularer Netze entwickelt: Abdeckung der Fläche durch ein Netz von Basisstationen, die jeweils einen näherungsweise kugelförmigen Bereich versorgen => **Zellen**

3.2.2 Vorteile von Zellen

- Geringe Distanz zwischen mobilem Gerät und Basisstation

- Ökonomische Nutzung der Frequenzen und Zeitschlitze

3.2.3 Nachteile von Zellen

- Es müssen sehr viele Basistationen betrieben werden.

3.2.4 Anordnung der Zellen in Clustern

Man ordnet die Zellen in Clusytern an, die die Parkettierung der Ebene erlauben. Relevante Größen sind

- k – die Anzahl an Zellen pro Cluster
- D – der Abstand zwischen zwei Zellen gleicher Frequenz und
- R – der Zellradius.

Es gilt:
D = RWurzel aus 3k

3.3 Architektur und Eigenschaften von GSM-Netzen

Ein GSM-Netz besteht aus Betriebssubsystem, Vermittlungssubsystem, Funksubsystem sowie den mobilen Endgeräten.

3.3.1 Das Funksubsystem – Base Station Subsystem (BSS)

Die Kommunikation zwischen Mobilgerät und Basisstation erfolgt über Base Tranceiver Stations/BTS) , deren jede eine Zelle versorgt. Sie bestehen aus Sende- und Empfangssystem, die eigentliche Weiterverarbeitung wird durch Base Station Controller (BSC) durchgeführt; jeder versorgt mehrere BTS, über sie wird auch der Handover abgewickelt. Nach der Luftschnittstelle zwischen mobilem Endgerät und BTS wird der Rest leitungsgebunden abgewickelt.

3.3.2 Das Vermittlungssubsystem – Mobile Switching and Management Subsystem (SMSS)

Der Kern sind Mobile Switching Center (MSC), die jeweils eine Service Area abdecken. Sie wickeln den Verkehr zwischen BSCs ab und führen das Roaming durch. Sie lokalisieren die Benutzer und bedienen sich des Home Location Register (HLR) und des Visitors Location (VLR) Register. Pro Netzwerk gibt es ein HLR und pro MSC ein VLR.

- Das HLR speichert die relevanten Daten eines Nutzers einschließlich des aktuellen Aufenthaltsorts.
- Das VLR speichert Daten der Nutzer, die sich gerade im Einzugsbereich eines MSC befinden. Nach Verlassen werden sie gelöscht.

3.3.3 Das Betriebssubsystem – Operatikon and Maintenance Subsystem (OMSS)

Das Betriebssubsystem kontrolliert und wartet das Netzwerk:

- Verwaltung geschäftsrelevanter Daten wie Kundendaten, Endgeräte, Gebührenabrechnung, Statistiken
- Sicherheitsmanagement
- Konfiguration
- Das Authentication Center speichert vertrauliche Daten des Kunden und Schlüssel
- Das Equipment Identity Register speichert die Sereinnummern der Endgeräte z. B. zum Sperren

3.3.4 Die Endgeräte – Mobile Stations (MS)

Autotelelefone mit 20W
Tragbare Geräte mit 8W
Handgeräte mit 5W
Handgeräte mit 2W

3.3.5 Die Adressierung von Benutzern und Geräten

3.3.5.1 Benutzer über die SIM-Karte (Subscriber Identity Module)

- Geheimnummer
- Daten der persönlichen Konfiguration (Tel-Nr....)
- Nicht gelöschte SMS
- Technische Daten des Mobilfunkbetreibers
- Eine weltweit eindeutige Benutzernummer (International Mobile Subscriber Identity - IMSI)
- TMSI – Temporary Mobile Subscriber Identity – wird zum Schutz der Identität des Teilnehmers zeitweise vergeben und zur Identifizierung benutzt, wird periodisch geändert.

3.3.5.2 Geräte über die IMEI

Die International Mobile Station Equipment Identity wird bei der Herstellung des Mobiltelefons fest vergeben

3.3.5.3 Weitere Nummern

- MSISDN – Telefonnummer des Anschlusses
- MSRN – Temporäre Nummer, wenn man in einem fremden Netz ist
- LAI – Location Area Identity, CI – Cell Identityfier – Dient zur weltweit eindeutigen Kennzeichnung von Funkzellen.

3.3.6 Die Luftschnittstelle

Es werden Raum-, Zeit- und Frequenzmultiplex verwendet: Zellulares Netz, 124 Kanäle (124 für jede ‚Richtung) und 8 Zeitschlitze à 0,577ms.im D-Netz, 372 Kanäle im E-Netz, 7 Zellen pro Cluster.
Gesendet wird in Bursts:

- Normale
- Zur Frequenzkorrektur
- Dummy
- Zugriffsbursts

=>13000 Bit/s für Daten und 9600 Bit/s für Sprache.

3.3.7 Handover & Roaming

Intra-/Intercell
Internes-/Externes
Der MSC, der die Kontrolle über eine Verbindung hat, behält sie auch nach dem Handover und erweitert die Verbindung logisch zu dem MSC, in dessen Verwaltgungsb ereich der Teilnehmer ist.
Roaming heißt die Nutzung fremder Netze.

3.3.8 Weiterentwicklungen

3.3.8.1 High Speed Circuit Switched Devices - HSCD

Höhere Datenraten durch bessere Kodierung und Bündelung von Frequenzen. Bis 57,6 kBit/s, verbindungsorientiert, geringe Änderungen an der Infrastruktur.

3.3.8.2 General Packet Radio Service - GRPS

Packetvermittelt, Abrechnung nach Datenaufkommen, erhebliche Änderungen an der Infrastruktur. Höhere Datenrate durch Bündelung. Unterscheidung der Geräteklassen nach Anzahl der belegbaren Kanäle in Up- und Downrichtung. Bis 53,5 kBit down und 26,8 kBit/s up bei der höchsten Slotklasse.

3.3.8.3 Enhanced Data Rates for GSM-Evolution - EDGE

Bündelung und neue Modulation; bis 59,2 kBit/s **pro Kanal**. Bis 8 Kanäle gebündelt. Umfangreiche Modifikationen notwendig.

3.4 Universal Mobile Telecommunications System – UMTS

3.4.1 Anforderungen

- Zugang über Schnurlos-Technologie, zellularen Mobilfunk oder Satellit.
- Sprach- und Datenübertragung bis 2 Mbit/s
- Dienstgüte-Eigenschaften, Paket- und leitungsvermittelte Übertragung
- Zugang zu anderen Netzen (ISDN, TCP/IP)
- Virtual Home Environments, d. h. immer dieselben Dikensgte.
- Roaming und Handover auch ins GSM-Netz

3.4.1.1 Anwendungen

- Internet
- Unterhaltung
- Ortsbasierte Dienste
- Finanzdienste
- Kommunikation

3.4.1.2 Zellarten

Name	**Größe**	**Maximale Datenrate**
Pikozellen	50m	2 Mbit/s
Mikrozellen	Einige km	384 kBit/s
Makrozellen	Einige 10 km	144 kBit/s
Noch größere Zellen über Satellit	?	144-384 kBit/s

3.4.2 Die Funkschnittstelle

UTRA-FDD oder UTRA-TDD.

3.4.3 Dienstgüteklassen

3.4.3.1 Klasse	**Charakteristik**	**Beispiele**
Conversational	Niedrige zeitliche Varianz, niedrige Verzögerung	Telefonie, Videokonferen-zen

Streaming	Niedrige Zeitliche Varianz	Video, Audio
Interactive	Request-Response-Paradigma, Niedrige Verzögerung, Gewährleistung der Integrität	WWW, Datenbanken
Background	Keine zeitlichen Garantient, Gewährleistung der Integrität	Download, E-Mail

3.4.4 Architektur

3.4.4.1 User Equipment Domain

User Services Identity Module (Identifikation auch bei Nutzung verschiedener Endgeräte) und Mobile Equipment.

3.4.4.2 Access Network

Zugang zum Netzwerk, z. B. Funk mit UTRAN

3.4.4.3 Core Network

- Serving Network Domain für ortsabhängige Funktionen, paket- und leitungsvermittelte Übertragung.
- Home Network Domain für ortsunabhängige Dienste, z. B. von Service Providern
- Transit Network Domain für Kommunikation mit anderen Netzwerken.

3.5 DECT

3.5.1 Architektur

Fixed Radio Termination und Portable Radio Termination, Reichweite 50-300m. 1880-1920 MHz mit 10 Kanälen, TDMA mit 24 Kanälen pro Frequenzkanal, d. h 120 Vollduplex-Kanäle.

KE 2

4 Drahtlose lokale Netze

- Vor- und Nachteile drahtloser lokaler Netze nennen
- Die wichtigsten Anwendungsgebiete nennen
- Einen Überblick über Standards zu drahtlosen lokalen Netzen geben
- Wissen, wie die jeweiligen Standards die Eigenschaften der Funkkommunikation berücksichtigen
- Den Standard IEEE 802.11 beschreiben

4.1 Vor- und Nachteile drahtloser lokaler Netze

4.1.1 Vorteile

Es gibt keine Kabel, daher

- Keine Kosten für ihre Verlegung
- Die Verkabelung muß nicht schon bei der Planung von Gebäuden berücksichtigt werden
- Man kann auch Gebäude vernetzen die nicht verkabelt werden dürfen oder können
- Der Netzwerkzugang kann über die Grenzen des Gebäudes hinaus ausgedehnt werden
- Keine herumliegenden Kabel, über die man stolpern kann
- Der Aufbau geht schneller (Messe, Katastrophengebiet)
- In Krankenhäusern können Geräte verschoben werden, die vernetzt sind
- Ebenso in Produktionsbereichen

4.1.2 Nachteile

- Drahtlose Netze haben eine um Größenordnungen geringere Bandbreite und eine signifikant höhere Fehlerrate.
- Es sind ggf. natikonale Restriktionen beim Funken zu beachten
- Funksignale sind leicht abhörbar und ausstrahlbar. Authentizität, Vertraulichkeit und Integrität muss über andere Maßnahmen sichergestellt werden, namentlich Verschlüsselung.
- Die Hardware für Funknetze ist wesentlich teurer als die für Drahtnetze.
- Das Funken geht auf die Batterie
- Die Abstrahlung von Funksignalen kann andere Systeme stören und eventuell den Menschen beeinflussen.

4.2 Der Standard IEEE 802.11 – Wireless LAN (WLAN)

Der WLAN-Standard 802.11 wurde seit 1997 definiert. 802.11 bis 2 Mbit/s, 802.11a bis 54, 802.11b bis 11.

4.2.1 Die Struktur

Sicherungsschicht (Data LinkLayer) LLC	802.2 Logical Link Control
MAC	802.11 MAC
Bitübertragungsschicht (Physical Layer) PHY	802.11 PLCP (Physical LayerConvergence Protocol)
	802.11 PMD Infrarot 802.11 PMD FHSS 802.11 PMD DHSS

4.3 Betriebsmodi

4.3.1 Infrastrukturmodus

Anbindung der mobilen Rechner über Access Points. Ein Access Point ist ein Rechner mit Funknetz und konventionellem Netz

4.3.2 Ad-hoc-Modus

Es werden nur mobile Rechner untereinander verbunden => Kein Zugriff auf ein stationäres Netz

4.4 Weitere Komponenten

4.4.1 Service Sets

4.4.1.1 Basic Service Set

Zwei oder mehr verbundene Rechner.

4.4.1.2 Extended Service Set

Zwei oder mehr verbundene Basic Service Sets, dies unterscheidet sich für die Rechner nicht von einem Basic Service Set.

4.4.2 Portal

Verbindung zu anderen Netzwerken

4.5 Die Bitübertragungsschicht

4.5.1 Grundlagen

Die höhere Fehlerrate beruht auf

- Rauschen und Interferenzen
- Funksignalen von anderen WLAN-Stationen
- Funksignalen von anderen Netzwerken im gleichen Frequenzbereich
- Störungen durch Geräte die in diesem Bereich Strahllung als Abfall erzeugen.

Es gibt drei Frequenzbänder: 900MHz, 2,4 GHz, 5GHz; am verbreitetsten ist das 2,4 GHZ-Band (ISM), außerdem eine Infrarotschnittstelle, die aber keine Verbreitung gefunden hat.

4.5.2 Verfahren zur Funkübertragung

4.5.2.1 Frequency Hopping Spread Spectrum (FHSS)

Das verfügbare Frequenzspektrum wird auf 79 Kanäle aufgeteilt (Frankreich, Spanien Japan: 23) und die Sendefrequenz wird mindestens 2,5 mal pro Sekunde nach einer Pseudozufallsfolge gewechselt.
1-2Mbit/s

4.5.2.2 Direct Sequence Spread Spectrum (DSSS)

Aufteilung auf 14 Kanäle, CDMA. Hat sich durchgesetzt.

4.5.3 Zugriff auf das Funkmedium

Collision Detect ist nicht möglich, da der Sender an seinem Ort alle anderen überdeckt, daher muss Collision Avoidance durchgeführt werden. Hier sind drei Verfahren definiert:

4.5.3.1 Einfaches CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance)

Der Sender hört das Medium ab. Findet eine Übertragung statt, wird deren Ende und eine zusätzliche Wartezeit abgewartet. Ist dann immer noch frei, wird gesendet. Sendet während der Wartezeit eine andere Station, beginnt der Backoff. Die Wartezeit setzt sich aus einer konstanten Anteil DIFS und einem zufallsabhängigen zusammen. Bei besetztem Medium wird eine Zufallszahl ermittelt und anschließend heruntergezählt. Ist wieder besetzt, wird der Zähler nicht neu initialisiert. □ei Kollisionen wird er mögliche wert für die Zufallszahl exponentiell erhöht um auf Überlastung des Funkmediums zu reagieren.
Wird an eine bestimmte Station gesendet, muss diese den Erhalt bestätigen. Hierfür muss sie nicht so lange warten, wie sonst, sondern nur einen Short Interframe Space(SIFS)

4.5.3.2 CSMA/CA mit RTS/CTS (Request to send/Clear to send)

Eine sendewillige Station sendet an den Empfänger einen RTS-Frame, den dieser nach einem SIFS mit einem CTS-Frame bestätigt. In diesem Frames ist die gewünschte Belegungszeit für das Funkmedium (NAV-Net Allocation Vector) enthalten.(Löst das Hidden Terminal-Problem)

4.5.3.3 Point Coordination Function

Im Infrastruktur-Modus kann eine Station den Zugriff auf das Funkmedium koordinieren. Diese reserviert das Medium für eine Zeit und fragt dann alle Stationen nacheinander ab, ob sie was senden wollen.

4.5.3.4 Weitere Funktionen

4.5.3.5 Uhrensynchronisation

4.5.3.6 Power Management

4.5.3.7 Roaming

4.5.3.8 Sicherheit

4.6 HIPERLAN/1

4.6.1 Eigenschaften

- ~5 GHz, 5 Kanäle
- bis ca 24 Mbit/s
- bis ca 50 m
- Forwarding
- Batteriesparmechanismen

4.6.2 Architektur

Bitübertragungsschiht wie bei WLAN (?!)
Sicherungsschicht aus Channel Access Control und Medium Access Control, letzteres ziemlich ausgefeilt:

4.6.3 Zugriff auf das Funkmedium

Bei freiem Kanal wird noch eine Zufallszeit gewartet und dann gesendet, wenn immer noch frei ist.
Beibesetztem Kanal gibt es die

1. Priorisation Phase (Die wichtigsten Stationen bleibe übrig)
2. Contention Phase (Die gleichwichtigen Stationen senden einen Burst zufälliger Länge, der längste Burst kriegt das Mediuim)
3. Transmission Phase (hier wird gesendet)

4.6.4 Hidden-Terminal-Elimination

- Das Funksignal kann empfangen aber nicht mehr entschlüsselt werden.
- Eine Station verliert die Contention Phase, danach bleibt das Medium aber frei.

4.6.5 Forwarders

Bestimmte Stationen reichen Pakete weiter und stellen dafür eigene Ressourcen zur Verfügung

4.7 HIPERLAN/2

4.7.1 Eigenschaften

- ~5GHz
- bis 54Mbit/s
- 30m innen, 150 draußen
- Ad-Hoc-Modus und Infrastruktur-Modus
- Dienstgüte
- Batteriesparen

4.7.2 Architektur

4.7.2.1 Bitübertragungsschicht

wie immer.

4.7.2.2 Sicherungsschicht

Radio Link Control(Verschlüsselung, Handover, Power Management)
Error-Control (Im Wesentlichen ARQ)
Media Access Control (wie in 802.11)

4.7.2.3 Convergence Layer

Paketunterteilung und Abbildung von Anforderungen höherer Schichten auf die DLC.

- Zellenbasiert für Atm
- Paketbasiert z. B. für Ethernet

4.7.3 Core Networks

Interaktion mit anderen Netzwerken

4.8 Wireless ATM

ATM basiert auf virtuellen Verbindungen und benutzt Pakete konstanter Länge. Es setzt extrem niedrige Bitfehlerraten und Paketverlustraten voraus. Es können Dienstgüten garantiert werden, was der interssanteste Punkt ist. Einsatz vorwiegend als Backbone-Technologie.
Die Erweiterung in den Wireless-Bereich ist wegen der großen Einsatzmöglichkeiten, der Fortsetzung der Backbones und der Dienstgüte interessant.
Die Technologie ist komplex und teuer, setzt sich wahrscheinlich nicht durch.

4.9 HomeRF

4.9.1 Eigenschaften

- ~2,4 GHz
- 10 Mbit/s
- 50m
- FHSS
- 8 priorisierte Kanäle für Multimedia
- 8 bidirektionale Audiokanäle
- 127 Stationen
- Ad-Hoc- und Infrastrukturmodus, in Ad-Hoc aber keine prioriserten- und keine Audiokanäle

4.9.2 Architektur

Mac und Phy wie immer.
Danach IP, TCP, UDP, bzw bei DECT direkter Durchgriff auf MAC

4.10 Vergleich der Netze

Netz	**Organisation**	**Spezifiziert**	**Datenrate**	**Frequenz**	**Reichweite**
IEEE 802.11	IEEE	1997	2 Mbit/s	2,4 GHz	30-300m
IEEE 802.11a	IEEE	1999	54 Mbit/s	5 GHz	100 m
IEEE 802.11b	IEEE	1999	11 Mbit/s	2,4 GHz	30-300m
HIPER-LAN/1	ETSI	1996	24 MBit/s	5 GHz	50m
HIPER-LAN/2	ETSI	1999	54 Mbit/s	5 GHz	30-150m
Wireless ATM	ATM Forum	-	25 Mbit/s	5 GHz	30-300m
HomeRF	HomeRF	1998	10 Mbit/s	2,4 GHz	50 m

4.11 Besonderheiten

- IEEE 802.11 gliedert sich nahtlos in IEEE 802 ein.
- HIPERLAN hat ein ausgefeiltes Zugriffsverfahren auf das Funkmedium und Core Networks
- Wireless ATM ist noch nicht fertig, Schwerpunkt ist die Anbindung drahtloser Stationen an ein Weitverkehrsnetz
- HomeRF ist für den Konsumbereich, kann aber ein vollwertiges Netz bilden.

KE 3

5 Wireless Personal Area Networks

- Möglichleiten, Einsatzgebiete und Grenzen von WPANs kennen
- Vor- und Nachteile der Infrarotkommunikation gegenüber der funkbasierten
- IrDA und Buetooth beschreiben
- Die Unterschiede zwischen IrDA und Bluetooth beschreiben

5.1 Definition und Einsatzgebiete

WPANs dienen zur Vernetzung kleinerer Geräte über kurze Distanzen, wie Drucker, Armbanduhren usw.

5.1.1 Eigenschaften

- Kurze räumliche Distanz zu überbrücken
- Geringe Energiereserve wegen Batterienutzung
- Massen- und Konsummarkt, daher kostengünstig
- Nur minimale Konfiguration
- Es ist kein vollwertiges Netz erforderlich
- Nur Point to Multipoint-Kommunikation

5.1.2 Einsatzgebiete

- Druckeranschluß
- Anschluß eines Headsets an ein Mobiltelefon
- Anschluß von Rechnerperipherie
- Vernetzung von Haushaltsgeräten
- Vernetzung von PDAs

5.2 IrDA

Es gibt IrDA-Control für Rechnerperipherie und IrDA-Data für anspruchsvolle Aufgaben.

5.2.1 Eigenschaften von IrDA-Data

- Bis 16Mbit/s
- Bis 1 m
- Suchen von Geräten in Kommunikationsreichweite und ihren Diensten
- Automatisches Aushandeln von Kommunikationsparametern
- Mehrere zuverlässige logische Kanäle
- Unzuverlässiger Broadcast
- Transportprotokoll für lange Nachrichten
- Protokoll zur Netzwerkanbindung
- Protokoll für komplexe strukturierte Datenobjekte

5.2.2 Vergleich zwischen Infrarot- und Funkkommunikation

Eigenschaft	Infrarot	Funk
Reichweite	Klein	groß
Einsatzumgebung	Nur innerhalb von Gebäuden	Innerhalb und außerhalb von Gebäuden
Anordnung von Sender und Empfänger	Sichtverbindung erforderlich	Beliebig innerhalb der Reichweite
Abhörsicherheit	Groß	klein
Störquellen	Sonnenlicht, Kunstlicht, Streuung, Reflexion	Elektromagnitische Quellen, Streuung, Reflexion
Frequenzen	Keine Beschränkung	Hoheitlich geregelt

5.2.3 Protokollstapel

5.2.3.1 Pflicht

- Bitübertragungsschicht – OSI 1. 20 cm oder 1 m Reichweite, mindestens 15 Grad Kegel, bis 16 MBit
- Infrared Link Access Protocol (IrLAP) – OSI 2. Zugriffskontrolle, Suche, Aushandeln von Kommunikationsparametern, Beginnen und Beenden von Verbindungen, Gesicherte bidirektionale Verbindung. Normal Disconnect Mode/Normal Response Mode. Primary/Secondary-Verfahren.
- Infrared Link Management Protocol (IrLMP) – OSI 3. Tauschen der Primary/Secondary-Rolle. Mehrere logische Kanäle. Rudimentäres Discovery
- Information Access Service (IAS) – kein OSI. Zugriff auf Dienste üner Namen

5.2.3.2 Optional

- TinyTP - Miniprotokoll für große Nachrichten, Flusskontrolle auf Kanalbasis über Kredite.
- IrCOMM – Serielle oder parallele Schnittstelle
- IrOBEX Austausch komplexer Objekte
- IrLAN – Anmeldung an ein lokales Netz über einen Access-Point, Peer to Peer oder Hosted

5.3 Bluetooth

5.3.1 Einsatzmöglichkeiten

- Drei in eins-Telefon (Schnurlos, GSM, Bluetooth)
- Drahtloser Internetzugang
- Synchronisation von mobilen Geräten mit einem PC
- Drahtloses Headset
- Drahtlose interaktive Konferenz

5.3.2 Eigenschaften

- Bis 1 Mbit/s
- Bis 10 m
- 0,8 W
- 2400-2483 MHz

- 79 Kanäle mit Hopping
- Automatische Verbindung zu Geräten in Reichweite
- Suche installierten Diensten eines anderen Geräts
- Mehrere zuverlässige logische Kanäle zwischen zwei Geräten
- Unzuverlässiger Broadcast
- Audiokanäle mit reservierter Bandbreite
- Dienstgüte
- Transportprotokoll mit Flußkontrolle für lange Nachrichten
- Emulation serieller Schnittstellen
- Authentifizierung und Verschlüsselung

5.3.3 Protokollstapel

- Bluetooth Radio (OSI1)
- Baseband (OSI2) (Piconet und Scatternet, Master/Slave
- Link Manager Protocol (LMP) – logische Verbindungen
- Logical Link Control and Adaption Protocol (L2CAP) – Segmentierung großer Nachrichten, logische Kanäle (OSI4?)
- Host Controller Interface (Zugriff höherer Schichten auf das Baseband)
- Service Discovery Protocol (SDP), Telephony Control Protocol Binary (TCS BIN), RFCOMM(serielle Schnittstelle)

5.3.4 Links und Paketformate

- Synchronous Connection Oriented Links mit reservierter Bandbreite. Drei Links pro Gerät, Verbindung zu verschiedenen Slaves und Mastern erlaubt. Drei Verbindungen pro Gerät. Bevorzugt Audiokanäle. 4 Kanäle. Unzuverlässig.
- Asynchronous Connection-less Links. Genau einer zwischen Master und Slave, zuverlässig, Broadcast möglich. Es gibt 8 ACL-Kanäle, daher kann ein Piconet zunächst nur 8 Geräte umfassen.

5.3.5 Aufbau von Verbindungen und Betriebsmodi

- Standby – nicht verbunden
- Inquiry (Pakete versenden und den Funkverkehr abhören)
- PageScan – Ein Gerät erhält eine Nachricht mit der eigenen Adresse und verbindet sich dann mit dem Piconet, es ist dann Slave.
- Active Mode: Auf SCO und ACL verbunden.
- Sniff Mode: Bei reduziertem Kommunikationsaufkommen wird das Gerät seltener angesprochen
- Hold Mode: Nur noch SCO
- Park Mode: Keine Kommunikation aber Verbleiden im Piconet

5.3.6 Link Management

- LMP deckt die Baseband-Schicht nur teilweise ab. Einige Funktionen können von oben benutzt werden. Keine eigentliche Schicht. Folgende Funktionen:
- Authentification und Verschlüsselung
- Uhrenvergleich
- Tausch der Master/Slave-Rollen
- Ändern der Betriebsmodi
- Ändern der Sendeleistung
- Dienstgüte

- Einrichten von SCO-Links

5.3.7 L2CAP

- Mehrere logische Kanäle pro ACL-Link (Verbindunsorientierte, zuverlässige und verbindungslose unzuverlässige)
- Zerlegung von großen Datenpaketen (Pakete bis 64k in einer Operation)
- Dienstgüte:
- Typ: keine, Best Effort, Garantie
- Token Rate=Bit/s, token Bucket Size=Kreditrahmen, danach blockierts
- Maximale Bandbreite
- Latenzzeit: maximale ms zwischen Übergabe des Pakets und Versand
- Verzögerungsschwankung: Differez zwischen maximaler- und minimaler Übertragungsdauer

5.3.8 SDP

Dient dazu in unbekannten Umgebungen Dienste zu finden.
Jetzt:

- Dienste mit bekannter Dienstklasse (z. B. Drucken)
- Dienste mit konkreten Attributen (z. B. 600 dpi)
- Übersicht verfügbarer Dienste

Evt künftig:

- Weitervermittlung von Diensten (großer Nutzen)
- Zugriffskontrolle
- Rechnungsstellung
- Nachrichten über die aktuelle Verfügbarkeit eines Dienstes

Ein Dienstanbieter startet einen SDP-Server, der eine Datenbank mit Service Records betreibt.

5.3.9 RFCOMM

Emuliert eine RS 232-Schnittstelle. So kann man z. B. TCP/IP an Bluetooth anbinden, nämlich über PPP.

5.3.10 TCSBIN

Telefonfunktionen

5.4 Vergleich IrDA – Bluetooth

5.4.1 Eigenschaften

Eigenschaft	IrDA	Bluetooth
Bitübertragung	Infrarot	Funk
Zugriffsverfahren	Master/Slave	Master/Slave
Geräte mit reduziertem Funktionsumfang	Nur-Slave-Geräte	Nein
Point to Multipoint	Nicht in Version 1.1	Ja
Verbindung zwischen Geräten	Nur, wenn logische Verbindungen eingerichtet werden	Wenn Geräte in Reichweite
Nichtverbundene Geräte in Reichweite	Normal Disconnect Mode	Park Mode
Unzuverlässiger Broadcast	Ja	Ja

Zuverlässige bidirektionale Übertragung	Ja	Ja
Sicherung	ARQ	ARQ + FEC
Bandbreitenreservierung für Audio	Nein	Ja
Überlappung von Netzen	Nein	Scatternet
Brutto-Übertragungsgeschwindigkeit	2,4kBit bis 16Mbit	1 M Bit
Authentifizierung und Verschlüsselung	Nein	ja

5.4.2 Protokollvergleich

Aufgabe	**IrDA**	**Bluetooth**
Zugriffskontrolle, Verbindungsauf- und –abbau, zuverlässige Verbindung	IrLAP	Baseband, LMP
Verschlüsselung und Authentifizierung	Nein	LMP
Mehrere logische Kanäle	IrLMP	L2CAP
Segemtation & Reassembly	TinyTP	L2CAP
Kanalkennung	LSAP-SEL	CID
Protokollkennung	Nein	PSM
Gerätesuche vor Verbindungsaufbau	IrLMP	Werden automatisch verbunden
Service Discovery	IAS	SDP
Kreditbasierte Flusssteuerung	TinyTP	L2CAP
Dienstgüte	Nein	L2CAP

5.4.3 Höhere Protokollschichten

Eigenschaft	**IrDA**	**Bluetooth**
Schnittstellenemulation	IrCOMM (RS 232 und Centronics)	RFCOMM (RS232)
Netzwerkschnittstelle	IrLAN	Über RFCOMM
Objektaustausch	OBEX	ÔBEX

KE 4

6 Protokolle zur mobilen und spontanen Vernetzung

Einfluß der mobilen Kommunikation auf höhere Kommunikationsschichten
Mobilität im Internet
Routing in Ad-hoc- Netzen
Dienstsuche und Dienstvermittlung in mobilen Umgebungen

6.1 Mobilität im Internet

6.1.1 Probleme bei der Anwendung von TCP/IP im mobilen Bereich

1. Die Paketvermittlung setzt voraus, dass Rechner stationär sind und weder ihre Adresse noch ihr Subnetz ändern.
2. TCP geht davon aus, dass Pakete selten verloren gehen, wenn das passiert, liegt es an Routerüberlastung und nicht am Medium.

Lösungsansätze:

1. Ein mobiler Rechner bekommt beim Wandern dauernd neue Adressen
2. Die Vermittlungsschicht des Internet wird für mobile Rechner angepasst.

6.1.2 Zu 1. – DHCP – Dynamic Host Configuration Protocol

- Ein Rechner bekommt automatisch eine Adresse zugewiesen, wenn er in ein neues Netzwerk eingebunden wird. Dies kann manuell, automatisch oder dynamisch erfolgen(s. u.!).
- Der Rechner wird über die Subnetzmaske, die Adresse des DNS-Servers und des Routers informiert.
- Optional auch die Adresse des Mailservers und des Webservers
- Dies erfolgt vollautomatisch.

6.1.2.1 Adressvergabe

- Manuell: der Admin wird über die Anfrage informiert und vergibt eine freie Adresse
- Automatisch: Die freie Adresse wird ohne Admin vergeben.
- Dynamisch: Die freie Adresse wird für eine bestimmte Zeit vergeben. Nach Ablauf muss die Anfrage erneuert werden. Ablauf: Rudimentäre Einbindung (über UDP) -> DHCPDISCOVER ->DHCPOFFER (an die MAC-Adresse des Clients) -> DHCPREQUEST -> DHCPACK. Es werden T1 und T2 mitgeteilt. Nach t1 versucht der Client beoi seinem Server den Lease zu erneuer. Klappt dies nicht bis T2 muss er einen neuen Broadcast machen.

6.1.2.2 Sicherheitsfragen

- Darf jeder dahergelaufene Client mit Subnetzprivilegien ausgestattet werden?
- Woher weiß der Client, dsass er dem DHCP-Server trauen kann?

6.1.3 Mobile IP

Will der mobile Rechner selbst Dienste anbieten, kann sich die Adresse nicht mehr ändern, weil man den Rechner nicht wiederfindet. Mit Mobile IP bleibt die Adresse konstant.

6.1.3.1 Rechnertypen bei Mobile IP

- Mobiler Rechner ist der der sich bewegt uns seine Adresse dabei behält
- Kommunikationspartner ist der Rechner, der zum mobilen Rechner Kontakt aufnehmen möchte.
- Der Heimagent vertritt den mobilen Rechner solange dieser nicht in seinem Heimnetz ist. Er kennt den aktuellen Aufenthaltsort des mobilen Rechners und reicht die Kommunikation durch.
- Der Fremdagent ist im aktuellen Netz des mobilen Rechners und leitet die Anfragen durch.

6.1.3.2 Adresstypen bei den mobilen Rechnern

1. Die Heimadresse ist die unter der der Rechner stets erreichbar ist.
2. Die Care-of-Adresse verwendet der mobile Rechner im fremden Netz. Es gibt
   - Die Foreign-Agent-Care-of-Adresse, hier übernimmt der Fremdagent die Weiterleitung
   - Die Collacated-Care-of-Adresse, die wird an den Heimagenten mitgeteilt, der die Nachrichten an sie schickt.

6.1.3.3 Agent Discovery

- Agent Advertisement: Die Agents senden periodischBroadcasts
- Agent Solicitations: Der mobile Rechner broadcastet die Aufforderung, Agent Advertisements zu senden.

6.1.3.4 Registrierung

Der Heimagent verwaltet das Mapping zwischen der Heimadresse und der Care-of-Adresse. Die Kommunikation zwischen mobilem Rechner und Heimagent erfolgt verschlüsselt.

6.1.3.5 Tunneling

Die weiterleitung vom Heimagenten zum Fremdagenten erfolgt getunnelt, d. h. das IP-Paket wird in ein weiteres verpackt und am Ziel wieder ausgepackt.

6.1.3.6 IPV6

Hier ist mobile IP schon im Standard berücksichtigt, sodass nur noch Collacated care of Adressen verwendet werden und die Heimagent-Funktion von Router übernommen wird.

6.1.4 Cellular IP

Versucht die häufigen Registrierungen beim Zellenwechsel durch mobile Rechner zu verringern, setzt auf Mobile IP auf.

6.1.4.1 Prinzip

Der Heimagent vermittelt nur an das aktuelle Netzwerk über Mobile IP, von da reicht Cellular IP durch. Das Funknetz hat ein Gateway, das als Fremdagent dient, im Funknetz wird durchgereicht. Dazu merkt syich jeder Rechner den nächsten Nachbarn in Richtung Gateway und zu jedem mobilen Rechner. Diese Informationen werden periodisch aktualisiert.

6.1.4.2 Handover

Hard Handoff: Route Update zur neuen Basisstation.

Semisoft Handoff: mit Ankündigung und zeitweisem Doppelversand.

6.1.4.3 Paging

Weckt inaktive Rechner auf.

6.1.5 Mobilität auf Transportebene

Prinzipiell kann man TCP benutzen, wenn man IP hat. Es ist aber für nahezu fehlerfreie Übertragungsmedien optimiert. Namentlich wird bei Fehlern die Übertragungsrate reduziert, weil Routerüberlastung unterstellt wird. Richtig wäre es aber, die Geschwindigkeit beizubehalten und das fehlende Paket nachzusenden.
Lösungsansätze unterstellen, dass es nur eine drahtlose Strecke am Ende der Route gibt.

6.1.5.1 Split Connection-Verfahren

Es wird die Fehlerbehandlung für den drahtgebundenen- und den drahtlosen Teil der Verbindung optimiert. Am Übergang wird gepuffert. Problem: Die Basisstation quittiert schon, obwohl der mobile Rechner das Paket noch nicht erhalten hat.

1. Snoop-Protokoll: Ein Rechner belausch den Quittungsverkehr in beide Richtung und puffert die Pakete, bis sie wirklich angekommen sind (Funktioniert nicht bei verschlüsselter Kommunikation).
2. Fast Retransmission. Es werden beim Stationswechsel die bisher erhaltenen Pakete noch einmal quittiert. TCP sendet die fehlenden nach, ohne die Rate zu reduzieren.
3. Selektive Quittung und Explicit Loss Notification. Es wird nicht mehr kumulativ sondern einzeln Quittiert, bzw. der Verlust explizit gemeldet.
4. Remote Socket-Architektur: Zwischen Basisstation und mobilem Rechner wird nicht TCP, sondern ein einaches Protokoll verwendet.

I-TCP, Mobile TCP??

6.1.6 UDP

Hier kann man nicht viel machen.

6.2 Routing in Ad-hoc-Netzen

Die verwendbaren Verfahren hängen von der Änderungsrate ab. >Bei hoher wird geflutet, bei niedriger normal geroutet. Dazwischen „strukturierte Ansätze“.

6.2.1 Klassifikation der Verfahren

Adaptive ⇔ nichtadaptive Verfahren (Für Ad-hoc-Netze nur adaptive)
Proaktive ⇔ reaktive Verfahren (table driven ⇔ on demand)
Distance-Vektor ⇔ Link-State (Jeder tauscht mit seinen Nachbarknoten Distanzinformationen aus, auch über nicht benachbarte ⇔ Jeder Knoten ermittelt die Distanz zu seinen Nachbarn und schickt die Info an alle)

6.2.2 Besonderheiten von Ad-hoc-Netzen

- Die Adressen spiegeln die Topologie nicht wider und können daher nicht zur Wegeauswahl herangezogen werden.
- Es gibt keine hierarchische Gliederung
- Die Dinger beqwegen sich auch noch.
- Die Weiterleitung kann nicht auf Router abgewälzt werden.

6.2.3 DSDV (Destination-Sequenced Distance-Vector)

6.2.4 Prinzip

Jeder Knoten hat für jeden anderen die Information, über welchen Nachbarn ein Paket weitergeleitet werden muss und wie weit es bis zum Ziel ist..

6.2.5 Klassifikation

Adaptiv, proaktiv, Distance Vector.

6.2.5.1 Ermittlung der Distanz und des Weges

Die Knoten senden nach und nach die Information über alle Zielknoten an alle anderen Knoten. Dabei kann jeder Knoten seine bisherige Information vergleichen. Ist (ein neuer Weg zu einem Zielknoten + der Weg vom berechnenden Knoten zum Startknoten des neuen Weges) kürzer als der bisherige kürzeste Weg ist dies der neue kürzeste Weg.

6.2.5.2 Unterbrochene Verbindungen

Bei einer unterbrochenen Verbindung wird zwar nach und nach die Distanz hochgezählt, allerdings wird der Sachverhalt, dass keine Verbindung mehr existiert im einfachen Ansatz nie widergespiegelt.

6.2.5.3 Lösung

1. Die Routingtabelle wird um eine Sequenznummer erweitert, die vom Zielknoten vergeben wird. Distanzinfos werden nur aktualisert, wenn eine höhere sequenznummer vorliegt oder bei gleicher sequenznummer eine niedrigere Distanz.
2. Nach jede Verbreitung an alle Nachbarn erhöht ein Knoten die eigene Sequenznummer um 2.
3. Erkennt ein Nachbarknoten eine Unterbrechung , so verschickt er Nachrichten mit dem Inhalt, dass der Hop unbekannt und die Distanz unendlich ist und er erhöht die Sequenznummer um 1.

6.2.5.4 Hauptnachteil

Es werden ständig große Netzwerkpakete zur Aktualiserung der Routingstabellen versandt, auch wenn sonst nix los ist.

6.2.6 DSR (Dynamic Source Routing)

6.2.6.1 Prinzip

Bei Bedarf wird der Weg zum Ziel ermittelt und im Paket hinterlgt.

6.2.6.2 Klassifikation

Adaptiv, Reaktiv, Distance Vector

6.2.6.3 Ermittlung des Weges

Ein Sender schickt an alle Nachbarn Roue Request-Pakete mit einer Identifikationsnummer. Weiß ein Nachbar eine Route, schickt er sie per Routte-Reply zurück. Weiß er keins, schickt er es weiter an seine Nachbarn. Ein Paket mit einer Identifikationsnummer, die ein Knoten schon einmal bearbeitet hat, wird ignoriert. Wird ein Paket durchgereicht, das auf einer inzwischen unterbrochenen Route basiert, werden Error-Meldungen zurückgeschickt und es muss eine neue Wegermitttlung durchgeführt werden.

6.2.7 OLSR – Optimized Link State Routing

6.2.7.1 Klassifikation

Adaptiv, proaktiv, Link state.

6.2.7.2 Vorgehen bei Link State-Verfahren allgemein

Suchen vor Nachbarknoten
Messen der Distanz zu den Nachbarn
Erzeugen eines Kontrollpakets
Senden des Kontrollpakets an alle Knoten des Netzwerks (durch Fluten)
Erstellen eines Abbilds der Netzwerktopologie

6.2.7.3 Optimierungen für OLSR

- Verkleinern der KontrollpaketeEs werden nicht mehr alle Nachbarn in die Knontrrollpakete aufgenommen, sondern nur eine Untermenge, die aber ausreicht, den Graphen zu rekonstruieren
- Optimierung des FlutensStatt alle Nachbarknoten zu fluten, werden nur ausgewählte mit Kontrollpaketen versorgt, derart, dass immer noch alle Knoten alle Pakete bekommen.

6.2.7.4 Mengen

- N(Ni) die Menge der Nachbarn eines Knotens Ni
- N2(Ni) die Menge der Knoten, die von Ni zwei Schritte entfernt sind
- MPR die Menge der Nachbarknoten eines Knotens, die von diesem als Multipointrelays ausgewählt wurden
- MPRsel die Menge der Nachbarknoten eines Knotens, die diesen als Multipointrelay ausgewählt haben.

6.2.7.5 Vorgehen zur Berechnung

- MPR = {}
- Die Knoten aus N hinzufügen die eine einzige Verbindung zu Knoten aus N2 darstellen
- Solange es noch Knoten in N2 gibt, die nicht aus MPR erreicht werden:
    - Wähle den Knoten aus, von dem die meisten nicht erreichbaren abgedeckt werden.
    - Bei mehreren gleichwertigen nimm den mit den meisten Nachbarn
- Entferne die Knoten aus MPR ohne die immer noch alle erreicht werden

6.2.7.6 Nutzen von MPR und MPRsel

Die Kontrollnachrichten werden nur noch in MPRsel verbreitet. (muß das nicht MPR sein??)
Es werden nur noch Kontrollnachrichten aus MPRsel weitergereicht, die anderen nur noch verarbeitet

6.2.7.7 Ermittlung des Weges

6.2.8 Link Reversal Routing

Es wird nicht versucht, einen optimalen, sondern nur irgendeinen Weg zu berechnen. Es treten kaum noch Kontrollnachrichten auf, Netzveränderungen wirken sich hauptsächlich lokal aus.

6.2.8.1 Klassifikation

Adaptiv, reaktiv, Distance Vector(?? Keine Distanzinformation)

6.2.8.2 Vorgehen

- Für jeden Zielknoten wird von jedem Knoten ein gerichteter azyklischer Graph aufgebaut.
- Pakete werden entlang dieses Graphen verschickt.

Die Verfahren unterscheiden sich darin, wie auf einen Verbindungsverlust reagiert wird:

6.2.8.3 Full Reversal

Verliert ein Knoten alle Downstreams, kehrt er alle Kanten zu Nachbarn um.

6.2.8.4 Partial Reversal

Es werden alle Kanten umgedreht, außer denen, die im letzten Schritt schon gedreht wurden. Wurden alle im letzten Schritt gedreht, werden alle noch mal gedreht.

6.2.8.5 Höhenbasiertes Partial Reversal

Downstream hat die geringere Höhe. Entsteht eine Senke, wird die angehoben.

6.2.8.6 Problem dieser Verfahren

Sie terminieren nur in nicht partitionierten Netzwerken.

6.2.8.7 Lösung 1: Lightweight Mobile Routing (LMR)

Einführung zusätzlicher ungerichteter Kanten. Zunächst sind alle Kanten ungerichtet. Gerichtete Kanten werden über Anfragepakete erzeugt. Auf das Verlieren aller Downstreams wird mit Fehlerpaketen reagiert. Gibt es noch einen Weg, ist dieser in einem Antwortpaket enthalten; gibt es keinen, wird aus dem Fehlen eines Antwortpakets nach bestimmter Zeit geschlossen, dass es keinen mehr gibt.

6.2.8.8 Lösung 2: Temporally-Ordered Routing Algorithm (TORA)

Funktioniert, ist aber kompliziert.

6.3 Dienstvermittlung in Mobilen Umgebungen

Die verfügbaren Dienste in einem Netzwerk sollten automatisch verwaltet und gefunden werden können.

6.3.1 Dienstvermittlung in WPANs

- IAS für IrDA
- SDP für Bluetooth

6.3.2 Generelles Prinzip für alle Netzformen

Ein Kunde kann einen Dienstvermittler fragen, der eine Datenbank der verfügbaren Diesnte pflegt. Dieser Vermittler kann entweder auf jedem Gerät oder zentral liegen. Liegt er auf jedem Gerät, verwaltet er nur dessen Dienste, dann muß bei jedem Gerät angefragt werden, ob es den gewünschten Dienst hat. Liegt er zentral, müssen die anbietenden Geräte ihn finden und sich registrieren.

6.3.3 Service Location Protocol (SLP)

Funktioniert so. Die entsprechenden Funktionen werden von

- User Agents
- Service agents
- Directory Agents

übernommen.
Der Directory Agent wird über Multicast IP gefunden. Oder über DHCP.
Netzwerke können über Scopes aufgeteilt werden. Es können mehrere Directory Agents betrieben werden, die sich untereinander abgleichen.

6.3.4 Java Intelligent Network Infrastructure (JINI)

JINI basiert auf Java, bietet seine Vorteile, kann aber auch nur aus Java genutzt werden.

6.3.4.1 Protokollstapel

DIENSTNUTZER	KOMMUNIKATIONSFORM	DIENSANBIETER
Anwendung	Dienstnutzung	Dienst
Jini	Jini-Protokoll	Jini
Java/RMI	Methodenaufrufe	Java/RMI (JNI(C++))
Netzwerk	TCP/IP UDP Multicast IP	Netzwerk

6.3.4.2 Ablauf der Dienstnutzung

1. Dienstanbieterdiscovery – er meldet sich bei einem Lookup-Dienst an (??Wie meldet sich der Lookup-Dienst an)
2. Join – er trägt sich beim Lookup ein.
3. Dienstnutzerdiscovery – der Nutzer sucht einen Lookup-Dienstag
4. Lookup – er fragt nach dem gewünschten Dienstag Nutzung

KE 5

7 Positionsbestimmung

7.1.1 Anwendungsmöglichkeiten

- intelligenten Führersystemen, die Empfehlungen aussprechen (Touristeninformationssysteme), bzw. den Weg zum nächsten Exemplar einer bestimmten Einrichtung weisen (Geldautomat, Theater, Restaurant) [Rand02], [Adam99], [Marm00],
- kontext- und ortssensitivem Messaging [Roth03a]
- Navigationssystemen [Roth03a]
- m-Commerce-Plattformen [Roth03a],
- eines Lokalisierungs- und Hilfedienst für Patienten, die u. U. rasch gefunden werden müssen [Dix90], [Magnavox]
- Spielen [Nick01]
- Flottenverfolgung [Rodd02]
- LokalemWetterdienst [Rodd02]
- Supermarkt
- Verknüpfung mit dem Internet
- Verbesserung des Routings in Ad-hoc-Netzen

7.1.2 Ausprägungen von Positionsdaten

- Länge, Breite Höhe
- Relative Position zu einem Punkt
- Roll/Nick/Gierwinkel
- Geschwindigkeit
- Semantische Position

7.1.3 Kontext Awareness

- Informationen über die Umgebung beeinflussen die Ausführung einer Anwendung.
- Infarstruktiukontext
- Systemkontext
- Domänenkontext
- Physikalischer Kontext

7.2 Verfahren und Systeme zur Positionsbestimmung

7.2.1 Kategorien

7.2.1.1 Tracking

Die Position wird durch das Netzwerk bestimmt, die Information liegt im Netzwerk vor.

7.2.1.2 Positioning

Das Netzwerk stellt dem Nutzer Informationen zur Verfügung, die es ihm ermöglichen, seine Position zu bestimmen. Die Information liegt im Netzwerk nicht vor.

7.2.2 Basistechniken zur Positionsbestimmung

- Cell of Origin
- Time of Arrival
- Angle of Arrival
- Messung der Signalstärke

7.3 Satellitennavigation

7.3.1 Vorteile

Die Positionsbestimmung kann überall auf der Erde erfolgen
Umweltbedingungen haben nur einen geringen Einfluß
Hohe Genauigkeit

7.3.2 Nachteile

Immense Kosten
Nur außerhalb von Gebäuden, wenn die Signale von genügend vielen Satelliten empfangen werden.

7.3.3 Prinzip

Es wird die Laufzeit des Funksignals vom Satelliten gemessen. Dies ergibt den Abstand zum Satelliten, d. h. eine Kugelschale als mögliche Position. Berücksichtigung von drei Satelliten ergibt zwei Schnittpunkte, deren einer im Weltraum liegt. Da der Uhrenfehler nicht genau bekannt ist, wird ein vierter Satellit benötigt. Es ergibt sich ein nichtlineares Gleichungssystem mit 4 Gleichungen und 4 Unbekannten, das geschlossen, über Kalman-Filter oder iterativ-linear gelöst werden kann.

7.3.4 GPS

24 Satelliten auf 6 Bahnen mit 12 Stunden Umlaufzeit, minimal 5 maximal 11 Satelliten über dem Horizont. Zuordnung zum Satelliten über CDMA. Das System wird in Benutzersegement, Raumsegment und Kontrollsegment eingeteilt.

7.3.4.1 Dienste

Dienst	Genauigkeit horizontal	Genauigkeit vertikal
Precise Positioning Service	22 m	27,7 m
Standard Positioning Service mit Selective Avaliability	100 m	156 m
Standard Positioning Service ohne Selective Availability	25 m	43 m

7.3.4.2 Fehlerquellen

Fehlerquelle	Fehlergröße
Uhrenfehler	1,5 m
Schwankungen der Umlaufbahn	2,5 m
Störungen der Atmosphäre	0,5 m
Störungend er Ionosphäre	5,0 m
Multipath-Fehler	0,6 m

7.3.5 DGPS

Die Genauigkeit von GPS wird dadurch verbessert, dass eine Bodenstation ihre eigene Position mit GPS bestimmt. Da sie sie genau kennt, kann sie für jeden Satelliten einen Korrekturfaktur ermitteln (nicht für ihre eigene Position, da kombinatorische Explosion wegen der Zahl der Satelliten). Dieser Korrekturfaktor wird an User in der Nähe mittels terrestischen Funks übermittelt. Die Genauigkeit verbessert sich dadurch auf 1-3 m.

7.3.6 WAAS

Funktioniert genauso, allerdings werden die Korrekturdaten über an einen geostationären Satelliten an den Nutzer übermittelt. Genauigkeit?

7.3.7 Weitere Systeme

- GLONASS
- GALILEO

7.4 Positionsbestimmung in Gebäuden

Trägersystem	Name	Prinzip	Genauigkeit	Bemerkung
Infrarot	Active Badge System	Ein Badge sendet einen Infrarotpuls, der den Benutzer identifiziert. Im Raum sind Sensoren angebracht, die dies empfangen und weitermelden.	Raum	Tracking. In späteren Ausbaustufen zwei-Wege Kommunikation
Infrarot	Wireless Indoor Positioning System WIPS	Die im Raum angebrachten Infrarotbaken senden Impulse, die von der Badge verarbeitet und an den Location Server durchgereicht werden. Dieser verarbeitet und gibt an die Badges zurück	Raum	Tracking. Positioning mit besseren mobilen Einheiten denkbar.
Funk	SpotON	Die Funkempfänger sind über das Gebäude verteilt, die Funkbadge sendet.. Da der Funk Wände durchdringt, ist die Lokalisierung schwieriger.	3 m	Tracking. Verbesserung de Genauigkeit durch Training?
Funk	RFIDS	Empfänger ohne eigene Batterie, die auf per Funk an sie übermittelte Befehle reagieren. Sie dienen dazu, Objekte z. B. auf einem Fließband oder Kunden im Supermarkt zu verfolgen	1m, da der Funk nicht weiter reicht	Tracking
Ultraschall	Active Bat	Der Nutzer trägt ein Bat, das Ultraschallimpulse aussendet. Diese werden von an de Decke in einem 1,2m-Rastzer angebrachten Sensoren Empfangen. Anhand der Laufzeit wird die Position bestimmt	10 cm	Tracking

Ultraschall	Cricket	Die im Raum aufgestellten Baken senden Ultraschall- und Funkimpulse gleichzeitig. Postionsbestimmung über die Laufzeit des Ultraschalls. Kein zentraler Server	Raum	Positioning
Sichtbares Licht	verschiedene	Der User wird auf Videobildern identifiziert und verfolgt.	?	Tracking

7.5 Netzwerkgestützte Positionsbestimmung

7.5.1 GSM – MPS (Mobile Positioning System)

- Cell of Origen
- (Angle of Arrival)
- Time of Arrival – Timing Advance
- Uplink Time of Arrival, wenn im Bereich mehrerer Basistationen

Die Auswertung erfolgt zentral durch das Mobile Positioning Center, daher Tracking.

7.5.2 WLAN – Nibble

Bestimmung der Position anhand der Signalstärke zu allen Access Points. Positionsbestimmung anhand der Ähnlichkeit ndes Signalmusters zum während der Trainingsphase ermittelten.

7.6 Geografische Adressierung

7.6.1 Idee

- Adressierung nicht anhand der Netzwerktopologie, sondern der geografischen Lage.

7.6.2 Probleme

- Hinreichende Adressgröße, z. B. 10 Byte erforderlich
- Der rEchner muss seine Position kennedn
- Alle aktuellen Netzwerkprotokolle müssen umgestellt werden

7.6.3 Geo-Routing

Wie bei LSI das Domänensystem.

7.6.4 Multicast

7.6.4.1 Begriffe

- Atom: kleinste adressierbare Fläche
- Partiton: größee Fläche aus Atomen oder Partitionen zusammengesetzt.
- Wichtig: Atome und Partitionen werden nicht an einer Partitionsgrenze geschnitten

7.6.4.2 Verfahren

Jedem Atom und jeder Partition wird eine eigene Multicast-Gruppe zugeordnet. Das Paket wird an die kleinste Partiton geschickt, in der das Zielpolygon vollständig ent-

halten ist. Die Beschreibung des Zielpolygons ist im Paket enthalten. Basisstationen die nicht hinein fallen, verwerfen das Paket.

7.6.5 Geografische Adressierung mit DNS

Erweiterung der mit den DNS-Servern verwalteten Informationen um geografische Koordinaten. Oder Verwendung Geografischer- statt Netzwerkdomänen wie bei LSI.

KE 6

8 Sicherheit in mobilen Netzen

8.1 Eigenschaften von Sicherheit

8.1.1 Vertraulichkeit

Bei einer Verletzung der Vertraulichkeit gewinnt neben den Berechtigten noch ein unbefugter Dritter Kenntnis über Inhalte. Es handelt sich hier um einen absichtlichen oder unabsichtlichen passiven Angriff nichttechnischer Natur. Er kann einerseits dadurch geschehen, dass ein Nachrichtenkanal abgehört wird, andererseits kann sich ein Unbefugter Zutritt zu dem Gerät verschaffen, auf dem die Daten abgelegt sind. Es kann sich um einen Server handeln oder um den Verlust oder Diebstahl eines mobilen Clients. Im Zusammenhang mit der nachträglichen Rekonstruktion eines Bewegungsprofils wirft dies Fragen danach auf, ob eine Speicherung zurückliegender Positionsangaben auf dem Client erfolgen darf.
Eine Verletzung der Vertraulichkeit kann durch eine Verschlüsselung erschwert werden. Diese kann sich sowohl auf die Nachrichtenübertragung als auch auf die Ablage von Daten erstrecken.

8.1.2 Integrität

Bei einer Verletzung der Integrität werden Daten aktiv verändert. Dies geschieht i. d. R. absichtlich, nicht-technisch bedingt, ist jedoch auch unabsichtlich durch technische Probleme möglich, bzw. durch eine Fehlbedienung. Auch diese Bedrohung kann sich sowohl in der Übertragung als auch auf dem Server oder Client manifestieren.
Ein mögliches Mittel gegen Integritätsverletzung ist die Erzeugung von Redundanz. Um auch aktive Angriffe abzudecken, muss diese aber so ausgelegt sein, dass die Redundanzinformation nicht einfach aus den geänderten Daten erzeugt werden kann (Signierung). Auch eine Verschlüsselung erschwert eine Modifikation beträchtlich, da keine gezielte Datenveränderung mehr möglich ist. Ein einfaches Hinzufügen von z. B. Paritätsbits deckt dagegen nur eine unbeabsichtigte Modifikation auf.

8.1.3 Identifikation und Authentizität

Bei einer Kommunikation oder auch nur der Benutzung eines Rechners muss sich ein Benutzer zunächst identifizieren, z. B. durch eine Login-Prozedur, bei der er sich neben der Nennung seines (Benutzer)namens durch weitere „Beweise“ authentisiert [Kelt92]. Bei einer Authentizitätsverletzung stammt z. B. eine Nachricht nicht von dem Absender, der der Nachricht zu entnehmen ist. Es handelt sich um einen aktiven, nichttechnischen, beabsichtigten Angriff oder um einen Konfigurations- oder Bedienfehler, in diesem Falle wäre er unabsichtlich. Es ist einerseits daran zu denken, dass sich ein Fremdcomputer als LSI-Server ausgeben könnte, andererseits könnte sich ein Client unberechtigt LSI-Dienste zunutze machen.
Ein Mittel, um Authentizitätsverletzungen zu begegnen ist die Verwendung von Message Authentication Codes, z. B. digitaler Signaturen oder auch in diesem Falle die Verwendung einer Verschlüsselung, die den Urheber erkennen lässt. Hier ist allerdings die begrenzte Rechenkapazität mancher Clients zu berücksichtigen, darüber

hinaus ist die Sicherheit von hinterlegten Schlüsselinformationen auf mobilen Geräten als eher gering einzustufen.
Grundsätzlich ist eine Identifikation und Authentisierung pro Kommunikationssitzung oder pro Nachricht möglich.

8.1.4 Autorisierung und Zugriffssteuerung

Mit der Identifikation und Authentisierung eines Benutzers geht i. d. R. eine bestimmte Autorisierung einher, d. h. der Benutzer hat Zugriff auf nur einen Teil eines Systems [Roth02]. Bei einer Verletzung der Autorisierung, die das ganze Spektrum der Systematik umfassen kann, erlangt ein Benutzer Zugriff auf Systembestandteile, die ihm nicht zustehen. Hierzu muss natürlich klar definiert sein, auf welche Systemteile welcher Benutzer Zugriff haben soll. Diese Überlegungen sind im Zusammenhang mit LSI insbesondere in der Serverkommunikation anzustellen: Wer darf Informationen anbieten?

8.1.5 Nicht-Abstreitbarkeit

In diesem Zusammenhang ist sicherzustellen, dass einerseits der Empfänger nachweisen kann, dass eine konkrete Nachricht tatsächlich vom vorgeblichen Absender kommt. In Erweiterung des Authentizitätsbegriffs kann der Sender also nicht mehr abstreiten, die fragliche Nachricht erzeugt zu haben. Andererseits kann der Sender beweisen, dass ein Empfänger eine Nachricht tatsächlich erhalten hat. Die Einstufung in die Systematik ist hier genauso vorzunehmen wie bei der Authentizität.
Dieser Aspekt kann durch die Erzeugung von authentischen Quittungen für eine Nachricht sichergestellt werden.

8.1.6 Verfügbarkeit

Bei einem Angriff auf die Verfügbarkeit steht der entsprechende Dienst bei Bedarf nicht zur Verfügung. Es handelt sich hier i. d. R. um einen aktiven, beabsichtigten und technischen Angriff (z. B. Denial of Service-Attacke) oder um ein passives, unabsichtliches und technisches Problem (Antennenmast umgefallen).
Das klassische Gegenmittel sind hier hochverfügbare Systeme, die redundant ausgelegt sind, so dass einzelne Ausfälle den Betrieb nicht unterbinden.

8.1.7 Verlässlichkeit

Ein weiterer zentraler Sicherheitsaspekt eines Systems ist dessen Verlässlichkeit, d. h. die Funktionsweise eines Systems muss den gestellten Anforderungen genügen; insbesondere muss der Benutzer sich auf die Ergebnisse verlassen können, und er muss sie in einer Zeit erhalten, die seinen Bedürfnissen entspricht. In diesem Zusammenhang existiert ein Interessenkonflikt zwischen den Sicherheitsanforderungen und den durch die begrenzte Rechenkapazität der Clients hervorgerufenen Antwortzeiten, wenn z. B. durch die Verwendung komplexer Verschlüsselungsverfahren deren Prozessoren überlastet werden.

8.1.8 Beherrschbarkeit

Für den Nutzer eines Systems stellt dessen Beherrschbarkeit einen zentralen Aspekt dar. Wohlfeil definiert Beherrschbarkeit als Schutz vor den unerwünschten Auswirkungen von Technologien und Systemen [Wohl99]. Im Zusammenhang mit der LSI ist hier wohl in erster Linie an die Erstellung von Bewegungsprofilen zu denken, die schon durch die technische Grundkonzeption der Identifizierung und Autorisierung verhindert werden sollte.

Darüber hinaus gehört zur Beherrschbarkeit, dass der Benutzer weiß, was mit seinen Daten passiert (s. folgendes Kapitel Datenschutz!). Schließlich kann sich für den Benutzer der Eindruck einer mangelhaften Beherrschbarkeit und daraus folgend erhebliche Akzeptanzprobleme auch durch die ausgeprägte Asymmetrie in der Beziehung zum Provider ergeben [Haus02], der Benutzer hat den (zutreffenden) Eindruck, der Provider könne mit seinen Daten machen „was er wolle“.

8.2 Arten der Verschlüsselung

Symmetrisch/Asymmetrisch; Block/Stream, Cipher Block Chainig.

8.2.1 Symmetrisch

DES, TDEA = Triple DES, AES

8.2.2 Asymmetrisch

8.2.2.1 RSA

Öffentlicher Schlüssel: e, n
Privater Schlüssel: d, n
Klartext: Zahl M mit 0 <= M <= n. Wird M zu groß, muss der Text in Blöcke zerlegt werden.
Verschlüsselter Text: Zahl C
Verschlüsselung: $C = M^e \bmod n$
Entschlüsselung: $M = C^d \bmod n$

d, e, und n müssen so gewählt werden, dass gilt:
$M = C^d \bmod n = (M^e)^d \bmod n = M^{ed} \bmod n$

Rezept
1. Der Empfänger wählt zwei beliebige Primzahlen p, q. Diese bleiben geheim.
2. Er berechnet n = pq und Phi(n) = (p - 1)(q - 1)
3. Er wählt ein e mit ggT(e, Phi(n)) = 1, 1 < e < Phi(n)
4. Er berechnet d mit (de) mod Phi(n) = 1
5. E, n sind der öffentliche Schlüssel

8.2.3 Diffie Hellmann

8.2.4 Hashfunktionen

8.2.5 Authentifizierung

8.3 Wireless Transport Layer Security (WTLS)

8.3.1 Ziele

Integrität, Vertraulichkeit, Authentizität, Schutz gegen Denial of Service

8.3.2 Verfahren

- Asymmetrische Verschlüsselung zum Vereinbaren eines symmetrischen Sitzungsschlüssels
- Symmetrische Verschlüsselung für die eigentliche Kommunikation
- Hashfunktionen zur Authentifizierung

Es wird eine Sitzungsstand verwendet, bestehend aus
Sitzungskennung
Zertifikat des Kommunikationspartners
Symmetrrischer Verschlüsselungsaölgorithmus
Hashfunktion
Gemeinsames Master Secret

8.3.3 Protokolle

- Handshake
- Change-Cipher
- Alert

8.3.3.1 Handshake Protokoll

Client Hello(WTLS-Version, Zufallszahl, Sitzungskennung, unterstützte Schlüsselaustauschverfahren (Diffie-Hellman oder RSA), unterstützte symmetrische Verfahren (DES, TDEA, RC5), Unterstützte Hashfunktionen (MD5, SHA1), unterstützte Komprimierungsverfahren, Frequenz der Neuvereinbarung der krypt.-Verfahren)
Server Hello(WTLS-Version, eine neue Zufallszahl, Sitzungskennung, Schlüsselaustauschverfahren, symmetrisches Verschlüsselungsverfahren, Komprimierungsverfahren, Wechselhäufigkeit)
Change Cipher Spec beidseits
Finish beidseits mit Hash über das gesamte bsiherige Protokoll
Optional(beiderseits Zertifikate, beiderseits Zertifikatprüfungsanforderung)

8.3.4 Nutzdaten

Aufteilung in Blöcke, optional Komprimierung. Signierung mit Hash, symmetrische Verschlüsselung. Nach Ablauf der vereinbarten Frist neuer Schlüsselabgleich.

8.3.5 Master Secret

Verknüpfung des mit asymmetrischen Verfahren ausgetauschten Pre Master Secrets mit den Sitzungszufallszahlen.

8.3.6 Denial of Service

Da die Nachrichten authentifiziert sind, müssen sie sich gegen das Handshake-Protokoll richten. Um dies nicht zu einfach zu machen, können zu häufige Aufforderungen zum Schlüsselabgleich ignoriert werden.

8.4 Authentifizierung durch das Challenge-Response-Verfahren

Das zu authentifizierende Gerät wird aufgefordert, den Besitz eines Schlüssels nachzuweisen, indem es ihn benutzt um eine vorgegebene nur einmal zu verwendende Zeichenkette (Challenge) zu verschlüsseln. Es schickt den verschlüsselten Challenge zurück (Response). Das authentifizierende Gerät, dem der Schlüssel auch bekannt sein muß, führt dieselben Berechnungen durch und vergleicht.

8.5 Sicherheit in GSM-Netzen

8.5.1 Ziele

- Schutz vor nicht autorisiertem Telefonieren
- Schutz vor Abhörung von außerhalb des Netzes
- Schutz vor Trackingvon außerhalb des Netzes

8.5.2 Entitäten des Sicherheitskonzepts

- Drei kryptografische Funktionen A3, A5, A8
- Schlüssel Ki zur Authentifikation, Kc zur Verschlüsselung der Kommunikation
- Die SIM-Karte mit IMSI, Ki sowie A3 und A8
- Das Mobiltgelefon mit A5
- Das Authentication Center AUC mit seinem Mapping von IMSI auf Ki

Es wird nur die Luftschnittstelle abgesichert

8.5.3 Authentifizierung

Es authentifiziert sich nur der Teilnehmer gegenüber dem Netzbetreiber mittels eines Challenge-Response Verfahrens:.Der Netzbetreiber schickt eine Zufallszahl an den Teilnehmer, dieser verschlüsselt mit A3 diese Zahl und seinen Ki.

8.5.4 Kommunikationsverschlüsselung

Kc wird gebildet, indem A8 auf die Zufallszahl und Ki angewendet wird. Kc dient als Eingabe für A5, eine Stromchiffre.

8.5.5 Roaming

Das Challenge-Response-Verfahren wird vom Fremdnetzbetreiber an den Heimat-netzbetreiber des Teilnehmers delegiert.

8.5.6 Anonymität

Durch Verwendung der TIMSI.

8.5.7 Kritik an diesem Konzept

- Die Funktionen A3, A5 und A8 sind geheim und damit keiner Peer Review unterworfen. A5 scheint gebrochen.
- Kc ist mit nur 64 Bit zu kurz.
- Keine Authentifikation des Netzbetreibers => IMSI-Catcher

8.6 Sicherheit in Wireless LANS

8.6.1 Möglichkeiten nach IEEE 802.11

Zugriffslisten
Gemeinsames Kennwort
Verschlüsselung der Pakete mit diesem Kennwort

8.6.2 Wired Equivalent Privacy

8.6.2.1 Architektur

- Alle haben einen gemeinsamen geheimen Schlüssel.
- Jedes Paket wird damit symmetrisch verschlüsselt.
- Der Schlüssel wird nur selten geändert.
- Zusätzlich wird ein 24 Bit Initialiserungsvektor verwendet.
- Es gibt 40 Bit Schlüssel und 104 Bit Schlüssel.
- Es wird RC4 verwendet
- Integritätscheck mit CRC

8.6.3 Kritikpunkte

Der geheime Schlüssel setzt voraus, dass alle Teilnehmer vertrauenswürdig sind.

40 Bit sind zu wenig.
Der Initialisierungsvektor ist zu kurz, manche Karten ändern ihn nicht.
RC4 ist gebrochen.

8.7 Sicherheit in Bluetooth-Netzen

8.7.1 Sicherheitsmodi

Modus 1: keine Sicherheit
Modus 2 Sicherheit auf Dienstebene
Modus 3 Sicherheit auf Verbindungsebene

8.7.2 Entitäten

- Kryptografische Funktionen E0, E1, E21, E22, E3
- Zufallszahlengenerator
- Geräteadresse 48 Bit, nicht änderbar
- (4-Stellige) Geheimzahl (bei einfachen Geräten)
- Link Key für gegenseitige Authentifizierung, Encryption Key zur Verschlüsselung

8.7.3 Schlüsselgenerierung

Ein Benutzer muss an beiden Geräten dieselbe PIN eingeben. Daraus wird mit einer Zufallszahl ein Unit Key, Combination Key oder Master Key erzeugt.

8.7.4 Authentifizierung

Challenge-Response Verfahren.

8.7.5 Verschlüsselung

Stromchiffre

8.7.6 Sicherheit auf Dienstebene

Einstufung der Dienste in 3 Klassen:
1. Nur nach Authentifikation und Autorisierung
2. Nur nach authentifikation
3. Jeder darf.

8.7.6.1 Zugriff auf Dienste

Über eine L2CAP-Verbindung und den Security Manager. Bei höheren Protokollschichten eventuell separat zusätzlich.

8.7.7 Kritikpunkte

- Frequency-Hopping ist kein Schutz.
- Der Zufallszahlengenerator ist nicht genügend spezifiziert
- Unit Keys werden in allen Geräten gespeichert, die mit dessen Besitzer reden wollen. Somit können sie sich unter Änderung ihrer MAC-Adresse für dieses Gerät ausgeben.
- 4-Stellige, nicht änderbare PINs sind Mist.
- Bluetooth-Geräte, die nicht im Non-discoverable Mode sind, reden mit jedem. Sind sie in diesem Mode, kann man sie nicht richtig benutzen

9 Mobile Endgeräte

Kategorie	Universalgerät	Spezialgerät
Mobile Standardcomputer	Notebook	Spezielle mobile Computer in Vermessungstechnik, Kartografie, Archäologie
Bordcomputer	-	In Fahrzeugen, Flugzeugen Satelliten
Handhelds	PDA Smart-Phone Kommunikator Mobile Spielekonsole Programmierbarer Taschenrechner	Elektronischer Kalender Lesestift #E-Book Web-Pad Mobiles Datenerfassungsterminal GPS-Empfänger Mobiltelefon Pager Digitalkamera Smart-Phone Kommunikator Mobile Spielekonsole Programmierbarer Taschenrechner
Wearables	Programmierbares Wearable	Armbanduhr Pulsmesser
Chipkarten	Smart Card	SIM-Karte EC-Karte Telefonkarte

9.1 Geräte für Palm OS

Prinzipiell sind es Universalgeräte, sie sind aber für

- Terminverwaltung
- Adressverwaltung
- ToDo_listen
- Merkzettel und Notizen

optimiert.

9.1.1 Das Betriebssystem

9.1.1.1 Aufgaben

- Starten und Stoppen von Anwendungen
- Handschrifterkennung
- Energiesparen
- Einschalten bei hzeitabhängigen Ereignissen z. B. Weckerfunktion
- Vewaltung der Daten im gepufferten speicher
- Kommunikation

9.1.1.2 Besonderheiten

- Single Thread
- Ereignisgesteuert

- Nur rudimentäres Filesystem. Vorwiegend Datenbankgestützt.

9.1.1.3 Betriebsmodi

- Sleep-Mode = „ausgeschaltet“
- Doze Mode = „eingeschaltet“ Das Gerät reagiert auf Eingaben, der Prozessor tut aber nix
- Running Mode: Der Prozessor arbeitet, z. B. die letzte Eingabe ab. Danach geht er sofort wieder in den Doze Mode

9.1.1.4 Handschrifterkennung mittels Graffiti

9.1.1.5 Bei der Softwareentwicklung sind die Besonderheiten des Einsatzes zu beachten

9.2 Geräte für Windows CE

Lehnt sich mehr an einen Desktop an.

KE 7

10 Datenübertragung in mobilen Umgebungen

10.1 Besonderheiten

- Spontaner Verbindungsauf- und –abbau.
- Kommunikation zwischcen Geräten unterschiedlicher Hersteller
- Möglichst keine Konfiguration „von Hand“
- Charakteristik mobiler Geräte
- Sicherheitsaspekte von besonderer Bedeutung

10.2 OBEX (Object Exchange Protocol)

10.2.1 Idee

Das Versenden von Objekten wird erlaubt, ohne dass das konkrete Datenformat im Protokoll spezifiziert wurde. Es kann auf jedem zuverlässigen Transportprotokoll aufsetzen (TCP/IP, Tiny TP, L2CAP...)

10.2.2 Sitzungsprotokoll

Nach dem Request-Response-Paradigama. Eined Sitzung umfasst den Zeitraum, der für eine komplexe Operation benötigt wird.

10.2.2.1 Ablauf

Connect ->
Success <-
Put (Header) ->
Continue <-
While not fertig {
    Put (Body) ->
    Continue <-
}
Put (End of Body) ->
Success <-
Disconnect ->
Success<-

Objekttypen, MIME-Kodierung
Prinzipiell kann Objekte ohne Typinformation übertragen werden, diese werden dann binär gespeichert. Sollen sie verarbeitet werden, muss der Typ

- Über seinen amen (Name Header: „txt“, „gif“...) oder
- Über eine explizite Typangabe (Type Header: nutzt MIME-Typen)

identifiziert werden.

10.2.3 Anwendungsmodell

- Clients initiieren eine Verbindung
- Server reagieen auf die Verbindungen

- Default-OBEX-Server existiert einmal pro Gerät und ist die Anlaufstelle für OBEX-Anfragen
- Inbox speichert ankommende Objekte. Diese können von anderen Geräten gelesen werden
- Eigenschaftsabfragen liefern Informationen über das Gerät zurück
- Gerichtete verbindungen ermöglichen es, objekte gezielt an Anwendungen zu verschicken statt sie in die Inbox zu legen

10.2.4 Authentifizierung

Nach dem Digest-Challenge-Prinzip in beide Richtungen mit MD5.
Nur auf Sitzungsebene über gespeicherte Kennworte. Da es aus der Infrarotkommunikation stammt wurde nicht an eine Übernahme der Sitzung gedacht. Die Annahme stimmt bei Bluetooth nicht mehr.
Asymmetrische Verschlüsselung des Nachrichtenaustausches möglich.

10.3 SyncML

Wurde von verschiedenen Firmen zur Datenübertragung zwischen mobilen Geräten und einem stationären Netzwerk entwickelt, z. B.:

- Synchronisation von Geschäftsdaten zwischen Firma und Außendienstlern
- Synchronisation von PDA-Kalendern mit einem zentralen Kalendern
- Lesen von E-Mails über mobile Endgeräte bei konsistenter zentraler Mailbox
- Synchronisieren von mobil veränderten Dokumenten

Nutzen für

- Endnutzer
- Geräteentwickler
- Anwendungsentwickler,

weil es nur einen Synchronisationsmechanismus zu berücksichtigen gälte.

10.3.1 Architektur

- Synchronisationsprotokoll (SyncML Sync Protocol) für die eigentliche Synchronisation
- Repräsentationsprotokoll (SyncML Representation Protocol) für den Datentransport

Die Initiative zum Datenabgleich geht vom Client aus.

10.3.1.1 Unterstützte Protokolle

- HTTP
- WSP
- OBEX

Evt. zukünftig möglich:

- SMTP, POP3, IMAP
- TCP/IP
- ...

10.3.1.2 Voraussetzungen an die Daten

Satzweise in Datenbanken abgelegt
Eindeutiger Identifikator („Primärschlüssel“)
Eigene Identifikatoren auf Clientseite möglich, Mapping muss dem Server bekannt sein.
Client und Server können Änderungslogs führen

10.3.2 Synchronisationsmodi

Typ	Beschreibung	Initiative
Zwei-Wege-Synchronisation	Gegenseitiger Austausch der Änderungen	Client
Langsame Synchronisation	Gegenseitiger Austausch aller Daten und vergleich aller Felder	Client
Einweg-Synchronisation (Client)	Der Client sendet alle Änderungen an den Server	Client
Erneuerungssynchronisation (Client)	Der Client sendet alle Daten an den Server, dieser überschreibt seine Version	Client
Einweg-Synchronisation (Server)	Der Server sendet alle Änderungen an den Client	Client
Erneuerungssynchronisation (Server)	Der Server sendet alle Daten an den Client, dieser überschreibt seine Version	Client
Serverinitiierte Synchronisation	Der server initiiert eine beliebige Synchronisation	Server

Die Synchronisationsnachrichten werden in XML verschickt.

10.3.3 Konflikte – Lösungsmöglichkeiten

Mischen
Eine Seite gewinnt
Duplizieren
Eine Operation hat Vorrang vor einer anderen
Meldung des Fehlschlags an beide Parteien

10.3.4 Authentifikation im Digest-Challenge-Verfahren

10.4 vCard und vCalendar

- vCard – virtuelle Visitenkarte
- vCalendar – virtueller Terminbucheintrag

11 Plattformen und höhere Dienste

11.1 WAP

Für mobile Einsatzszenarien entworfenes Protokoll, das die Beschränkungen der Geräte berücksichtig:

- Langsame CPUs
- Wenig Speicher
- Geringer Stromverbrauch
- Kleine Anzeigen, keine Grauwerte
- Rudimentäre Eingabemöglichkeiten
- i. d. R. über Mobilfunknetz

Beschreibunssprache ist WML (Wireless Markup Language) mit li mitiertem Sprachumfang.

11.1.1 Protokollstapel

Anwendungsschicht	Wireless Applicatrion Environment
Sitzungsschicht	Wireless Session Protocol
Transaktionsschicht	Wireless Transaction Protocol

Sicherheitsschicht	Wireless Transport Layer Security
Transportschicht	Datagrams (UDP/IP oder WDP)
Netzwerkschicht	Bearers(GRPS SMS SMSCB DECT CDMA IDEN CDPC PDC-P)

11.1.2 Sicherheit über WTLS

11.1.3 WAP-Seiten

Karten und Kartenstapel
Bilder in Schwarzweiß
Hyperlinks
WMLScript als Scriptsprache

11.2 i-Mode

11.2.1 Eigenschaften

- Farbige, animierte Grafiken
- Paketvermittelte Übertragung => Abrechnung nach Volumen
- cHTML als Seitenbeschreibungssprache

11.2.2 cHTML

- Untermenge von HTML
- Nur gif-Bilder
- Keine Tabellen, keine Frames
- Eingeschränkter Satz von Schriftarten und –stilen
- Keine Hintergrundbilder und –farben
- Keine Image Maps

11.3 Coda

Mobiles Netzwerkdateisystem. Mobiltransparent.

11.3.1 Eigenschaften

- Transparenz
- Mehrere gekoppelte Dateiserver, die ihre Bestände untereinander abgleichen
- Clientcache, falls kein Server erreichbar ist. Es können Dateien explizit gecacht werden
- Nach Trennung gleichen Client und Server die Daten automatisch ab.

11.3.2 Konliktbehandlung

- Pessimistiscshe Strategie: nur ein Benutzer darf auf eine Datei zugreifen. Für mobile Clients ungeeignet, nicht in Coda verwendet
- Optimistische Strategie: jeder Client darf ändern. Entstehen Konflikte, müssen sie von Benutzer aufgelöst werden. Es werden Replay Logs geführt.

11.3.3 Zustände

Hoarding
Emulating
Reintegration
Write Disconnect (für schwach angebundene Clients

11.4 Rover

Mobilitätsbewußte Plattform, die nicht die Objekte austauscht, sondern die Änderungsoperation. => Bessee Konfliktbehandlung.

- RDOs – Relocatable Dynamic Objects – lauffähige austauschbare Objekte
- QRPCs – Queued Remote Procedure Calls – Nichtblokierende Fernaufrufe, zur Reaktion werden Callback-Funktionen verwendet

11.5 Quickstep

- Datensatzaustausch zwischen mobilen Geräten reduzierter Fähigkeiten.
- Mobilitätsbewußt.
- Mit zentralem Server.
- Lebenszeitbegrenzung für fremde Datensätze
- Nur der Besitzer darf ändern
- Context Aware