

## **Kapitel 1: Begrifflichkeiten**

Was versteht man unter der Forschungsrichtung Mobile Computing?

Das Forschungsgebiet Mobile Computing befasst sich sowohl mit Fragen der Kommunikation von mobilen Benutzern (Mobilkommunikation), als auch mit mobilen Endgeräten und den dazugehörigen Anwendungen.

Was versteht man unter Ubiquitous Computing?

Allgegenwärtiges Rechnen. Kleine Weltweit vernetzte Systeme, die stationär oder mobil eingesetzt werden können und die überall verfügbar sind.

Was versteht man unter Nomadic Computing?

Nomadic Computing legt den Schwerpunkt auf die Mobilität des Anwenders.

Was versteht man unter Personal Computing?

Mobile Endgeräte werden häufiger als persönlich betrachtet, wie stationäre Endgeräte. Um die persönliche Natur der Verwendung zu betonen spricht man von Personal Computing.

Was versteht man unter tragbare Computer?

Physische Mobilität der Endgeräte.

- Handheld Computing: Computer, die in einer Hand gehalten werden können. (z.B.:Palm)
- Wearable Computing; In Kleidung integrierte Rechner. (z.B. in Armbändern oder Brillen)
- Augmented Reality: Anreicherung der physischen Realität durch zusätzliche Daten. (z.B. Reparaturredateneinblendung in Sichtschirm des Datenhelms des Technikers)

Was versteht man unter Ad-hoc-Vernetzung (spontane Vernetzung)?

Ad-hoc-Vernetzung beschreibt die kurzfristige Verbindung von Geräten ohne aufwendige Konfiguration.

Ad-hoc-Vernetzung im strengen Sinne beschreibt die Verbindung mobiler Endgeräte untereinander, nicht die Verbindung mobiler Rechner mit einem stationären Netzwerk.

Was versteht man unter mobiler Vernetzung?

Im Kurstext werden die Ad-hoc-Vernetzung und die Vernetzung mobiler Rechner mit einem stationären Netzwerk unter dem Begriff mobile Vernetzung zusammengefasst.

Was versteht man unter Embedded Networking?

Einbindung von Geräten der Haushalts-, Unterhaltungs- und Konsumelektronik in Netzwerke. (z.B. Internet tauglicher Kühlschrank)

Was versteht man unter Everyday Computing?

Die Verwendung von mobilen und stationären Computern im Alltag wird als Everyday Computing bezeichnet.

Was versteht man unter Mobilkommunikation (Mobile Communication)?

Bei der Mobilkommunikation liegt der Schwerpunkt auf der reinen Kommunikation, wobei diese sowohl drahtgebunden, als auch drahtlos erfolgen kann.

Was versteht man unter drahtloser Kommunikation?

Drahtlose Kommunikation beschreibt die Art der Anbindung eines mobilen Gerätes über eine Funk- oder Infrarotschnittstelle. Drahtlos angebundene Endgeräte können ohne weiteres stationär betrieben werden.

## Zusammenfassung Mobile Computing (1679)

Welche Arten der Mobilität gibt es?

- Endgerätemobilität: Ein Endgerät bleibt vernetzt auch wenn es räumlich bewegt wird. (z.B. Mobiltelefon)
- Benutzermobilität: Ein Benutzer kann beliebige Endgeräte verwenden um bestimmte Dienste zur Kommunikation zu nutzen. Die Identifizierung gegenüber dem Netzwerk erfolgt über Geheimcode und/oder Chipkarte (z.B. Geldautomatennutzung).
- Dienstmobilität: Der Dienst steht im Mittelpunkt der Betrachtung. Ein Benutzer kann immer auf denselben Dienst zugreifen, ungeachtet von welchem Ort der Dienst genutzt wird. (z.B. E-Mailaccount)

Beispiele für Mobile Computing:

- M-Commerce
  - o Mobile Banking
  - o Mobile Brokering
  - o Mobile Payment
  - o Logistik Routenplanung, zentrale Überwachung der Standorte und Stati der Fahrzeuge
- HPs Cool Town
  - o CoolTown-Museum (elektronischer Museumsführer durch Infrarotbaken gesteuert)

## Kapitel 2: Drahtlose Kommunikation

OSI-Referenzmodell

Anwendungsschicht (Application Layer)		Kommunikation zwischen den Anwendungen
Darstellungsschicht (Presentation Layer)		Darstellung der Übertragungsdaten in einheitlicher Betriebssystem unabhängiger Form.
Kommunikationssteuerungsschicht (Session Layer)		Synchronisation und Flusssteuerung, Verwaltung von logischen Verbindungen
Transportschicht (Transport Layer)	Nachrichten	Entkoppelt die höheren Schichten von Kommunikationsdetails bei der Übertragung von Nachrichten zu fremden Rechnern. Eventuelle Fehler werden behandelt und sind für höhere Schichten nicht sichtbar. Mechanismen zur Flusskontrolle regulieren den Datenstrom.
Vermittlungsschicht (Network Layer)	Pakete	Kommunikation zwischen Rechnern die nicht direkt miteinander verbunden sind. (Routingverfahren)
Sicherungsschicht (Data Link Layer)	Frames	Dienste zur Übertragung und Überprüfung der Daten für eine gesicherte Übertragung: Prüfsummenverfahren CRC (Cyclic Redundancy Check)/ ARQ (Automatic Repeat Request) Den Nutzdaten werden redundante Informationen beigefügt, an hand derer der Empfänger Bitfehler feststellen kann. Der fordert bei festgestelltem Fehler eine erneute Übertragung des Frames über die Sequenznummer an. FEC (Forward Error Correction) Hierbei wird die Prüfsumme so zusammengesetzt, dass der Empfänger begrenzte Bitfehler selber ohne erneute Sendung rekonstruieren kann.
Bitübertragungsschicht (Physical Layer)	Bits	Übertragung einzelner Bits über eine Medium (Kabel oder drahtlos). Festlegung der elektrischen und elektromagnetischen Eigenschaften der Bitübertragung. Definition von Steckern, Verkabelungen und Repräsentation einzelner Bits durch (elektrische) Signale.

## Zusammenfassung Mobile Computing (1679)

TCP/IP existierte schon vor Einführung des OSI-Referenzmodells und ist nicht zum OSI-Referenzmodell kompatibel.

OSI-Referenzmodell	TCP/IP-Referenzmodell
Anwendungsschicht	Anwendungsschicht (FTP, http, SMTP, Telnet, NNTP, DNS, DHCP)
Darstellungsschicht	
Kommunikationssteuerungsschicht	
Transportschicht	Transportschicht (TCP transmission control protocol, UDP user datagram protocol)
Vermittlungsschicht	Internetschicht (IP internet protocol, ICMP internet control message protocol, ARP address resolution protocol, Multicast IP, Mobile IP)
Sicherungsschicht	Netzwerkschicht (SLIP serial line internet protocol, PPP point to point protocol, Ethernet, Token Ring, WLAN)
Bitübertragungsschicht	

Die Bitübertragungsschicht und die Sicherungsschicht des OSI-Modells nach IEEE 802.

Sicherungsschicht (Data Link Layer)	Logical Link Controll (LLC)	802.2 Logical Link Control (3 Arten: unbestätigt/verbindungslos, bestätigt/verbindungslos, verbindungsorientiert)					
	Media Access Controll (MAC) Zugriff auf gemeinsames Medium	802.3 Ethernet	802.4 Token Bus	802.5 Token Ring	802.11 Wireless LAN	802.15 Wireless Personal Area Networks	802.16 Broadband Wireless Metropolitan Area Networks
Bitübertragungsschicht (Physical Layer)	PHY						

### Kategorien der drahtlosen Kommunikation

- Mobiltelefonie (Satellitennetze oder landgestützte zellulare Netze die durch drahtgebundenes Netzwerk verbunden sind.)
- Drahtlose lokale Netze
  - o Ersetzen aufwendige Verkabelung in Gebäuden
  - o Vermeiden fliegende Verkabelung bei nur kurzfristig eingebundenen Geräten
- Wireless Personal Area Networks (WPAN) überbrücken nur einige Meter um traditionelle Verkabelung von Rechnerequipment zu ersetzen (kabellose Mäuse und Tastaturen)
- Satellitennetze decken große Flächen ab. (techn. Anforderungen und Kosten sind hoch)
- Richtfunkstrecken stationäre Datenverbindungen über mehrere Kilometer können Gebäude einer Firma vernetzen ohne, dass Erdarbeiten erforderlich werden.
- Wireless local loop (WLL) Überbrückung der „letzten Meile“ vom Verteilungsknoten zum Haushalt erfolgt drahtlos.
- Fahrerlose Transportsysteme
- Einseitige Übertragung beispielsweise bei Rundfunksystemen
- Bündel- /Betriebsfunk dient der innerbetrieblichen Kommunikation beispielsweise bei Taxis, Bussen, Polizei und Feuerwehr.

Unterschiede zwischen drahtloser und drahtgebundener Kommunikation grob kennen

- Funkkommunikation ist störanfälliger als drahtgebundene Kommunikation
  - o Fehlende Möglichkeit der Abschirmung gegen Störquellen

## Zusammenfassung Mobile Computing (1679)

- Mehrwegeausbreitung, dasselbe Signal gelangt durch Reflexion und Streuung mehrfach zu verschiedenen Zeitpunkten beim Empfänger an.
- Zugriffssteuerung bei Mehrfachzugriff
- Niedrigere Datenraten
  - Geringere Bandbreite der eingesetzten Frequenzbänder zur Datenübertragung
  - Viel mehr Benutzer teilen sich ein Medium
  - Höhere Frequenzen ermöglichen theoretisch höhere Datenraten, jedoch ist die Technik dann erheblich kostenintensiver und störanfälliger. Außerdem wird mehr Energie benötigt.
- Sicherheitsmechanismen erforderlich
  - Abhören ist bei drahtloser Kommunikation nicht vermeidbar, aber die Auswertung der Nutzdaten kann durch Verschlüsselung erschwert werden.
- Hoheitliche Restriktionen müssen beachtet werden
  - Gesperrte Frequenzbänder
  - Reichweitenbegrenzungen
  - Frei verfügbare Frequenzen

## Problemkreise der drahtlosen Kommunikation:

Anwendungsschicht	<ul style="list-style-type: none"> <li>- Übertragung von Daten</li> <li>- Dienstvermittlung</li> <li>- Berücksichtigung der Endgeräte (Energiesparen, Anzeigengröße)</li> </ul>
Transportschicht	<ul style="list-style-type: none"> <li>- Flusskontrolle</li> <li>- Dienstgüte</li> </ul>
Vermittlungsschicht	<ul style="list-style-type: none"> <li>- Handover &amp; Roaming</li> <li>- Ad-hoc-Routing</li> <li>- Geografische Adressierung</li> </ul>
Sicherungsschicht und Bitübertragungsschicht	<ul style="list-style-type: none"> <li>- Bit und Frameübertragung per Funk/Infrarot</li> <li>- Mehrfachzugriff (Regelung)</li> <li>- Sicherheit</li> </ul>

## Verfahren zum Mehrfachnutzung von Funkressourcen:

### Unterscheidung nach Art/Anzahl der Verbindungen:

- Duplex
  - Gemeinsamer Zugriff auf ein Medium durch zwei Kommunikationspartner im Rahmen einer bidirektionalen Verbindung (Frequency bzw. Time Division Duplex FDD/TDD))
- Multipel Access
  - Nutzung des Mediums durch mehrere Sender. (Space, Time, Frequency, Code Division Multiple Access SDMA, TDMA, FDMA, CDMA)

### Unterscheidung nach Art der Aufteilung

- Räummultiplex (SDM Space Division Multiplex)
  - Funksignale verlieren mit Abstand zur Senderquelle an Stärke, so dass in ausreichender Entfernung eine weitere Übertragung über denselben Kanal nicht mehr gestört wird. Deshalb können Funkressourcen bei einer zellularen Aufteilung der Gesamtfläche mehrfach genutzt werden.
  - Des Weiteren können durch Antennen mit Richtungscharakteristik Funksignale so gesteuert werden, dass nur ein schmales Segment der Funkzelle abgedeckt wird. Damit können dieselben Ressourcen innerhalb einer Zelle mehrfach verwendet werden.

- Frequenzmultiplex (FDM Frequenz Division Multiplex)
  - Mehrere Sender verwenden gleichzeitig das Funkmedium, aber jeder nutzt eine andere Frequenz, der Empfänger kann durch einstellen einer bestimmten Frequenz einen speziellen Sender herausfiltern (z.B. Radioprogramm).
  - Innerhalb eines Frequenzbandes benötigt jeder Kanal eine gewisse Breite, zusätzlich müssen zwischen benachbarten Kanälen gewisse Abstände eingehalten werden. Damit kann ein verfügbares Frequenzband nicht in beliebig viele Kanäle geteilt werden.
  - Für einen Duplexkanal zwischen Sender und Empfänger werden im Frequency Division Duplex Verfahren Uplink (mobiles Gerät zur Basisstation) und Downlinkkanal (Basisstation zum mobilen Endgerät) um eine konstante Frequenz gegeneinander verschoben.
  - Frequency Hopping, das Springen zwischen Frequenzen in einer festgelegten Pseudozufallsfolge, soll verhindern, dass durch Störung einer Frequenz ein Endgerät dauernd nicht erreichbar ist.
  
- Zeitmultiplex (TDM Time Division Multiplex)
  - Beim Zeitmultiplex teilen sich mehrere Sender eine Frequenz in dem sie nacheinander das Medium für eine bestimmte Zeit verwenden.
  - Die Zeiträume der Belegung werden Zeitschlitze (Slots) genannt.
  - Um Kollisionen zu vermeiden müssen die Zeitschlitze der Geräte synchronisiert werden
    - Zentrale Synchronisation. Hier gibt es einen ausgezeichneten Sender (Basisstation), der den anderen Sendern Zeitschlitze zum Senden zur Verfügung stellt.
    - Dezentrale Synchronisation. Die beteiligten Stationen handeln die Zeitschlitze untereinander aus. Es gibt keinen „Master“.
  - Wird ein Duplexkanal über Zeitmultiplex genutzt, so spricht man von Time Division Duplex. Hierbei wird Up- und Downlink zeitversetzt das Senderecht eingeräumt.
  
- Codemultiplex (CDM Code Division Multiplex)
  - Gleichzeitige Übertragung von Daten auf einer Frequenz
  - Spezielle Codierung stellt sicher, dass der Empfänger die überlagerten Daten rekonstruieren kann.
  - Schlüsselkomponente des Codemultiplexverfahrens ist der Spreizcode, der jedem Sender zugeordnet wird. Ein Empfänger muss den Spreizcode seines Senders kennen um das empfangene Signal filtern zu können.
  - Der Spreizcode ist die unendliche Aneinanderreihung eines speziellen Codeworts, dessen einzelne Bits als Chips bezeichnet werden.
  - Jedes Bit der Nutzdaten wird zunächst auf die Länge des Codewortes „aufgebläht“ und dann mit dem Codewort multipliziert. (Dazu wird die binäre 0 auf -1 und die binäre 1 auf 1 abgebildet.)
  - Das resultierende Signal wird übertragen. Da bei wird es in der Regel von mehreren anderen Signalen überlagert werden.
  - Das empfangene überlagerte Signal wird jetzt vom Empfänger wiederum mit dem Spreizcode multipliziert.
  - Das Resultat ändert sich noch mit dem Takt des Chips des Spreizcodes und muss noch über die Länge des Codewortes integriert werden, um die ursprünglichen Nutzdaten zu erhalten.
  - Voraussetzungen, damit es so einfach funktioniert:

## Zusammenfassung Mobile Computing (1679)

- Der Empfänger kennt den exakten Beginn des Spreizcodes und ist mit dem Sender synchronisiert, denn ist der Spreizcode nur um ein Bit verschoben, kann das ursprüngliche Signal nicht rekonstruiert werden.
  - Zur Synchronisation kann der Empfänger das Signal abhören und den Spreizcode solange verschieben, bis eine charakteristische Sequenz empfangen wird.
- Rauschen wird ignoriert und die Signalstärke als fest angesehen.
- Die von den verschiedenen Sendern verwendeten Spreizcodes müssen zueinander orthogonal sein. Zwei Vektoren  $x(x_1, x_2, x_3, \dots)$  und  $y(y_1, y_2, y_3, \dots)$  sind orthogonal, wenn das Skalarprodukt gleich null ist, d.h.:  $0 = \sum_{i=1}^n x_i * y_i$
- Sätze von Spreizcodes können über die Walsh Hadamard-Matrix berechnet werden. Die Walsh-Hadamard-Matrizen haben als Dimensionen Zweierpotenzen und sind rekursiv definiert:  $H_1 = [1]$   $H_n = \begin{bmatrix} H_{n/2} & H_{n/2} \\ H_{n/2} & -H_{n/2} \end{bmatrix}$
- Eine Zeile der Walsh-Hadamard-Matrix wird Walsh-Sequenz genannt. Walsh-Sequenzen sind zueinander orthogonal, so dass sie als Spreizcodes in Frage kommen.

## Kapitel 3: Mobiltelefonie

### Mobilfunkgenerationen und ihre Eigenschaften

1.Generation	1958-1977	A-Netz	Analog, handvermittelt (Autotelefone)	Größte Verbreitung 10.000 Nutzer (1970)	150 MHz
	1972-1994	B-Netz	Analog, Selbstwahl, keine automatische Weiterleitung bei verlassen des Bereiches einer Sendestation	27.000 Nutzer (1986)	150 MHz
	1986-2001	C-Netz	Analog, zellular, Weiterleitung laufender Gespräche in anderen Sendebereich (Handover)	800.000 Nutzer (1992)	450 MHz
2.Generation	1992-	D1	Digital GSM900	13 Mio. Nutzer (2000)	900MHz
	1992-	D2		19 Mio. Nutzer (2000)	
	1994-	EPlus	Digital DCS1800 [DigitalCellularSystem] (GSM1800)	5,8 Mio. Nutzer (2000)	1800 MHz
	1998-	O2		3,2 Mio. Nutzer (2000)	
3.Generation			UMTS		

GSM (Global System for Mobile Communication) 900 und 1800 MHz weltweiter Standard nach Vertrag von 1987. Dadurch kann mit einem Dualband-Handy, dass sowohl GSM900 als auch DCS1800 unterstützt dank Roaming Abkommen weltweit telefoniert werden.. Ausnahme sind die USA und Japan, die abweichend 1900 MHz GSM verwenden. Hier ist ein Triband-Handy erforderlich.

### Grundlagen zellularer Mobilfunknetze

- Verhalten elektromagnetischer Wellen
  - Idealisiert breiten sich elektromagnetische Wellen kugelförmig um einen Sender aus.

## Zusammenfassung Mobile Computing (1679)

- Die Wirkung elektromagnetischer Wellen reduziert sich mit dem Quadrat des Abstandes, d.h. verdoppelt man den Abstand von Sender und Empfänger reduziert sich die Wirkung der Wellen auf ein Viertel.
- In realen Umgebungen kommt es zu vielfältigen Abweichungen von diesem Ideal, durch Gebäude und Geländeformen, sowie elektromagnetische Störquellen nimmt die Wirkung von elektromagnetischen Wellen mit der 4. Potenz ab, d.h. verdoppelt sich die Entfernung von Sender und Empfänger sinkt die Sendeleistung um das 16fache.
- Isolation von Kanälen
  - Die elektromagnetischen Wellen von verschiedenen Transmissionen überlagern sich beim Empfänger.
  - Eine einfache Isolation durch die Verwendung mehrere Leitungen, wie es in drahtgebundenen Netzen üblich ist, ist bei drahtlosen Netzen nicht möglich.
  - Die Trennung erfolgt deshalb über den Einsatz von Raum-, Zeit-, Frequenz- oder Code-Multiplexverfahren ggf. in Kombination.
- Die begrenzte Reichweite elektromagnetischer Wellen führt zum Konzept der zellularen Netze.
  - Die Fläche auf der sich potentielle Mobilfunkteilnehmer befinden, wird durch ein Netz von Zellen abgedeckt.
  - Jede Zelle deckt einen bestimmten Bereich ab und enthält eine Stationäre Basisstation (Sende-/Empfangsstation)
  - In den Übergangsbereichen zwischen zwei Zellen kommt es zu Überlappungen, d.h. ein Teilnehmer befindet sich im Bereich von 2 oder mehr Basisstationen.
  - Vorteile:
    - Die Distanz die das mobile Endgerät zur nächsten Basisstation überbrücken muss ist relativ gering (D-Netz max. 35km im E-Netz max. 8 km)
    - Zellen die einen gewissen Abstand haben können dieselben Frequenzen benutzen ohne sich gegenseitig zu stören.
  - Nachteil:
    - Es müssen entsprechend viele Basisstationen errichtet und miteinander vernetzt werden, was hohe Kosten verursacht.
- Zur Planung Abdeckung der Fläche mit identischen Clustern aus „idealisierte“ identisch großen 6 eckigen Zellen. Dabei gilt:
  - $F_{Ges}$  ist die Menge aller Frequenzen, die einem Mobilfunkbetreiber zugeordnet sind.
  - $F_i \subseteq F_{Ges}$  paarweise verschieden für alle  $i$  aus  $\{1,2,\dots,k\}$ , wobei  $k$  die Anzahl der Zellen pro Cluster wiedergibt, so dass die Vereinigungsmenge aller  $F_i$   $F_{Ges}$  entspricht.
  - Der Abstand  $D$  zweier Basisstationen derselben Frequenz wird berechnet mit  $D = R\sqrt{3*k}$ , wobei  $k$  die Anzahl der Zellen im Cluster und  $R$  den Radius der Zellen wieder gibt.
  - Der Abstand zwischen zwei Basisstationen muss dabei hinreichend groß sein, damit Störungen minimiert werden.
  - Je größer der Abstand, desto kleiner die Anzahl der Frequenzen, die auf eine einzelne Basisstation entfallen.
  - Im GSM-Netz wird eine Clustergröße von 7 Zellen verwendet.

## Architektur und Eigenschaften von GSM-Netzen (Global System for mobile Communication)

- Grundstein der Entwicklung von GSM war 1982 die Groupe Special de Mobile, die einen europäischen digitalen Mobilfunkstandard entwickeln sollte. Diese Gruppe wurde 1989 von der European Telecommunication Standards Institute als Technical Comitee aufgenommen.

## Zusammenfassung Mobile Computing (1679)

- GSM wurde so ausgelegt, dass viele Millionen Kunden pro Netzwerk versorgt werden können.
- Mehrere Mobilfunkanbieter können die gleiche Fläche abdecken ohne sich gegenseitig zu stören.
- Eine Vollständige Flächenabdeckung je Netz wird angestrebt. Diese ermöglicht es den Teilnehmern überall innerhalb eines Landes mobil zu telefonieren.
- Die Bewegung des Teilnehmers von einer Mobilfunkzelle in eine andere wird auch während einer laufenden Verbindung ohne Unterbrechung durch Handover sichergestellt.
- Durch Roamingabkommen der Mobilfunkbetreiber unterschiedlicher Länder, bleibt der Teilnehmer auch im Ausland unter seiner gewohnten Rufnummer erreichbar.
- Neben den Sprachdiensten werden auch Dienste zur Übertragung von Textnachrichten (SMS = Short Message Service) und spezialisierte Webprotokolle (WAP Wireless Application Protocol) die es ermöglichen Informationsseiten ähnlich Internetangeboten auf dem Handy darzustellen angeboten.
- Das GSM-Netzwerk besteht aus 3 Subsystemen:
  - o Betriebssystem (OMSS= Operation and Maintenance System)
    - Dient der Administration und Kontrolle des Netzwerks
    - Die Kontrolle erfolgt über das Operation and Maintenance Center (OMC)
    - Verwaltung der Geschäftsrelevanten Daten (Kundendaten, Endgeräte, Gebühren, Statistik)
    - Sicherheitsmanagement
    - Netzwerkkonfiguration
    - Vertrauliche Daten über Kunden und Schlüssel sind im Authentication Center (AUC) gespeichert, sie dienen dazu Kunden zu identifizieren und registrierte Dienste freizuschalten.
    - Im Equipment Identity Register (EIR) werden die Seriennummern (IMEI) der Endgeräte gespeichert
      - White List enthält die Gerätenummern der registrierten Geräte
      - Black List enthält die Gerätenummern der Geräte die nicht mehr betrieben werden sollen (verloren, gestohlen). Sie wird zwischen den Netzbetreibern ausgetauscht
      - Gray List (optional) speichert Nummern von Geräten, die zwar operabel sind, deren Software oder Ausstattung jedoch veraltet ist oder Fehlfunktionen aufweist.
  - o Vermittlungssystem (SMSS = Mobile Switching and Management System)
    - Vermittelt die Nutzdaten innerhalb des Netzes und stellt eine Anbindung anderer Netze zur Verfügung
    - Kern sind die Mobile Switching Center (MSC), die jeweils mehrere BSC verwalten.
    - Pro Netzwerk können dabei mehrere MSC existieren, die jeweils sogenannte Service Areas verwalten.
    - Der MSC wickelt den Netzverkehr zwischen den Funksubsystemen ab und vermittelt Verbindungen zu externen Netzen über das Gateway Mobile Switching Center (GMSC) bzw. für internationale Gespräche über das International Switching Center (ISC).
      - MSRN (Mobile Station Roaming Number) wird vergeben, wenn der Benutzer in ein fremdes Netz wechselt. Diese Nummer ist für Anrufer und Angerufenen transparent und dient nur der technischen Abwicklung zwischen den Netzbetreibern.
    - Darüber hinaus ist der MSC für die Lokalisierung der Benutzer über 2 Datenregister zuständig:
      - Home Location Register (HLR)

## Zusammenfassung Mobile Computing (1679)

- Daten von Teilnehmern, die sich im aktuell im Zuständigkeits Bereich des MSC befinden.
- Einträge werden nur temporär vorgenommen, verlässt ein Kunde die Service Area werden die Daten gelöscht.
- Neben eigenen Kunden können auch Kunden fremder Netze (z.B. im Rahmen Roaming) in das Register aufgenommen werden.
- MSISDN (Mobile Subscriber ISDN) eigentliche Telefonnummer des mobilen Gerätes
  - 3 Ziffern Nationalcode (049)
  - 2-3 Ziffern Code des Mobilfunkbetreibers (171,172,..)
  - max. 10 Ziffern Anschlussnummer
- Visitors Location Register (VLR)
  - Daten von Teilnehmern, die sich im aktuell im Zuständigkeits Bereich des MSC befinden.
  - Einträge werden nur temporär vorgenommen, verlässt ein Kunde die Service Area werden die Daten gelöscht.
  - Neben eigenen Kunden können auch Kunden fremder Netze (z.B. im Rahmen Roaming) in das Register aufgenommen werden
- Funk subsystem (BSS = Base Station Subsystem)
  - Bindet die Mobilfunkteilnehmer an das Netzwerk an
  - Die Kommunikation zwischen Endgerät und GSM-Netzwerk erfolgt über Base Transceiver Stations (BTS).
  - Je Funkzelle existiert eine BTS.
    - LAI (Location Area Identity) und CI (Cell Identifier) identifizieren international eindeutig jede Zelle.
    - LAI und CI werden von der Basisstation permanent gesendet, so dass jedes Endgerät weiß, wo es sich gerade befindet.
  - Mehrere BTS werden von einem Base Station Controller (BSC) kontrolliert,
  - Das BTS beherbergt:
    - das eigentlichen Sende- und Empfangssystem
    - Protokollarbeit zur Datenübertragung über die Funkschnittstelle
  - Die eigentliche Datenverarbeitung erfolgt im Base Station Controller
    - Die BSC sind auch für das Handover eines Teilnehmers in eine andere Zelle verantwortlich
  - Der Datenverkehr innerhalb des GSM-Netzes wird mit Ausnahme des Kontaktes BTS-Endgerät in der Regel leitungsgebunden über Glasfaser oder Richtfunkstrecken abgewickelt.
- Adressierung von Geräten und Benutzern:
  - GSM unterscheidet Endgeräte und Benutzer bei der Identifizierung
  - Benutzer werden an Hand ihrer SIM (Subscriber Identity Modul) identifiziert, auf der folgende Informationen gespeichert sind:
    - PIN (optional)
    - Daten der persönlichen Konfiguration (Telefonnummern)
    - Eingetroffene aber noch nicht gelöschte SMS-Nachrichten
    - Technischen Daten des Mobilfunkbetreibers (Frequenzen)
    - IMSI (International Mobile Subscriber Identity) weltweit eindeutige Nummer, die den Benutzer auch in fremden Netzen identifiziert. (Nicht zu verwechseln mit der Rufnummer des Anschlusses! = MSISDN)

## Zusammenfassung Mobile Computing (1679)

- Die IMSI ist in der Home Location Register Datenbank gespeichert
- TMSI (Temporary Mobile Subscriber Identity) Um die Identität des Benutzers zu schützen, wird in der Kommunikation zwischen Netz und Benutzer nicht die IMSI verwendet, sondern regelmäßig eine neue TMSI ausgehandelt und gespeichert.
- Endgeräte werden über eine weltweit eindeutige IMEI (International Mobile Station Equipment Identity) identifiziert. Die IMEI ist in der Equipment Identity Register Datenbank gespeichert:
- Die Luftschnittstelle
  - GSM verwendet eine Kombination aus Frequenz Division Multiple Access (FDMA) und Time Division Multiple Access (TDMA), sowie Space Division Multiple Access (SDMA), da ein zellulares Netz vorliegt.
  - Vom Endgerät zur Basisstation (Uplink) wird das Frequenzband 890-915 MHz genutzt
  - Von der Basisstation zum Endgerät (Downlink) das Frequenzband 935-960 MHz
  - Jedes Band wird in 124 Kanäle à 200 kHz aufgeteilt und von 1 – 124 durchnummeriert.
  - Für die Bidirektionale Kommunikation werden jeweils die Kanäle mit der gleichen Kanalnummer genutzt, die immer um 45 MHz gegeneinander verschoben sind.
  - Die beiden freien Bänder von je 100 kHz am Ende der Frequenzbänder dienen dem Sicherheitsabstand zu anderen Diensten.
  - Analog wird im DCS1800 (GSM1800) eine Aufteilung in 372 Kanäle auf die Frequenzbänder 1710-1785 MHz und 1805-1880 MHz abgebildet.
  - Durch Frequenzhopping wird vermieden, dass eine Störung auf einer Frequenz über einen längeren Zeitraum die Verbindung eines bestimmten Endgerätes zur Basisstation stört.
  - Die 124 GSM-Kanäle teilen sich in Deutschland D1 und D2 mit je 57 Kanälen.
  - Davon bekommt jede Basisstation eines Mobilfunkbetreibers jeweils rund 1/7 zugeordnet, d.h. ca. 8 Frequenzen je Basisstation
  - Damit trotz der beschränkten Frequenzanzahl möglichst viele Teilnehmer telefonieren können, werden die Kanäle jeweils in 8 sich zyklisch wiederholende Zeitschlitze von je 0,5ms Dauer (Burst Periode BP) aufgeteilt.
  - Ein bestimmtes Endgerät benutzt immer nur Zeitschlitze mit der selben Nummer für die Übertragung.
  - Die Zeitschlitze für Up- und Downlink sind gegeneinander um 3 BP verschoben, damit kein mobiles Endgerät gleichzeitig senden und empfangen muss.
  - Innerhalb einer Burst Periode wird ein sogenannter Burst gesendet.
    - Normal Bursts dienen der Datenübertragung
    - Frequency Correction Bursts dienen dem mobilen Endgerät zur Frequenzkorrektur
    - Synchronisation Burst dienen der zeitlichen Synchronisation zwischen Endgerät und Basisstation
    - Dummy Bursts werden gesendet, wenn weder Nutz- noch Verwaltungsdaten anstehen
    - Access Bursts Zugriff des mobilen Endgerätes auf die Basisstation ohne vorherige Anmeldung
  - Ein Burst enthält 114 Bit Nutzdaten aufgeteilt in zwei Sequenzen à 57 Bit.
  - Theoretische Obergrenze 24.700 Bit/s praktisch werden jedoch nur 13.000 Bit/s für die Sprach und 9.600 Bit/s für die Datenübertragung erreicht.
- Handover und Roaming
  - Bewegt sich ein Teilnehmer von einer Zelle zur Anderen bzw. wird die Signalqualität aus anderen Gründen zu schlecht, muss die Verbindung neu konfiguriert werden (Handover)

## Zusammenfassung Mobile Computing (1679)

- Intracell Handover: Aus Gründen der Signalqualität wird innerhalb einer Zelle auf eine neue Frequenz umgeschaltet
- Intercell Handover: Umschaltung der Kommunikationsverbindung durch das Vermittlungssystem auf eine neue Basisstation. Gleichzeitig wird vom mobilen Endgerät die Frequenz gewechselt.
  - Internes Handover: Die beteiligten Basisstationen werden vom gleichen Basis Station Controller (BSC) verwaltet.
  - Externe Handover: Die beteiligten Basisstationen werden von unterschiedlichen BSC verwaltet.
- Unabhängig von der Verlagerung der Verbindung behält ein einmal zuständiges Mobile Switching Center (MSC) die Kontrolle über die Verbindung als sogenannter Anker-MSC. Die Verbindung wird lediglich logisch in den Bereich des anderen MSC erweitert.
- Network-originated Handover: Der Handover wird vom Funksystem initiiert, damit kann der Handover-algorithmus geändert werden, ohne das die Endgeräte angepasst werden müssen.
- Entscheidung zum Handover:
  - Empfangspegel sinkt unter einen gegebenen Schwellenwert
  - Bitfehlerhäufigkeit steigt über einen gegebenen Schwellenwert
  - Maximale Entfernung zwischen Endgerät und Basisstation ist erreicht
- Roaming
  - Eigenschaft des Mobilfunknetzes, die es ermöglicht einen Teilnehmer an beliebigen Orten anzurufen, ohne das dieser explizit seinen Aufenthaltsort hinterlegt. Der Aufenthaltsort wird vom Netz automatisch bestimmt.
  - Nutzung fremder Netze mit denen kein Vertrag vorliegt, wenn die Mobilfunkanbieter ein Roaming-Abkommen unterzeichnet haben. (Ermöglicht telefonieren im Ausland)
- Es werden 4 Klassen von Endgeräten unterschieden:
  - Autotelefone mit 20 W
  - Tragbare Geräte mit 8 W
  - Handgeräte mit 5 W
  - Handgeräte mit 2 W
- Weiterentwicklungen von GSM (Phase 2+)
  - High Speed Circuit Switched Device (HSCSD)
    - leitungsvermittelter Verfahren der Nutzer zahlt auch dann, wenn keine Daten übertragen werden.
    - Verbesserte Kodierungsverfahren ermöglichen 14.400 Bit/s Datenraten auf einem Kanal
    - Durch Bündelung von Kanälen kann die Datenrate vervielfacht werden. (theoretisch bis 115.2 kBit/s bei 8 Kanälen)
    - Bündelung muss nicht symmetrisch erfolgen, d.h. es können mehr Empfangs- als Sendekanäle gebündelt werden.
    - Neue Endgeräte erforderlich, während die Änderungen am GSM-Netzwerk gering sind.
  - General Packet Radio Service (GPRS)
    - Paketvermittelter Verfahren, nur wenn Datenpakete ausgetauscht werden, wird die Infrastruktur belastet, so dass nur während der eigentlichen Datenübertragung Kosten anfallen.
    - Besser Ausnutzung der Kapazitäten bei schwankendem Kommunikationsbedarf
    - Theoretisch Datenraten bis 171,2 kBit/s bei Bündelung von 8 Funkkanälen und optimaler Empfangsqualität

## Zusammenfassung Mobile Computing (1679)

- Neue Endgeräte und erhebliche Änderungen am bestehenden GSM-Netz erforderlich, da dieses für leitungsvermittelte Kommunikation ausgelegt ist.
- GPRS-Endgeräte werden eingeteilt:
  - Klasse A; Unterstützt den zeitgleichen Transfer von Daten und Sprache via GPRS und GSM
  - Klasse B: Keine zeitgleiche Unterstützung von Daten und Sprachübertragung. Während eines Gespräches werden keine GPRS-Pakete versandt/empfangen und während einer Datenübertragung werden GSM-Anrufe nur gemeldet.
  - Klasse C: Endgeräte müssen manuell in den Sprach- bzw. Datenmodus geschaltet werden.
- Multislot-Klassen geben an, wie viele Funkkanäle gleichzeitig für Up- bzw. Downlink genutzt werden können.
- Enhanced Data Rates for GSM Evolution (EDGE)
  - Durch ein geändertes Modulationsverfahren werden pro Takt 3 Bit statt 1 Bit bei GSM übertragen.
  - Zusätzliche Korrekturverfahren ermöglichen pro Kanal max. 59,2 kBit/s als Datenrate bei 8 Kanalbündelung also 473,6 kBit/s
  - Steigt die Fehlerrate über ein bestimmtes Maß wird auf das alte Modulationsverfahren zurückgeschaltet.
  - EDGE kann mit HSCSD und GPRS kombiniert werden. (ECSD bzw. EGRPS)
  - EDGE gilt als sanfter Übergang zur 3. Mobilfunkgeneration (UMTS)
  - Es sind allerdings sowohl bei den Endgeräten, als auch bei den Basisstationen umfangreiche Änderungen erforderlich.

## Universal Mobile Telecommunications System (UMTS)

- Verschiedene Varianten des Funkzugangs sollen möglich sein. (Idealerweise mit nahtlosem Übergang)
  - Schnurlostechnologie
  - Zellularer Mobilfunk
  - Satellitentechnik
- Nicht nur Sprachübertragung, sondern auch Datenübertragung und Internetzugriff sollen möglich sein auch Multimedia soll mit Datenübertragungsraten von bis zu 2MBit/s möglich sein.
- Verbindungen sollen konfigurierbar sein:
  - Dienstgüteklassen
    - Conversational:
      - Höchste Anforderungen an die Datenübertragung.
      - Für Sprachverbindungen gedacht
      - Anwendungen mit hohen Bandbreitenanforderungen wie Videokonferenzen
      - Niedrige Verzögerung bei der Datenübertragung
    - Streaming
      - Einwegkommunikation
      - Bandbreite und zeitliche Konstanz des Datenflusses muss gewährleistet sein.
      - Streaming Video oder Streaming Audio
    - Interactive
      - Anwendungen des Internets oder Datenbankanwendungen
      - Benutzer verschickt Anfrage oder Kommando
      - Bekommt Ergebnis zugeschickt
      - Niedrige Verzögerung und niedrige Fehlerrate

## Zusammenfassung Mobile Computing (1679)

- Background
  - Integrität der Nutzdaten ist gewährleistet
  - Keine Garantien für die Übertragungszeit
  - Für Download großer Dateien oder Versenden von E-Mails
- Paket- oder leitungsvermittelte Übertragung
- Unterstützung Asymmetrischer Datenverkehr
- Zugang zu weiteren Netzwerken, wie ISDN oder TCP/IP soll möglich sein.
- Virtuell Home Environment (VHE) soll es dem Nutzer ermöglichen immer auf dieselben Dienste zugreifen zu können
- Roaming und Handover soll zwischen verschiedenen Anbietern und vor allem auch mit Mobilfunksystemen der 2. Generation (GSM) funktionieren.
- Zellengrößen und Übertragungsraten:
  - Pikozone (50 m) innerhalb von Gebäuden Datenraten bis 2 MBit/s möglich [Hot Spots]
  - Mikrozellen (bis zu einigen km) decken Vorstädte oder Bereiche von Städten ab. Datenraten bis 384 kBit/s
  - Makrozellen (bis zu einigen 10km) in ländlichen Gebieten bieten Datenraten bis 144kBit/s
  - Satellitenzellen können noch größere Bereiche abdecken. Datenraten zwischen 144 und 384 kBit/s können erreicht werden.
- Schnittstellen:
  - UTRA FDD (UMTS-Terrestrial Radio Access Frequency Division Duplex)
    - 1920-1980 MHz für Uplink und 2110-2170 MHz für Downlink
    - 12 Duplexkanäle a 5 MHz die um 190 MHz für Up- und Downlink gegeneinander verschoben sind.
    - Spezielle Form der Codespreizung Wideband Code Division Multiple Access WCDMA) als Modulationsverfahren
  - UTRA TDD (UMTS-Terrestrial Radio Access Time Division Duplex)
    - Verwendung derselben Frequenzen pro Kanal für Up- und Downlink
    - Für die jeweilige Richtung sind unterschiedliche Zeitschlitze vorgesehen
    - Für Deutschland stehen 5 Kanäle a 5 MHz zur Verfügung
- UMTS-Referenzarchitektur
  - Trennung zwischen User Equipment und Infrastruktur Domain
  - Verbindung über Referenzpunkt Uu
  - User Equipment Domain
    - Mobile Equipment (Endgeräte)
    - User Service Identity Modul (USIM) verwaltet Informationen über den Benutzer und ist auf einer Chipkarte untergebracht
  - Infrastruktur Domain
    - Gesamtes Netzwerk inkl. Luftschnittstelle
    - Access Network Zugang der Benutzer zum Trägernetzwerk (im terrestrischen Netzwerk durch die UTRAN repräsentiert)
    - Core Network alle Entitäten die zum Betrieb des UMTS-Netzwerks gehören
      - Serving Network Domain ortsabhängige Funktionen und paket-/leitungsvermittelte Übertragung
      - Home Network Domain Dienste die nicht vom aktuellen Aufenthaltsort abhängig sind (Dienste der Service Provider)
      - Transit Network Domain Dienste zur Kommunikation mit anderen Netzwerken
- Umstellungsaufwand ist hoch
- Vereinheitlichung des Mobilfunkmarktes wird durch UMTS nicht kommen, da mehrere Funkzugänge durch die IMT-2000 beschlossen wurden.

## Zusammenfassung Mobile Computing (1679)

- Multiband-Mobilfunk-Telefone werden erforderlich sein

## Digital Enhances Cordless Telecommunications (DECT)

- drahtlose Anbindung von Telefonen mit einem geringen Abstand zur Basisstation (Schnurlos Telefone)
- DECT kann nahtlos mit GSM eingesetzt werden (Genion O2)
- DECT ist einer der 5 Luftschnittstellenstandards für die 3. Mobilfunkgeneration.
- Unterteilung der Infrastruktur in Fixed Radio Termination (Basisstationen [Radio Fixed Part]) und eine Portable Radio Termination (mobiles Endgerät [Portable Part PP]).
- Einfachster Fall eine Basisstation die an das Festnetz angeschlossen ist unterstützt 1-x Endgeräte.
- Reichweite ist in Gebäuden auf ca. 50m und im freien auf ca. 300m beschränkt.
- Die Reichweite kann durch Einsatz von zusätzlichen Basisstationen erweitert werden, die über eine Central control Fixed Part (CCFP)-Station miteinander verbunden werden.
- Direkte Kommunikation zwischen zwei Endgeräte ist theoretisch auch ohne Basisstation möglich, wird von den aktuellen Endgeräte aber nicht unterstützt.
- Frequenzband 1880-1900MHz. Eingeteilt in 10 Kanäle a 1728kHz
- Jeder Kanal ist über Time Division Multiple Access Verfahren in 24 logische Kanäle eingeteilt.
- Framedauer 10 ms bei einer Datenrate von 1,152 MBit/s, damit stehen je Kanal 46 kBit/s zur Verfügung
- Üblicherweise erfolgt eine paarweise Nutzung der Kanäle, damit können auf einer Frequenz bis zu 12 Duplexkanäle eingerichtet werden. Damit sind insgesamt 120 Vollduplexkanäle möglich.
- Basisstationen suchen sich selber automatisch freie Kanäle aus, so dass in einem Wohnhaus problemlos verschiedene Basisstationen betrieben werden können.
- DECT ist nicht auf die Übertragung von Sprachdaten eingeschränkt.

## KAPITEL 4: drahtlose Netze

### Vor- und Nachteile drahtloser Netze

- Vorteile
  - o Kostenfaktor Netzwerkverkabelung entfällt
  - o Keine aufwendigen Änderungen der Netzwerkverkabelung in Gebäuden bei Ausbau des Netzwerkes erforderlich
  - o Verlegen von Kabeln ist in einigen Gebäuden schwierig (massive Wände) bis unmöglich (Denkmalschutz)
  - o Anschluss auch außerhalb von Gebäuden möglich
  - o Vernetzung von Gebäuden miteinander ohne Erdverkabelungsarbeiten
  - o Keine fliegenden verkabelten Rechner bei Einsatz von mobilen Rechnern
- Nachteile
  - o Geringere Bandbreite und höhere Fehlerrate als drahtgebundene Netze
  - o Nationale Restriktionen bei Verwendung des Funkmediums
  - o Leichte Abhörbarkeit, deshalb Mechanismen zur Verschlüsselung und Authentifizierung erforderlich
  - o Hardware für die Funkschnittstelle ist teurer, als die Hardware für drahtgebundene Netze
  - o Funkübertragung erfordert ein erhebliches Maß an Batteriestrom
  - o Abstrahlung von Funksignalen kann andere Systeme stören und evtl. bei Menschen zu gesundheitlichen Problemen führen

### Wichtige Anwendungsgebiete

- Einsatz in Messehallen für kurzfristigen Demonstrationsaufbau
- Unterstützung bei Katastropheneinsätzen zum Ersatz der zerstörten Infrastruktur

## Zusammenfassung Mobile Computing (1679)

- Mobilität von Diagnosegeräten z.B. in Krankenhäusern
- Mobile Transporteinheiten im Produktionsbereich

Überblick über die Standards drahtloser Netze inkl. Berücksichtigung der Eigenschaften der Funkkommunikation

- Wireless Local Area Network (WLAN)
  - o Sammelbegriff für drahtlose lokale Netzwerke
  - o Drahtlose Netze, die auf dem Standard 802.11 aufgebaut sind.

IEEE 802.11 beschreiben können

- Datenraten von 2MBit/s in 802.11.
- Erweiterungen in 802.11a (max. 54 MBit/s) und 802.11b (max. 11MBit/s)
- Protokollarchitektur 802.11 und Einbindung in 802.x:

Sicherungsschicht (Data Link Layer)	LLC	802.2 Logical Link Control		
	MAC	802.11 Media Access Control (MAC)		
Bitübertragungsschicht (Physical Layer)	PHY	802.11 Physical Layer Convergence Protocol (PLCP)		
		802.11 Infrarot (Physical Medium Depended PMD)	802.11 Frequency Hopping Spread Spectrum (PMD FHSS)	802.11 Direct Sequenz Spread Spectrum (PMD DSSS)

- Dabei bietet die Physical Layer Convergence Protocol Schicht einen einheitlichen Zugriff auf die Bitübertragungsschicht unabhängig vom vorhandenen Datenübertragungsmedium
- Betriebsmodi:
  - o Infrastrukturmodus
    - Anbindung mobiler Rechner erfolgt über feste Basisstationen (Access Points), die sowohl über eine drahtgebundene Anbindung, als auch eine drahtlose Anbindung verfügen und somit den mobilen Rechnern einen Zugang zum drahtgebundenen Netzwerk gewähren.
    - Das drahtgebundene Medium dient auch den Access Points untereinander zum Informationsaustausch, z.B. wenn mobile Geräte zwischen Funkzellen wandern.
    - Access Point kann zentrale Funktionen zur Koordination anbieten
      - Synchronisation der Uhren
      - Powermanagement
  - o Ad Hoc Modus:
    - Mobile Rechner werden untereinander verbunden
    - Keine Anbindung an ein festes Netz
    - Wird kein spezielles Protokoll eingesetzt, können nur Stationen miteinander kommunizieren, die sich in gegenseitiger Kommunikationsreichweite befinden.
    - Alle Stationen sind gleichberechtigt es gibt keine ausgezeichnete Station die Sonderaufgaben übernimmt.
- Service Sets
  - o Basic Service Set (BSS) zwei oder mehr Rechner werden miteinander verbunden, davon kann einer ein Access Point sein.
  - o Independent Basic Service Set (IBSS) einfachstes Basic Service Set aus zwei oder mehr Rechnern, die im Ad Hoc Modus miteinander verbunden sind.
  - o Extended Service Set (ESS) Verbindung mehrerer BSS zu einem System.
    - Die Access Points der beteiligten BSS werden hierzu über eine Distribution System (DS) miteinander verbunden.
    - Voraussetzung für automatischen Zellenwechsel mobiler Stationen (Roaming)
  - o Portal stellt die Verbindung zu weiteren Netzwerken dar.
    - Logische Komponente oder konkretes Gerät (z.B. kann Access Point Zugriff auf stationäres Netzwerk ermöglichen)

## Zusammenfassung Mobile Computing (1679)

- Bitübertragungsschicht
  - Größter Unterschied zu drahtgebundenen Netzwerken besonders wegen der hohen Fehlerrate der Luftschnittstelle
  - Fehlerursachen:
    - Rauschen und Interferenzen
    - Funksignale von anderen WLAN Stationen die mit der Übertragung kollidieren
    - Funksignale von Netzwerken mit gleicher Frequenz wie WLAN z.B. Bluetooth oder HomeRF
    - Störsignale von Geräten, die eigentlich nicht für die Funkübertragung vorgesehen sind (Mikrowellenherde)
  - Standard
    - Infrarotübertragung
    - Funkübertragung
      - Frequenzband 2400-2483,5 MHz (Industrial Science Medical (ISM)-Band) [genau genommen gibt es noch 2 weitere ISM-Bänder um 900 MHz und 5GHz es ist jedoch in der Regel das 2,4GHz Band gemeint.
      - Reichweite
        - In Gebäuden ca. 30 m
        - Außerhalb von Gebäuden ca. 300 m
      - Übertragungsverfahren:
        - Frequency Hopping Spread Spectrum (FHSS)
          - Das verfügbare Frequenzspektrum wird in 79 Kanäle a 1 MHz aufgeteilt
          - Die Frequenzen werden mindestens 2,5mal pro Sekunde nach einer Pseudo-Zufallsfolge gewechselt.
          - Datenrahmen:
            - 96 Bit Präambel
              - Synchronisation (80Bit)
              - Start Frame Delimiter (SFD) (16Bit)
            - 32 Bit Header
              - Länge des Datenfeldes (12Bit)
              - Datenrate der Nutzlast (4Bit)
              - CRC-Prüfsumme für den Header (16Bit)
            - Nutzlast (0-4095 Bit)
            - Präambel und Header werden grundsätzlich mit 1 MBit/s übertragen, während für die Nutzlast 1 und 2MBit/s möglich sind
        - Direct Sequence Spread Spectrum (DSSS)
          - Basiert auf einer Bandspreizung nach dem Code Division Multiple Access (CDMA)-Verfahren
          - Bessere Ausnutzung des Frequenzbandes als bei FHSS
          - Relativ unempfindlich gegen Störungen
          - 14 Kanäle im ISM-Band
          - Datenrahmen:
            - Präambel
              - Synchronisation (128Bit)
              - Start Frame Delimiter (16Bit)
            - Header
              - Signal (8 Bit) [Datenrate Nutzlast]

- Dienst (8Bit) reserviert für zukünftige Verwendung
  - Länge des Datenfeldes (16Bit)
  - CRC-Prüfsumme (16Bit)
  - Nutzlast (0-4095 Bit)
- Media Access Controll (MAC)- Schicht
  - Regelt den Zugriff auf das Funkmedium
  - Senden 2 oder mehr Stationen gleichzeitig, so können die Daten von den Empfängern nicht mehr gelesen werden, sie gehen verloren
  - Möglichkeiten der Kollisionsbehandlung
    - Verhinderung von Kollisionen bzw. Reduzierung der Wahrscheinlichkeit von Kollisionen
    - Mechanismen zur Kollisionsbehandlung werden integriert
  - Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) verringert Kollisionswahrscheinlichkeit zusätzlich wird durch Quittungsverfahren erreicht, dass im Falle von Kollisionen Nutzdaten nicht unerkannt verloren gehen.
    - Distributed Coordination Function /DCF
      - Einfaches CSMA/CA (verbindlich)
        - Sendewillige Station hört für eine Wartezeit, die sich aus einer konstanten Wartezeit und einer zufallsabhängigen Wartezeit zusammensetzt, das Medium ab.
          - Findet eine Sendung statt, wird bis zum Ende der Belegung unterbrochen. Danach beginnt zunächst wieder die feste Wartezeit die mit der reduzierten Zufallswartezeit verlängert wird (Backoff)
          - Ist das Medium frei, wird gesendet.
        - Konstante Wartezeiten (Interframe Spaces)
          - Distributed Control Function Interframe Space (DIFS) bevor Sendung
          - SIFS (Short Interframe Space) vor senden der Empfangsbestätigung (ohne zusätzliche Zufallswartezeit).Kürzer als DIFS. Dadurch automatisch priorisiert.
        - Zufallsabhängige Wartezeit, wird aus einem ganzzahligen Zufallswert multipliziert mit einem konstanten Zeitfaktor berechnet.
          - Contention Window Zeit die bei maximaler Zufallszahl gewartet wird.
            - Große Contention Window geringe Kollisionswahrscheinlichkeit jedoch geringer Datendurchsatz
            - Kleine Contention Window höhere Kollisionswahrscheinlichkeit, aber höherer Datendurchsatz
            - Optimale Contention Window Größe wird über Exponential Backoff ermittelt.
              - Mögliche Contention Window Größen: 7,15, 31,63, 127, 255
              - Es wird bei 7 begonnen, kommt es zu Fehlern wird die Größe des Contention Window schrittweise erhöht, bis das Maximum erreicht ist.

- Empfangene Nachrichten werden mit ACK Signal bestätigt, für das nur SIFS abgewartet werden muss..
- Ursachen für ausbleibende Quittungen:
  - Nachricht ging durch Kollision verloren
  - Quittung ging durch Kollision verloren
- Bei fehlender Quittung muss Sender den Frame erneut senden, jedoch mit der üblichen Wartezeit.
- CSMA/CA mit RTS/CTS (optional)
  - Nicht immer kann eine Station erkennen, dass das Medium belegt ist, da nicht alle Stationen zueinander in Sendereichweite sein müssen.
  - Das Medium wird um Störungen zu vermeiden von der sendewilligen Station und der Empfangsstation durch einen Request to Send (RTS) und Clear To Send (CTS) Dialog für andere Stationen für eine Zeitdauer Net Allocation Vector (NAV) gesperrt.
  - Hierbei reicht es, wenn fremde Stationen eines der beiden Signale RTS/CTS mit hören, um diese für NAV in den Wartezustand zu versetzen.
  - Zwischen RTS und CTS wird lediglich SIFS abgewartet.
  - Kollisionen werden zwar verringert, jedoch erhöhter Verwaltungsaufwand
  - Da mit großen Frames die Bitfehlerhäufigkeit steigt, gibt es einen speziellen Fragmentierungsmodus, der es erlaubt die Nachricht auf mehrere Framepakete zu verteilen, ohne dass jeweils eine neue RTS/CTS Nachricht zwischen Empfänger und Sender ausgetauscht werden muss.
- Point Coordination Function (optional)
  - Nur in Infrastrukturmodus verfügbar, da Access Point (oder andere ausgezeichnete Station) für Koordination erforderlich. (Point Coordinator)
  - Der PCF-Modus ermöglicht Garantien bzgl. Verzögerung und Bandbreite.
  - Für den Aufruf zum Wechsel von Distributed Coordinate Function- (DCF) und Point Coordinate Function-Modus (PCF) gibt es eine spezielle Wartezeit Point Coordinate Function Interframe Space (PIFS) die in der Länge zwischen SIFS und DIFS liegt, d.h. Quittungen und RTS/CTS-Frames sind höher priorisiert, aber andere sendewillige Stationen stehen zurück.
  - Beim Aufruf in den PIFS Modus wird eine NAV-Zeit mitgegeben, für die die Stationen in den Wartemodus versetzt werden bzw. in der sie nur auf Anfragen des Point Coordinators antworten.
  - Der Point Coordinator fragt nacheinander alle Stationen ab.
  - Zwischen den einzelnen Sendevorgängen wird nur SIFS abgewartet ⇒ hoher Durchsatz an Daten
  - Nach Abfrage der letzten Station sendet der Point Coordinator den EndCF Frame, der es den Stationen ermöglicht wieder in den normalen Distributed Coordinate Function-Modus überzugehen.
- Weitere Funktionen
  - Timing Synchronisation Function (TSF) Uhrensynchronisation
    - Gemeinsame Zeitbasis erforderlich
      - Zeitgleicher Wechsel der Frequenzen bei Frequenzhoppingverfahren

## Zusammenfassung Mobile Computing (1679)

- Berechnung der Wartezeiten für den Mediumszugriff
- Synchronisation erfolgt über periodisch versandte Beacon-Frames, die neben sonstigen Informationen auch die lokale Zeit enthalten. Alle Stationen korrigieren daraufhin ihre Zeit.
- In Infrastrukturnetzen ist der AccessPoint für den Beacon-Versand zuständig
- In Adhoc-Netzen wird folgendes Verfahren angewandt:
  - Jede Station bewirbt sich um das Recht den Beacon zu senden
  - Da nur einen Station das Medium erhält, wird nur ein Beacon gesendet, alle anderen Stationen geben den Versuch bis zur nächsten Beacon-Fälligkeit auf.
  - Alle Stationen, die das Beacon-Empfangen korrigieren ihre Uhrzeit entsprechend dem Beacon.
- Power Managment
  - Batteriestrom bei mobilen Geräten ist ein kostbares Gut
  - Sleep Mode Komplette Deaktivierung der Sende- und Empfangseinrichtung, wenn sie nicht benötigt wird.
    - Wenn eine Übertragung ansteht, wechselt die Station in den sogenannten Awake Mode und reaktiviert die Funkhardware.
    - Nachteil: Im SleepMode können keine Pakete von aussen empfangen werden. 2 Lösungsverfahren:
      - Für die schlafende Station bestimmte Pakete werden vom Sender zwischengespeichert. Der Empfänger wechselt periodisch in den wachen Zustand und holt für ihn zwischengespeicherte Pakete ab.
      - kann dieses Verfahren an den Beacon-Modus gekoppelt werden.
        - Infrastrukturmodus
          - Zum Zeitpunkt des Beacons wechseln alle Stationen in den Wachmodus,
          - der Accesspoint versendet zusätzlich zur Uhrzeit eine Information in der alle Stationen enthalten sind, für die zwischengelagerte Pakete vorliegen
          - Diese Stationen müssen solange „wach“ bleiben, bis sie alle für sie bestimmten Pakete empfangen haben.
        - Im Adhoc-Modus ist das Verfahren etwas komplizierter, da ggfs. Mehrere Stationen Pakete für die schlafenden Stationen zwischengespeichert haben.
      - Nachteil: Hohes Verkehrsaufkommen im Netz kurz nach Beginn der Beaconperiode
- Roaming
  - Ggf. müssen für die Abdeckung eines ganzen Gebäudes mit Wireless LAN mehrere Access Points eingerichtet werden
    - Netz soll homogen verfügbar sein
    - Zugang soll auch während der laufenden Übertragung erhalten werden
  - Roaming des WLAN lässt sich mit Handover in Mobilfunknetzen vergleichen

## Zusammenfassung Mobile Computing (1679)

- Verfahren;
  - Mobile Station erkennt das Sendeleistung des bisherigen Access Points zu niedrig ist
  - Mobile Station sucht durch entweder durch passives Mithören (Passive Scanning) oder durch aktives aufmerksam machen (Active Scanning) einen neuen Access Point.
  - Findet sich ein geeigneter Access Point registriert sie sich und wartet auf die Quittung
  - Der neue AccessPoint gibt die Information über den Zellenwechsel im Netz bekannt. (insbesondere informiert er den alten Access Point, dass er nicht mehr verantwortlich ist.)
- Funktioniert nur, wenn die Access Points über Distribution System mit einander verbunden sind.
- Für größere Flächen (Städte, Länder) ist dieses Verfahren nicht einsetzbar, da die Access Points nicht in einem durchgängigen Distribution System vernetzt sind.

### ○ Weiterentwicklungen von 802.11

802.11	WLAN für 1-2 MBit/s auf dem 2,4GHz Band
802.11a	WLAN bis 54 MBit/s auf dem 5 GHz Band
802.11b	Erweiterung von 802.11 bis 11 MBit/s auf dem 2,4GHz-Band
802.11bcor	Korrekturen zu 802.11b
802.11d	Anpassungen an nationale Regelungen
802.11e	MAC-Erweiterungen zu 802.11a und b um Quality of Service und besseres PowerManagment zu ermöglichen
802.11f	Kommunikation zwischen Access Points (Inter Access Point Protocol IAPP)
802.11g	Höhere Datenraten ab 20MBit/s auf dem 2,4 GHz Band
802.11h	Höhere Datenraten auf dem 5 GHz Band
802.11i	MAC Erweiterungen, um verbesserte Sicherheits- und Authentifikationsmechanismen zu ermöglichen

## HIPERLAN (High Performance Radio Local Area Network)

### - HIPERLAN/1

- kaum kommerziell genutzt jedoch bemerkenswertes Konzept
- Frequenzband 5120-5300MHz aufgeteilt auf 5 Kanäle
- Datenraten bis 23,5MHz
- Reichweite ca. 50m
- Knoten können Pakete weiterleiten
- Stromsparmechanismen für Batteriestrom
- Architektur

Sicherungsschicht (Data Link Layer)	Medium Access Control (MAC)
	Channel Access Control (CAC)
Bitübertragungsschicht (Physical Layer)	Bitübertragungsschicht (PHY)

- Medium Access Control: Versenden von Daten mit Hilfe von Dienstprimitiven und Prioritäten (0 bis 4), Verschlüsselung und Energiesparfunktion
- Channel Access Control: Vergleichbar MAC aus IEEE802.11. Regelt Zugriff auf Funkmedium unter Berücksichtigung von Prioritäten
- Bitübertragungsschicht, analog IEEE 802.11
- Zugriff auf das Funkmedium:
  - Elimination Yield Non pre emptive Priority Multiple Access (EY-NPMA)

- Channel free condition: Ist der Kanal frei und wird innerhalb einer bestimmten Zeit keine Übertragung festgestellt, kann mit dem Senden begonnen werden.
- Synchronized Channel Condition: Wird der Kanal belegt vorgefunden, so wird folgendes Senderauswahlverfahren gestartet, um möglichst nur einer sendewilligen Station das Senderecht zu erteilen:
  - Priorization Phase: Auswertung der Sendepriorität der Stationen, es kommen nur die Stationen mit der höchsten Priorität in die nächste Auswahlrunde. Alle anderen müssen sich im nächsten Zyklus erneut bewerben.
    - 5 Prioritätsstufen (0-4)
    - davon abhängige konstante Wartezeit
    - wird in der Wartezeit von einer anderen Station ein Priority Assertion - Burst (Signal) gesendet, hat diese höhere Priorität.
    - Der Sendevorgang der niederwertigen Station wird abgebrochen.
    - Wird in der Wartezeit kein Signal einer anderen Station empfangen sendet die Station selber ein Priority Assertion Burst.
  - Contention Phase:
    - Elimination Phase:
      - Es stehen 0 bis 12 Zeiteinheiten zur Verfügung
      - Die Länge beginnt bei 0.
      - Ein Zufallsgenerator bestimmt mit der Wahrscheinlichkeit 0,5 über die Verlängerung um jeweils eine Einheit
      - Am Ende der Wartezeit wird ein Elimination Burst gesendet.
      - Elimination Survival Verification: Das Medium wird abgehört. Sendet eine weitere Station später einen Elimination Burst, ist das Gerät ausgeschieden. Bleibt das Medium frei geht es in die nächste Auswahlrunde.
    - Yield-Phase
      - Yield Listening: Wartezeit von 0-9 Zeiteinheiten
      - Auswahl der Wartezeit durch Zufallsgenerator, der alle Zahlen mit gleicher Wahrscheinlichkeit auswählt.
      - Bleibt das Medium in der Wartezeit frei, so beginnt die Station selbst mit der Transmission.
  - Transmission Phase: Die einzig übrig gebliebene Station versendet ihre Daten. Entweder als bestätigungslosen Multicast oder als Unicast, im letzteren Falle erfolgt noch in der Transmission Phase die Quittung durch den Empfänger.
  - Kollisionen sind nicht ausgeschlossen, ihre Wahrscheinlichkeit ist aber sehr gering.
  - Hidden Terminal Problem

## Zusammenfassung Mobile Computing (1679)

- Ein Funksignal kann auch über große Entfernung erkannt werden, selbst wenn es nicht mehr einwandfrei erkannt werden kann, kann doch auf die Belegung des Mediums geschlossen werden
- Hidden Elimination Condition: Eine Station kann selbst ermitteln, ob sie gerade ein Hidden Terminal ist. Sie verlängert dann die Wartezeiten um die Gefahr von Kollisionen zu reduzieren.
  - Eine Station verliert in der Contention Phase gegen eine andere Station.
  - Das Medium bleibt dennoch unerwarteter Weise scheinbar unbelegt.
  - Da mindestens eine Station die Contention Phase übersteht, muss damit eine Station senden, die außerhalb der Empfangsreichweite liegt.
- Forwarders
  - Pakete können von so genannten Forwarders an Stationen weitergeleitet werden, die außerhalb der direkten Empfangsreichweite liegen.
  - Unterscheidung zwischen Unicast und Multicast-Paketen
    - Für Unicast Pakete existiert in jeder Station eine Liste von Forwardern, die zu einer bestimmten Zielstation führen. Das Paket erhält 2 Adressen, eine vom direkten Empfänger und eine vom nächsten Forwarder.
    - Für Multicast Pakete wird aus der Menge der Forwarder eine Teilmenge gebildet, die alle Zielknoten abdeckt. Entsprechende Forwarder werden Multipointrelays genannt,
  - Die Verwaltung der Informationen zur Paketweiterleitung ist aufwendig. Forwarder müssen deshalb einiges an Rechenleistung und Bandbreite für diese Aufgabe zur Verfügung stellen. Beim Aufbau eines Netzwerkes muss deshalb abgewogen werden, ob die Einrichtung einer zusätzlichen Basisstation sinnvoller ist.
- Power Management
  - Doze Mode: Sendeeinrichtung wird abgeschaltet und die Leistung des Empfängers reduziert. Der Empfänger kann nur noch die Header der Pakete abhören um zu erkennen ob Pakete für ihn bestimmt sind. Stellt er ein Paket für sich fest, wird die normale Sende und Empfangsbereitschaft wieder aktiviert.
  - P-Saver und P-Supporter: Sende und Empfangseinrichtung des P-Savers werden für einen bestimmten Zeitraum komplett deaktiviert. Jedem p-Saver ist ein p-Supporter zugeordnet, der während er Deaktivierung die Pakete für den P-Saver zwischenspeichert. Der P-Saver aktiviert periodisch sein Sende- und Empfangseinrichtung. Der P-Supporter kennt diese Wachphasen und überträgt dann die gepufferten Pakete.
- HIPERLAN/2
  - Eigenschaften:
    - Frequenzband 5150-5350 MHz und 5470-5725 MHz
    - Datenraten bis 54 MBit/s
    - Reichweite in Gebäuden ca. 30m, im Freien ca. 150m
    - 2 Modi:
      - Direct Mode (Ad Hoc Modus)
      - Centralized Mode (Infrastrukturmodus)
    - Quality of Service (QoS) Dienstgüteparameter werden unterstützt
    - Stromsparmöglichkeiten für Batteriestrom sind integriert
    - Vergleichbar 5 GHz Mode IEEE802.11
  - Referenzmodell:

## Zusammenfassung Mobile Computing (1679)

- 3 Schichten
  - Bitübertragungsschicht (PHY)
    - Entspricht der Bitübertragungsschicht anderer Referenzmodelle wie IEEE802.11 oder OSI
  - Data Link Control (DLC)
    - Radio Link Control (RLC)
      - Kryptographische Verschlüsselung
      - Handover
      - Power Management
      - Start und Ende von Verbindungen, Broadcast und Multicast
    - Error Control (EC)
      - Zuverlässige Datenübertragung durch Automatic Repeat Request (ARQ)-Mechanismus
    - Media Access Control (MAC)
      - Entspricht weitestgehend MAC aus IEEE802.11
  - Convergence Layer
    - Aufgaben
      - Unterteilung großer Pakete in kleinere Einheiten
      - Abbildung höherer Schichten auf die DLC-Schicht
    - 2 Arten
      - Zellenbasierte Convergence Layer übertragen Pakete fester Länge (z.B. für ATM-Netze notwendig)
      - Paketbasierte Convergence Layer übertragen Pakete unterschiedlicher Länge (z.B. für Ethernet notwendig)
- Core Networks:
  - verbinden einzelne HIPERLAN-Netze und bieten Zugang zu fremden Netzwerken
  - Access Points sind die Core Netzwerkvermittler und sorgen für die Vermittlung durch die unterschiedlichen Protokollstapel (Internet working Functions (IWF))
- HIPERACCESS bietet eine Drahtlose Verbindung von einem Zugangspunkt zum Endkunden (letzte Meile) mit einer Datenrate von 25km/h und einer Reichweite von bis zu 5 km
- HIPERLINK feste Punkt-zu-Punkt-Verbindung zwischen HIPERLAN oder HIPERACCESS Zugangspunkten. Datenrate bis zu 155 MBit/s über 150m.

### Wireless Asynchronus Transfer Mode (Wireless ATM)

- Erweiterung des drahtgebundenen ATM-Verfahrens für drahtlose Kommunikation
- Datennraten 25 MBit/s für das 5 GHz-Band
- Reichweite 30 – 300m
- Grundlagen ATM
  - Konzept der virtuellen Verbindung
  - Vor Datenübertragung wird im Netzwerk eine Wegeauswahl getroffen, die die Rechner verbindet und die über die gesamte Verbindung erhalten bleibt
  - Festvorgeschriebene Paketlänge (Zellengröße) von 53 Byte, davon sind 48 Byte Nutzdaten vermeidet Aufwand für Paketgrößenbegrenzer.
  - Im ATM-Netz werden Zellen zu beliebigen Zeiten (asynchron) transportiert.
  - Lediglich der Header wird durch eine Prüfsumme gesichert
  - Verwendung nur in Übertragungsschichten mit niedriger Bitfehlerrate.
  - Für einzelne Übertragungen können Dienstgüteparameter, die eine bestimmte Bandbreite reservieren festgelegt werden
- Motivation Wireless ATM

## Zusammenfassung Mobile Computing (1679)

- ATM bietet ein Protokoll für Weitverkehrsnetze und lokale Netze, die Weiterentwicklung zu wireless LAN ist Konsequenz
- Dienstgüteeigenschaften auch für Mobile Stationen interessant, obwohl durch temporäre Unterbrechungen Qualitätseinbußen auftreten können
- Existierende Telekommunikationsdienste die auf ATM basieren können zu mobilen Diensten erweitert werden.
- Problembereiche bei der Entwicklung:
  - Drahtloser Zugriff:
    - Definition der Dienstgüteeigenschaften für die Luftschnittstelle
    - Der Radio Access Layer (RAL) von Wireless ATM vereint die Funktionen der OSI-Schichten 1 und 2.
    - Als RALs sollten extern spezifizierte Netzwerke insbesondere HIPERLAN/2 eingesetzt werden
  - Mobilitätsmanagement (Mobile ATM)
    - beschäftigt sich mit Problemen des Roaming und Handover für drahtlose Stationen.
    - Vorwiegend Endgerätemobilität betrachtet
    - Benutzermobilität wurde nicht vertieft betrachtet.
    - 4 Aufgaben
      - Ortsmanagement
        - Registrierung von mobilen Stationen
        - Aktualisierung der Position
        - Verwaltung über Location Server (LS), die die betroffenen EMAS informieren
      - Verbindungsübergabe
        - Connection Forwarding kann nur eingesetzt werden, wenn eine Verbindung aufgebaut wird, nachdem die station sich bewegt hat.
        - Connection Handover unterbrechungsfreie Übergabe der Verbindung bei einer Bewegung während einer laufenden Verbindung
        - Netzwerk wird unterteilt
          - festes Segment, dass von der Übergabe nicht betroffen ist.
          - Handoversegment, dass auf die Übergabe reagieren muss.
            - Kann mehrere EMAS und RAS umfassen
        - Ankerpunkt ist der Knoten, der zwischen dem festen Segment und dem Handoversegment liegt.
        - Anforderungen:
          - Eine Station kann mehrere Verbindungen gleichzeitig haben, diese müssen beim Handover alle übergeben werden.
          - Auch Point to Multipointverbindungen müssen beim Handover übergeben werden, allerdings kommt es hier zu Einschränkungen wegen der Komplexität der Operation
          - Wahrung der Dienstgüteeigenschaften während des Handover
          - Es sollen möglichst wenig Zellen verloren gehen.
            - Zellen dürfen nicht doppelt oder in falscher Reihenfolge beim Empfänger eintreffen, da ATM-Anwendungen nicht darauf

eingerrichtet sind, entsprechende Fehler zu behandeln, da dies bei drahtgebundenen ATM-Netzwerken wegen der virtuellen Verbindung nicht vorkommen kann.

- Sicherheitsmanagement und Dienstmanagement
  - Authentifizierungskonzept über Authentifikation Server (AUS), der eng mit dem Location Server zusammen arbeitet.
  - Eng verknüpft mit dem Zugriff ist das Dienstmanagement, da der Dienstzugriff mit den mobilen Stationen wandern soll, wenn der Benutzer einen neue Administrative Umgebung betritt.
- Wireless ATM-Szenarien
  - Klassische ATM-Switches
  - ATM-Switches mit Mobilitätsunterstützung
    - End User Mobilty Enabled ATM Switches (EMAS) ermöglichen den Wechsel zwischen Zellen
      - EMAS-Edge (EMAS-E) sind direkt mit Funksystem verbunden
      - EMAS-Network (EMAS-N) befinden sich innerhalb des Netzwerkes
  - Radio Access System (RAS) ermöglicht die Einbindung drahtloser Stationen)
    - Access Point (Rechnereinheiten)
    - Radio Transceiver (Sende und Empfangseinrichtung)
  - Stationen selbst
    - Mobile Stationen (mobile Terminal)
    - Drahtlose Stationen (wireless Terminal)
    - Mobile drahtlose Stationen (Wireless Mobile Terminal)
  - Auch Ad Hoc Netze werden unterstützt.
    - Spezielle Station Ad Hoc Central Control Terminal (ACT) kontrolliert dann das Netzwerk
  - Auch Switches können mobil sein
  - Zugänge zu anderen Netzwerken sind denkbar
- Zukunft:
  - Da ATM auch im drahtgebundenen Bereich auf dem Rückzug befindet, da immer schnellere Ethernet-Switches den Geschwindigkeitsvorteil, den ATM ursprünglich bot aufgeholt haben, ist die Zukunft von Wireless ATM ungewiss. Insbesondere, da mit der Abdeckung der komplexen Szenarien hohe Technologiekosten verbunden sind.

#### Home RF (Shared Wireless Access Protocol SWAP)

- drahtloser Netzwerkstandard für Privat und Heimanwender
- Die Eigenschaften sind ähnlich mit IEEE 802.11b was Reichweite und Bandbreite betrifft.
- Die Hardwarekosten sind geringer als bei 802.11b
- Eigenschaften
  - 2,4 GHz Band
  - Datenrate 10 MBit/s
  - Reichweite ca. 50m
  - Für die Bitübertragung wird Frequency Hopping Spread Spectrum (FHSS) mit 50 Frequenzwechseln die Sekunde eingesetzt.
  - Bis zu 8 priorisierte Datenströme für Multimediaübertragungen sind möglich
  - 8 bidirektionale Audiokanäle können über DECT-Protokoll allerdings im 2,4GHz Band statt im 1,9GHz Band eingerichtet werden.
  - Es sind bis zu 127 Stationen im Netz zugelassen

## Zusammenfassung Mobile Computing (1679)

- Sowohl AdHoc, als auch Infrastrukturmodus werden unterstützt, allerdings sind im AdHoc-Modus keine priorisierten Kanäle oder Audiokanäle nutzbar.
- 3 verschiedene Arten der Datenübertragung:
  - reine Datenübertragung
    - beispielsweise über TCP.
    - auf der MAC-Ebene wird die Datenübertragung nicht priorisiert behandelt.
    - Es gibt keine Garantien für die Dienstgüte
    - Zugriff auf das Funkmedium wird über Carrier Sense Multiple Access mit Collisions Avoiding (CSMA/CA) realisiert.
  - Streams
    - z.B. Internet-Audio und Videoströme, sowie Sprachübertragung über IP (Voice over IP)
    - erhalten reservierte Zeitscheiben am Anfang am Anfang jeder Datenübertragung nur die nicht verbrauchten Bereiche können für die Übertragung nicht priorisierter Daten genutzt werden.
  - Audio:
    - Über DECT Protokoll
    - Feste Zeitrahmen
    - Nicht über CSMA/CA, da dort keine Zugriffszeiten garantiert werden, sondern über TimeDivisionMultipleAccess.(TDMA)
    - Besonderer Mechanismus erlaubt die sofortige Neuübertragung fehlerhaft übertragener Audiodpakete direkt nach dem Frequenzsprung, zur Steigerung der Sprachqualität.
- Zielsetzung:
  - vollständiges Netzwerk zur Vernetzung von Computern,
  - Anforderungen von Geräten des Konsummarktes wie schnurlosen Telefonen und MP3-Playern werden berücksichtigt.
  - HomeRF steht zwischen drahtlosen LANs und Wireless Personal Area Networks (WPAN)

## Besonderheiten der verschiedenen drahtlosen Netzwerke

- IEEE802.11
  - Nahtlose Eingliederung in IEEE 802-Rahmenwerk
  - Kann wie Ethernet-Standard verwendet werden erleichtert deshalb die Arbeit von Betriebssystem und Treiberentwicklern.
  - Einsatz in lokalen Netzen und HotSpots
- HIPERLAN
  - Wesentlich komplexeres und ausgefeilteres Verfahren für den Zugriff auf das Medium
  - Einzigartig ist die Weiterleitung von Paketen über spezielle Stationen
  - HIPERLAN/2 zeichnet sich durch die Zusammenarbeit mit CoreNetworks aus und eignet sich dadurch auch für HotSpots zur Entlastung des Mobilfunknetzes.
- Wireless ATM
  - Nicht endgültig spezifiziert
  - Kompliziertestes Verfahren, Abdeckung sehr vieler Einsatzszenarien.
  - Schwerpunkt auf die Anbindung drahtloser Stationen an eine Weitverkehrsnetz
- HomeRF
  - Auf Konsum und Privatanwendermarkt zugeschnitten
  - Niedrige Hardwarekosten
  - Priorisierung von Multimediaströmen und Audio
  - Trotzdem vollwertiges Computernetzwerk möglich.

## KAPITEL 5: Wireless Personal Area Networks

### Möglichkeiten, Einsatzgebiete und Grenzen von Wireless Personal Area Networks

- Netzwerke, die für die Vernetzung kleinerer Geräte (drahtlose Headsets, PDAs,...) konzipiert sind
- Kommunizierende Geräte haben keine große Distanz zueinander
- Reichweite wenige cm bis zu einigen Metern
- Stromsparende Kommunikationsverfahren, da Geräte mit mobiler Stromversorgung geringer Kapazität ausgestattet sind.
- Kostengünstige Hardware, da für Massen und Konsummarkt gedacht
- Minimale Konfiguration erforderlich, da Nutzer in Netzwerkfragen unkundig sind
- Automatische Verbindungsaufnahme und Suchfunktion für andere Geräte und Dienste
- Spezielle Netzwerktechnologien für hoch spezialisierte Geräte und Anwendungen
- Häufig nur point to point Verbindungen zwischen zwei Geräten möglich
- Point to Multipoint maximal für ein ausgezeichnetes Gerät
- Einsatzgebiete:
  - o Ausdrucken von Digicamfotos auf einem Fotodrucker
  - o Anschluss eines drahtlosen Headsets an ein Mobiltelefon
  - o Anschluss von Rechnerperipherie (Maus, Tastatur,..)
  - o Vernetzung von Haushaltsgeräten
  - o Vernetzung von PDAs zum Austausch kleiner Datenmengen

### Infrared Data Association (IrDA)

- Datenraten
  - o Serial Infrared (SIR) bis 155,2 kBit/s
  - o Fast Infrared (FIR) bis 4 MBit/s
  - o Very Fast Infrared (VFIR) bis 16 MBit/s
- 2 Teilstandards:
  - o IrDA Control
    - für die Anbindung von Rechnerperipherie (drahtlose Mäuse, Tastaturen, ...).
    - Datenrate bis 75 kBit/s
    - Reichweite bis zu 5m
  - o IrDA DATA
    - Datenraten bis zu 16MBit/s
    - Reichweite bis zu 1m
    - Suchfunktion für Geräte und Dienste in Kommunikationsreichweite
    - Automatische Aushandlung der Kommunikationsparameter
    - Mehrere logische Geräte zwischen 2 Geräten möglich
    - Unzuverlässiger Broadcast an mehrere Geräte möglich
    - Transportprotokoll für die Flusskontrolle und Segmentierung langer Nachrichten
    - Emulation serieller und paralleler Schnittstellen
    - Protokoll für Netzwerkanbindung vorhanden
    - Optionales Protokoll erlaubt die Übertragung komplexer strukturierter Datenobjekte
- Eigenschaften der Infrarotkommunikation
  - o Infrarotverbindungen sind zwingend Sichtverbindungen geringer Reichweite
  - o Störungen durch andere Infrarotsender nur bei unmittelbarer Nähe möglich
  - o Hohe Abhörsicherheit durch geringe Reichweite und Erfordernis der Sichtverbindung
  - o Sonnenlicht stört Infrarotübertragungen so massiv, dass Infrarotübertragungen auf das innere von Gebäuden beschränkt sind
  - o Infrarotkommunikation kann durch Kunstlicht gestört werden, ist aber unempfindlich gegen elektromagnetische Störungen und Funksendern

## Zusammenfassung Mobile Computing (1679)

- Infrarot unterliegt im Gegensatz zur Funkübertragung keinen hoheitlichen Beschränkungen

### - IrDA Protokollstapel

	IAS Information Access Service		IrLAN Infrared Local Area Network	IrOBEX Infrared Object Exchange Protocol	irCOMM
Tiny TP Tiny Transport Protokoll					
IrLMP Infrared Link Management Protokoll					
IrLAP Infrared Link Access Protocol					
Bitübertragungsschicht					

- Bitübertragungsschicht: optische Übertragung, Darstellung der Bits, Übertragungsgeschwindigkeit, optische Charakteristika
  - Infrarot Transceiver: Einrichtung zum Senden und Empfangen von Infrarotsignalen
  - Sendekegel mind. 15° der optischen Achse abdecken max. an den Rändern 30° Abdeckung. Lichtintensität muss für größere Winkel unter eine bestimmte Intensitätsschranke fallen
  - Reichweite mind. 1 Meter, jedoch LowpowerOption von 20cm Reichweite zulässig. (Datenrate bei LowPower maximal 115,2 kBit/s)
  - Modulationsverfahren
    - RZI Return Zero Inverted (bis 1,152 MBit/s Übertragungsrate)
      - Bei jedem 0 Bit wird ein kurzer Infrarotimpuls ausgesendet
      - 1 Bit haben keine Auswirkung auf die Infrarotquelle.
      - Lange Folge von 1 Bit ist störend, da evtl. Takt aus der Synchronität läuft, deshalb muss auf Senderseite sichergestellt werden, dass nicht zu viele 1 Bit aufeinander folgen.
    - 4PPM 4 Pulse Position Modulation (4 MBit/s Übertragungsrate)
      - Je zwei Bits werden als eine Einheit codiert durch eine Sequenz von 4 so genannten Chips, von denen immer genau ein (aktiver) Chip zu einem Infrarotimpuls führt
      - Die Position des aktiven Chip gibt den Wert des Doppelbits an.
      - Von den 16 möglichen Chipkombinationen werden nur 4 zur Nutzdatenübertragung genutzt.
      - Weitere Chipkombinationen werden zur Start und Endemarkierung von Datenblöcken verwendet.
      - Die Taktrate der Chips ist doppelt so hoch, wie der Datentakt
    - HHH1,13 Hirt, Hassner, Heise (Übertragungsrate 16MBit/s)
      - Die Zahlen 1 und 13 im Namen geben an, wie viel inaktive Chips mindestens und höchstens zwischen zwei aktiven Chips liegen dürfen.
      - Jeweils 3 Chips repräsentieren 2 Bit, d.h. die Kodierung nutzt die vorhandenen Kombinationsmöglichkeiten effizienter als 4PPM
  - Nur Halbduplexbetrieb möglich, d.h. es kann immer nur einer von 2 Kommunikationspartnern senden. Gleichzeitiges Senden und Empfangen ist wegen der Reflexion der Lichtimpulse nicht möglich.
- IrLAP Infrared Link Access Protocol: zuverlässige Übertragung zwischen zwei Geräten

## Zusammenfassung Mobile Computing (1679)

- Entspricht der Sicherungsschicht (Data Link Layer) im OSI-Referenzmodell
- Zugriffskontrolle auf den Infrarotkanal
- Suchen nach anderen Infrarotgeräten im Kommunikationsbereich
- Aushandeln von Kommunikationsparametern
- Beginnen und Beenden von Kommunikationsverbindungen
- Bereitstellen einer gesicherten Bidirektionalen Verbindung
- Nutzung einer Weiterentwicklung des HighLevelData Link Control (HDLC) Sicherungsprotokolles.
- Erweiterung der Nutzdaten um:
  - Eine CyclicRedunancyCheck (CRC)-Prüfsumme wird dem Datenblock angehängt
  - Hinter jedem Block von fünf 1 Bits wird ein 0 Bit eingefügt um beim RZI-Modulationsverfahren Probleme zu vermeiden
  - Begrenzungsflags (01111110) zeigen Anfang und Ende von Frames an. (Da das Flag 6 1Bits in direkter Folge enthält kann diese Kombination nicht im Datenfeld vorkommen.
  - Maximale Größe des Datenblockes liegt zwischen 64 und 2048 Byte
- Zustände:
  - Normal Disconnect Mode (NDM)
    - Geräte die nicht mit anderen Geräten verbunden sind.
    - Nur Discovery, d.h. Suche nach anderen Geräten in Kommunikationsreichweite möglich
  - Normal Response Mode (NRM)
    - Zuverlässige Kommunikationsverbindung zu einem anderen Gerät ist aufgebaut
    - Daten können ausgetauscht werden
- Zugriffskontrolle im NRM:
  - Master/Slave-Verfahren über Primary/Secondary Zuordnung
  - Der Primary regelt den Zugriff auf den Infrarotkanal
  - Der Secondary darf nur nach Aufforderung durch den Primary für bestimmten Zeitraum senden und muss danach Senderecht wieder an den Primary abtreten.
  - Bei mehreren Geräten ist 1 Gerät Primary, alle anderen sind Secondaries, allerdings können die Secondaries dann nicht miteinander kommunizieren, der Primary ist der einzige, der alle anderen erreichen kann.
  - Aufgrund geringer Hardwareausstattung, kann nicht jedes Gerät Primaryaufgaben erfüllen, dies ist vom IrDA-Standard erlaubt, jedoch können zwei reine Secondarygeräte nicht miteinander kommunizieren.
- Media Access Rules = Zugriffskontrolle im NDM:
  - Feste Datenrate von 9600 Bit/s (Für zugelassene Geräte, die nur 2400 Bit/s senden existieren besondere Regeln)
  - Laufende Kommunikation zwischen NRM-Geräten hat Vorrang vor NDM Kommunikation, d.h. eine NDM-Paket kann nur versandt werden, wenn der Infrarotkanal für mind. 500ms keine Aktivität aufgewiesen hat.
- IrLAP-Dienste können von der IrLMP-Schicht wie folgt angefordert werden:
  - DISCOVERY: Erstellt eine Liste von Geräten in Kommunikationsreichweite

## Zusammenfassung Mobile Computing (1679)

- NEW\_ADRESS: Vergabe einer neuen Adresse, falls es in der Discoveryliste doppelte Geräteadressen gibt
- UNITDATA: unzuverlässige Broadcastsendung an alle Geräte in Kommunikationsreichweite
- CONNECT: Verbindungsaufnahme zu anderem Gerät inkl. Aushandlung Primary/Secondary und Festlegung der Kommunikationsparameter. Die Verbindung kann anschl. Über eine 7 Bit Adresse identifiziert werden
- SNIFF: Wunsch für Verbindungsaufnahme als Secondary
- DATA: zuverlässige oder unzuverlässige Datenübertragung über die vorher eingerichtete Verbindung
- STATUS: Fragt den Verbindungsstatus für höhere Schichten ab.
- RESET: Neuinitialisierung der Verbindung nach Zustimmung beider Kommunikationspartner
- DISCONNECT: Verbindungsabbau und Rückkehr in Status NDM
- IrLMP Infrared Link Management Protocol: mehrere logische Kanäle für eine physische Verbindung
  - Verbergen der Rolle des Gerätes innerhalb von IrLAP.
  - Sowohl Primary als auch Secondary können Dienste anbieten
  - Aufteilung der Verbindung in mehrere logische parallel nutzbare Kanäle (z.B: Kann dann gleichzeitig gedruckt und Daten übertragen werden)
    - Konzept der logischen Dienstzugangspunkte (Logical Service Access Point (LSAP))
    - Jeder LSAP repräsentiert einen Dienst (Druckdienst) oder einen logischen Kommunikationskanal zu einer Anwendung
    - Identifikation über 7 Bit LSAP-Selector (LSAP-SEL)
      - 0x00 reserviert für den Information Access Service IAS
      - 0x01 bis 0x6f Freivergebbare Nummern
      - 0x70 reserviert für verbindungslose Kommunikation
        - IrLMP erlaubt die Verbindung zwischen zwei LSAPs auf einem einzigen Gerät, damit lokale Anwendungen ohne Nutzung der Infrarotschnittstelle miteinander kommunizieren können.
      - 0x71 bis 0x7F reserviert für zukünftige Zwecke
    - LSAP-SEL ist jeweils nur innerhalb eines Gerätes eindeutig
  - IrLMP ermittelt erheblich mehr Informationen über die Kommunikationspartner als IrLAP und stellt diese in kleiner Datenbank zur Verfügung
  - IrLMP erweitert zur Verwaltung der logischen Kanäle das Nachrichtenformat um 2 Byte, die Ziel und Quelle der Nachricht spezifizieren, dabei legt das 1.Bit des 1.Byte fest ob es sich
    - 0 um Daten
    - 1 um eine Kontrollnachricht handelt
- IAS Information Access Service: „gelbe Seiten“ Auskunft über verfügbare Dienste anderer Kommunikationspartner
  - Verzeichnis der Dienstnummern der zugreifbaren Dienste eines Gerätes
  - Austausch der Daten erfolgt über das Information Access Protocol (IAP)
  - IAS-Datenbasis besteht aus einer Reihe von Class-Objekten, die über Namen zugreifbar sind, die jeweils wieder aus einer Tabelle von Attributen und Werten bestehen.

- Jedes Gerät enthält in seiner Datenbasis 1 Objekt mit dem Namen Device, das Informationen über das Gerät enthält.
- Zu jedem Dienst gibt es eine weitere Klasse
- Jeder Dienst erhält nach IrDA Empfehlung mind. 2 Attribute (weitere Attribute können von den Diensteanbietern beliebig definiert werden)
  - IrDA:IrLMP:InstanceName: Unterscheidungsmerkmal, falls es mehrere Dienste mit demselben Namen gibt
  - IrDA:IrLMP.LsapSel: LSAP-SEL-Nummer unter der der entsprechende Dienst zugreifbar ist.
- TinyTP Tiny Transport Protocol: (optional, aber dringend empfohlen)
  - Flusskontrolle auf Basis von logischen IrLMP Kanälen.
    - Durch Verwendung mehrerer Kanäle auf einer einzelnen Verbindung kann es dazu kommen, dass eine Anwendung mit großem Datenaufkommen eine zweite Verbindung blockiert. Im Extremfall kann eine Anwendung mehrere Datenkanäle nutzen, die in einer bestimmten Reihenfolge ausgelesen werden. Wartet nun eine Anwendung auf eine Nachricht einer Verbindung, die von einer anderen blockiert wird, kommt es zum Deadlock.
    - Vergabe von Krediten = Erlaubnis eine bestimmte Menge von Daten zu versenden. Jede Nachrichtenübertragung verringert die Kredite um 1. Sind die Kredite aufgebraucht wird der Sender blockiert, bis er neue Kredite erhalten hat.
  - Große Nachrichten werden für Transport in kleine aufgeteilt und am Zielort wieder zusammengesetzt. (Segmentation and Reassembly)
  - Damit könne pro Sendeoperation bis zu 64KByte übertragen werden.
  - Erweiterung des Nachrichtenformates um 1 Byte:
    - 1.Bit: Signalfag (Pufferung der Daten beim Empfänger bis zum Empfang des Endesignals)
      - 0 letztes Teilpaket
      - 1 weitere Teilpakete folgen
    - letzte 7Bit Kredite (Kanalbezogene Sendeerlaubnis)
- IrCOMM: (optional) Emulation serieller oder paralleler Schnittstellen. Anwendungen für diese Schnittstellen können so ohne Modifikation die Infrarotverbindung nutzen.
- IrOBEX Infrared Object Exchange Protocol (optional) Austausch komplexer Objekte, wie z.B. Visitenkarten, Texten oder Grafiken (Beamen)
- IrLAN Infrared Local Area Network (optional) Anbindung an ein lokales Netz über Infrarotschnittstelle
  - Access Point: Zugriff auf Netzwerk wird über ein weiteres Gerät bewerkstelligt, das sowohl eine Netzwerkkarte, als auch einen Infrarotanschluss hat.
  - Peer-to-Peer: 2 Geräte werden über Infrarot miteinander verbunden und nutzen dabei Netzwerkdienste, als ob die Geräte Netzwerkkarten besitzen würden
  - Hosted: Mehrere Geräte sind mit einem Rechner verbunden, der über eine Netzwerkkarte verfügt. Im Gegensatz zum Access Point verfahren teilen sich die Geräte hierbei jedoch die Netzwerkkartenadresse und werden von außen als ein Gerät wahrgenommen.
- Infrared Mobile Communication (IrMC)
  - Rahmenwerk für die mobile Kommunikation mit IrDA
  - Sammlung von Formatspezifikationen für den Austausch mobiler Daten
    - Visitenkarten, Kalendereinträge, Texte und Nachrichten
  - Definition eines Audiokanals mit IrDA

### Bluetooth

- Eigenschaften
  - o Datenrate bis 1MBit/s (Brutto)
    - Datentransport max. 723,2 kBit/s für die Gegenrichtung bleiben dann 57,6 kBit/s. Keine Audioübertragung möglich
    - Gleiche Bandbreite für beide Richtungen 433,9 kBit/s auch hier ist keine Audioübertragung möglich
    - Bidirektionale Audioübertragung 64 kBit/s
  - o Entfernung bis zu 10m
  - o Frequenz 2400-2483,5MHz (ISM-Frequenzband) aufgeteilt in 79 Kanäle analog IEEE802.11
  - o Fast Frequency Hopping mit 1600 Frequenzwechseln pro Sekunde (Slotgröße 625µs)
    - Kollisionsvermeidung über Time Division Duplex (TDD)
    - Master senden grundsätzlich auf Slots mit gerader Nummer
    - Slaves auf Slots mit ungerader Nummer
    - Passt eine Datenübertragung nicht in einen Slot, darf die Übertragung auf 3 oder 5 Slots ausgedehnt werden. Der Partner antwortet danach jedoch auf der Frequenz die bei ständigem Slotwechsel gültig gewesen wäre.
    - Sind mehrere Slaves im Piconet, so sendet der Master abwechselnd zu jedem Slave einen Frame, der Slave darf nur antworten, wenn er vom Master dazu aufgefordert wird.
    - Die Frequenzfolge muss allen Geräte bekannt sein. Sie wird aus der Geräteadresse des Masters errechnet. Da jeder Master eine andere Adresse hat, kommt es auch im Überlappungsbereich der Scatternets nicht zu Störungen.
  - o Bluetooth ist auch gegenüber Störungen durch andere Netzwerke auf dem ISM-Band unempfindlich
  - o Automatische Verbindung von Geräten in Kommunikationsreichweite
  - o Gezielte Suche nach installierten Diensten anderer Geräte
  - o Mehrere zuverlässige logische Kanäle zwischen 2 Geräten möglich
  - o Unzuverlässige Broadcast Nachrichten an mehrere Geräte möglich
  - o Ein Audiokanal reservierter Bandbreite kann zwischen 2 Geräten eingerichtet werden
  - o Dienstgüteparameter sind einstellbar
  - o Transportprotokoll mit Flusskontrolle und Segmentierung langer Nachrichten ist vorhanden
  - o Serielle Schnittstelle kann emuliert werden
  - o Dienste zur Authentifizierung und Verschlüsselung sind integriert
  - o Funkbasiert
  - o Asynchrone und synchrone Verbindungen
- Einsatzszenarien
  - o 3 in 1 Telefon (GSM, Schnurlos und GSM)
  - o drahtloser Internetzugang (z.B. über ein Mobiltelefon)
  - o Synchronisation von Daten mit einem PC
  - o Drahtloser Headset für Mobiltelefone
  - o Drahtlose interaktive Konferenz (Austausch von Daten unter mehreren Bluetoothfähigen Geräten)
- Bluetooth Protokollstapel
  - o Bluetooth Radio und Baseband
    - Zugriff auf das Funkmedium für höhere Protokollschichten
    - Aufbau von Verbindungen zwischen Geräten und Übertragung der Daten über die Funkschnittstelle

## Zusammenfassung Mobile Computing (1679)

- Keine zentrale Administration für Netzwerkaufbau erforderlich
- 2-8 kommunizierende Geräte bilden eine Piconet
  - 1 ausgezeichnetes Gerät ist der Master des Piconet
  - die restlichen maximal 7 aktiven Geräte sind Slaves
  - Es gibt keine direkten Verbindungen zwischen Slaves
- Überlappen sich mehrere Piconets, so spricht man von Scatternets
  - 1 Gerät kann immer nur Master in einem Piconet sein, in dem anderen Piconet ist er ggf. normaler Slave
  - Wäre das Gerät Master in beiden Piconets würde ein einziges Piconet entstehen.
- Jedes Gerät muss sowohl Master- als auch Slave-Funktionalität beherrschen.
- Das Gerät, dass die Verbindungsaufnahme initiiert wird automatisch Master
- Ein Rollentausch in der laufenden Verbindung ist möglich, wenn beide Geräte dem Tausch zustimmen.
- 2 Verbindungsformate
  - Synchronus Connection oriented Links (SCO)
    - Symmetrische Punkt zu Punkt Verbindungen auf vordefinierten Slots
    - Maximal 3 SCO-Links pro Gerät zulässig
    - Verbindungen zu verschiedenen Slaves bzw. Mastern sind erlaubt.
    - Reservierung bestimmter Bandbreite
    - Pakete werden im Fehlerfall nicht erneut versendet
    - Bevorzugt für Audio verwendet
  - Asynchronous Connection-less Links (ACL)
    - Slots die nicht durch SCO-Links belegt sind.
    - Zwischen dem Master und jedem Slave existiert genau ein ACL-Link
    - Fehlerhafte Pakete werden erneut übertragen
    - Master kann ACL-Pakete auch als Broadcast ins Piconet versenden
- Paket hat 3 Teile
  - Access code:
    - Eindeutige Bitsequenz, die Beginn des Paketes signalisiert
    - ggf. die Zieladresse des Empfänger enthält
  - Header:
    - definiert den Pakettyp
      - ACL
        - DM1 bis DM5 (Data Medium Rate)
          - Für Datenübertragung gedacht
          - Absicherung des Datenblockes über Forward Error Correction (FEC) mit einer Rate von 2/3
          - Zusätzlich Cyclic Redunancy Check (CRC) Prüfsumme
          - Slotbelegung zwischen 1 und 5 Slots
        - DH1 bis DH5 (Data High Rate)
          - Keine Absicherung durch Forward Error Correction (FEC)
          - Dadurch etwas mehr Daten pro Paket

- Cyclic Redunancy Check-Prüfsumme
- AUX1
  - Spart auch die Prüfsumme ein
- SCO
  - Audioübertragung 4 Pakettypen
    - HV1 bis HV3 (High Quality Voice)
      - Unterscheiden sich durch die Datenmenge pro Paket und die FEC-Rate
      - Keine CRC-Prüfsumme
      - Reservierte Slots
      - HV1 jeder 2.Slot
      - HV2 jeder 4.Slot
      - HV3 jeder 6.Slot
    - DV (Data Voice)
      - Zusätzlich zur Audioinformation kann eine kleine Menge Daten transportiert werden
      - FEC 2/3
      - CRC nur für Daten
  - enthält Felder zur Flusskontrolle
  - jedes Bit wird 3 fach redundant versendet
- Daten
  - Eigentliche Nutzlast
- Betriebsmodi
  - Standby: Bluetooth nach dem Einschalten noch ohne Verbindung
  - Inquiry: Erlangung einer Liste von Geräten in Reichweite durch „abhören“ verschiedener Frequenzen. Periodischer Versand und Empfang von Inquiry-Paketen.
  - Page: Eigentliche Kontaktaufnahme.
    - PageScan: zyklischer Zustand in dem auf Page-Pakete gelauscht wird, die die eigene Geräteadresse enthalten
    - Wird die ein Page-Paket empfangen, wird eien Verbindung aufgebaut. Das Gerät, dass die Nachricht erhielt wird Slave.
    - Hat ein Piconet einmal einen Master gehen weitere Verbindungsaufnahmen nur noch von ihm aus.
- Verbindungszustände:
  - Active Mode: Normal verbundene Geräte tauschen mit der Gegenstelle Pakete auf allen SCO und ACL-Links aus.
  - Sniff Mode: stromsparender Modus, wenn keine nennenswerte Kommunikation zu erwarten ist.
    - Slave muss nicht mehr ständig auf Aufforderungen vom Master warten.
    - Master wartet zwischen den Sendeaufforderungen an diesen Slave länger als üblich
  - Hold Mode: Es werden nur noch auf dem SCO-Link Daten übertragen
  - Park Mode: Gerät kommuniziert nicht mehr aktiv mit der Gegenstelle, verlässt aber auch nicht das Piconet.
    - Pro Piconet dürfen sich 255 Geräte im ParkMode aufhalten

- Modus überwindet die harte Grenze von maximal 8 Geräten im Piconet.
- Geräte die nicht aktiv kommunizieren können sich in den ParkMode begeben und so einem Gerät im ParkMode die Rückkehr in den aktiven Modus ermöglichen
- Link Manager Protocol (LMP)
  - Kapselt Funktionen zur Verwaltung von Verbindungen
  - Lediglich zusätzliche Funktionen
  - Datenstrom der ACL-Links wird verwendet.
  - Spezieller Eintrag im Header ermöglicht Erkennung von LMP-Paketen durch die Gegenstelle
  - Funktionen:
    - Authentifikation der Gegenstelle bei Verbindungsaufbau und Verschlüsselung der Pakete über kryptografische Verfahren.
    - Abgleich der lokalen Uhren. Keine Veränderung der lokalen Uhren, sondern Offsetberechnung im Piconet.
    - Tausch der Master/Slave-Rollen kann für bestimmte Anwendungen erforderlich sein.
    - Ändern der Verbindungszustände (active, sniff, hold und park mode)
    - Ändern der Sendeleistung: Über den Receiver Strength Signal Indicator (RSSI) wird ständig die Signalstärke gemessen. Ist die Signalstärke außerhalb einer bestimmten Bandbreite, kann ein Gerät die Gegenstelle auffordern ihr Signal zu verstärken bzw. zu drosseln.
    - Einstellen von Dienstgüteparametern: Quality of Service QoS
      - Wahl des Pakettyps mit höherer FEC-Rate bei steigender Fehlerrate auf der Funkschnittstelle
      - Limitierung der Slavesendeslots durch einen Master um selber über mehr Bandbreite zu verfügen.
    - Einrichtung von SCO-Links: Nach Verbindungsaufbau existiert zunächst nur ACL-Link. Bis zu 3 SCO-Links können über LMP-Funktionen extra eingerichtet werden.
- Logical Link Control and Adaption Protocol (L2CAP)
  - Stellt mehrere logische Kanäle pro ACL-Link zur Verfügung
  - segmentiert große Datenpakete für den Datentransport (Segmentation and Reassembly (SAR))
    - maximale Nutzlast der Basebandschicht ist 339 Bytes
    - L2CAP kann bis zu 64kByte über eine Operation verschicken.
    - L2CAP stellt dazu sicher, dass nur Teilpakete einer einzigen Anwendung hintereinander über die Verbindung gesendet werden. Damit ist gewährleistet, dass die Empfängerseite ein Paket komplett rekonstruieren kann bevor andere Teilpakete eintreffen.
  - zusätzliche Einstellungen von Dienstgüteeigenschaften je logischem Kanal:
    - Dienstgütetyp
      - Keine Dienstgüteeigenschaft, weitere Einstellungen werden ignoriert
      - Best Effort : keine Garantie für Dienstgüte, aber Vorgaben werden so gut wie möglich erfüllt
      - Garantie: Anwendung kann sich auf die Einhaltung der Parameter verlassen. (L2CAP kann Garantieanforderung ablehnen, wenn beispielsweise Bandbreite nicht garantiert werden kann.

- Token rate, toke bucket size: Kreditmodell , das angibt, mit welcher Datenrate gesendet werden soll.
  - Token rate gibt an mit wie viel Bytes pro Sekunde im Durchschnitt gesendet werden sollen
  - Token Bucket size: Kreditrahmen für kurzfristige Überschreitungen der token rate. Ist der (Kredit-)Rahmen erschöpft wird die sendende Anwendung blockiert, bis wieder genug Kredite zur Verfügung stehen.
- Maximale Bandbreite: Byte die pro Sekunde maximal versendet werden dürfen
- Latenzzeit: Zeit in Millisekunden, die maximal zwischen Übergabe des Paketes an L2CAP und versand über die Funkschnittstelle vergehen darf
- Verzögerungsschwankung: Differenz zwischen maximaler und minimaler Dauer eines Übertragungsvorgangs
- Parameter die auf „do not care“ gesetzt werden, werden ignoriert.
  - hauptsächlich für Datenübertragung entworfen. Audioverbindungen auf der Basis von SCO-Links müssen sich direkt an die Basebandschicht wenden.
  - Prinzipiell zwar auch Audioübertragung über Datenkanal möglich, jedoch stehen dann keine reservierten Bandbreiten zur Verfügung, deshalb keine gleich bleibende Audioqualität gewährleistet.
  - AUX1 wird nicht verwendet, da keine Fehlererkennung möglich ist.
  - Keine Funktionen zur Sicherung des Datenkanals, zuverlässiger Datentransport bleibt der Basebandschicht überlassen.
  - Logische Kanäle werden über Channel Identifier (CID) identifiziert

0x0000	Null	Rückgabewert mit spezieller Bedeutung, darf nicht für einen logischen Kanal verwendet werden
0x0001	Signalisierung	Wird benutzt um weiter logische Kanäle einzurichten
0x0002	Empfang von Multicastnachrichten	
0x0003-0x003f	Reserviert	
0x0040-0xffff	Frei verfügbar	CIDs auf unterschiedlichen Geräten müssen nicht korrespondieren, jedes Gerät kann eigene Belegung vornehmen.

- 2 Kanalarten
  - Verbindungsorientierte Kanäle: zuverlässige bidirektionale Datenverbindung zwischen zwei Geräten
  - Verbindungslose Kanäle: ein Sender kann Nachrichten an mehrere Empfänger gleichzeitig versenden.
    - Definition von Empfängergruppen über logische CID-Verknüpfung
    - Verbindungslose Nachrichten erreichen den Empfänger grundsätzlich über CID 0x0002
    - L2CAP bietet spezielle Funktionen für die Verwaltung von Empfängergruppen an.
- Identifikation eines speziellen Dienstes erfolgt über Protocol an Service Multiplexer (PSM)-Nummern
  - PSM identifiziert einen speziellen Dienst ungeachtet unter welchen speziellen CID er angeboten wird
  - PSM sind immer ungerade Nummern.
  - Die Werte 0x0001, 0x0003 und 0x00005 sind für die Dienste Service Discovery Protocol (SDP), RFCOMM und TCS-BIN reserviert.
  - Der Wertebereich 0x1001 bis 0xffff steht zur freien Verfügung

## Zusammenfassung Mobile Computing (1679)

- Host Controller Interface (HCI)
  - Kommandoschnittstelle für höhere Schichten zum Zugriff auf die Basebandfunktionne
- Service Discovery Protocol (SDP)
  - Ermöglicht es Dienste anderer Bluetoothgeräte zu suchen
    - Von denen die Dienstklasse bekannt ist (z.B. Drucken)
    - Mit konkreten Attributen (z.B. drucken mit 600 dpi)
    - Übersicht der verfügbaren Dienste zu erstellen
  - Geräte die Dienste anbieten wollen müssen einen SDP-Server installieren
  - Bei Geräten, die lediglich Dienste nutzen wollen reicht ein SDP-Client
  - Nur Informationen über Dienste, Dienstnutzung ist nicht Bestandteil des Protokolls.
  - Keine Weitervermittlung von Diensten, es werden nur eigene Dienste vom SDP-Server angegeben
  - Keine Zugriffskontrolle, d.h. jedes Gerät kann auf alle Dienstdaten zugreifen und alle Dienste nutzen
  - Keine Rechnungserstellung für Dienstnutzer
  - Keine Nachrichten über die Verfügbarkeit von Diensten. Ausfälle oder Veränderungen von Dienstparametern werden nicht an potenzielle Nutzer weitergeleitet.
  - PSM-Nummer 0x0001 ist in L2CAP fest für SDP-Verbindungen registriert.
  - Verwaltung der Dienste im SDP-Server erfolgt über eine Datenbank, die eine Menge von Service Records als Einträge verwaltet.
  - Ein Service Record repräsentiert eine Menge von Attributen bestehend aus AttributID und AttributWert.
  - AttributID = 16 Bit Nummer, die das jeweilige Attribut repräsentiert. Einige Attribute haben eine feste Bedeutung, deren Attributwerte müssen entsprechend der speziellen Bluetooth-Spezifikation formatiert sein.
    - 0x0000 ist der Service Record Handle, der in allen Records die Bedeutung einer eindeutigen Recordidentifikation.
  - Attributwerte unterstützen eine Reihe von Datentypen
    - Nil: leerer Eintrag
    - Int: 1,2,4,8 oder 16 Bit Integer mit oder ohne Vorzeichen
    - Universal Unique Identifier UUID 128 Bit Zahl, die weltweit eindeutige Identifikation z.B. von Browsgroups und Dienstklassen erlaubt.
    - String: Zeichenkette
    - Boolean : Wahrheitswert
    - Universal Ressource Locator (URL) Zeichenkette die beispielsweise den Standort im Internet für weitere Informationen angibt.
    - List: Listen der vorgenannten Datentypen, auch Listen von Listen sind darstellbar.
  - Die Attribute Service RecordHandle und ServiceClassIDList sind für jeden Service Record verpflichtend vorgeschrieben.
    - Klassen geben vor, welche Attribute vorgeschrieben sind und welche Bedeutung sie haben.
    - Sind mehrere Klassen angegeben, so handelt es sich um eine Klassenhierarchie und es müssen die Attribute aller genannten Klassen angegeben sein.
    - Keine zentrale Administration der Klassen vorgeschrieben.

## Zusammenfassung Mobile Computing (1679)

- Die Verbreitung der Klasseninformationen obliegt den Herstellern
- ProtocolDescriptorList beschreibt, über welche Protokolle ein Dienstnutzer einen Dienst in Anspruch nehmen kann.
- RFCOMM
  - Emulation serieller Schnittstellen gemäss RS232 über Bluetooth
  - Bis zu 60 virtuelle Schnittstellen können simultan betrieben werden.
  - RFCOMM-Verbindungen werden über die fest vergebene PSM-Nummer 0x0003 identifiziert.
  - Mit RFCOMM können Anwendungen die eigentlich für serielle Schnittstellen konzipiert sind ohne Veränderung miteinander über den Bluetooth-Protokollstapel kommunizieren.
  - Beispielsweise nutzen die Internetprotokolle UDP und TCP das Point-to-Point Protokoll über die serielle Schnittstelle, dass eigentlich für Modemverbindungen gedacht war. Damit können Internetverbindungen über Bluetooth hergestellt werden.
  - Allerdings ist die TCP/IP Unterstützung nicht komplett, da keine Weiterleitung von Paketen zwischen Piconets möglich ist. Eine solche Routingfunktion müsste durch höhere Schichten realisiert werden.
  - Weitere Einsatzmöglichkeit ist das OBEX-Protokoll, dass von Bluetooth nahezu unverändert aus IrDA übernommen wurde, es wurde „nur“ die Transportschicht TinyTP durch RFCOMM ersetzt.
- Telephony Control Protocol Spezificaton Binary (TCS BIN)
  - Funktionen zur Anrufkontrolle bei Telefonen
  - Bluetoothgeräte können so als schnurlose Telefone betrieben werden.
  - Über eine Bluetooth-Basisstation erfolgt die Anrufweiterleitung ins Festnetz, aber auch eine Telefonverbindung zwischen zwei Bluetoothgeräten ohne Basisstation ist möglich.
  - Die Audioverbindung ist nicht Bestandteil von TCS-BIN, sondern läuft über einen SCO-Link, der direkt von der Basebandschicht zur Verfügung gestellt wird.
  - TCS\_BIN wird über Datenverbindungen mit der festen PSM-Nummer 0x0005 abgewickelt.
  - Hauptaufgaben
    - Kontrolle von Anrufen, d.h. Aufbau und Terminierung von Verbindungen über ACL-Kanäle
    - Über verbindungslose Kanäle können mehrere Geräte über eingehende Anrufe benachrichtigt werden
    - Gruppenmanagementdienste ermöglichen die Einrichtung von Teilnehmergruppen (Wireless User Groups WUG)
      - Die Verwaltung erfolgt über einen Groupmaster, der mit dem Master des Piconet identisch ist.
  - Während eines Gespräches zwischen zwei Slavegeräten kann für die Dauer der Telefonieverbindung ein Fast Inter Member Access geschaltet werden. In dem die 2 beteiligten Slaves vom WUG-Master genehmigt ein eigenes Piconet aufbauen.

### Vor und Nachteile der Infrarotkommunikation gegenüber der funkbasierten Kommunikation

Eigenschaft	Infrarot	Funk
Reichweite	Klein	Groß
Einsatzumgebung	Nur innerhalb von Gebäuden	Drinnen und draussen
Anordnung von Sender und Empfänger	Sichtverbindung erforderlich	Beliebig innerhalb der Reichweite
Abhörsicherheit	Groß	Klein
Störquellen	Sonnenlicht, Kunstlich, Streuung	Elektromagnetische Störquellen,

## Zusammenfassung Mobile Computing (1679)

	und Reflexionen	Streuung und Reflexion
Frequenzen	Keinerlei Beschränkungen	Hoheitlich geregelt

### Unterschiede IrDA und Bluetooth

Eigenschaft	IrDA	Bluetooth
Bitübertragung	Infrarot	Funk
Geräte mit reduziertem Funktionsumfang	Nur Slave möglich	Jedes Gerät muss Master sein können
Point-to-Multipoint	Nur 1 Slave erlaubt	Ja
Verbindung zwischen Geräten	Nur bei Bedarf wird logische Verbindung eingerichtet	Wenn Geräte in Reichweite
Nicht verbundene Geräte in Reichweite	Normal Disconnect Mode	Park Mode
Unzuverlässiger Broadcast	Ja	Ja
Zuverlässige Bidirektionale Datenübertragung	Ja	Ja
Sicherung	Automatic Repeat Request	Automatic Repeat Request und Forward Error Correction
Bandbreitenreservierung für Audio	Nein	Ja
Überlappung von Netzen	Nein	Scatternet
Bruttoübertragungsgeschwindigkeit	2,4 kBit/s bis 16MBit/s	1 MBit/s
Authentifizierung und Verschlüsselung	Nein	Ja
Einstellung von Dienstgüteparametern	Nein	Ja
Schnittstellen Emulation	Seriell und parallel	Nur seriell
Netzwerkschnittstelle	irLAN	Über RFCOMM (serielle Emulation)
Objektaustausch	IrOBEX	OBEX

## KAPITEL 6: Protokolle zur mobilen und spontanen Vernetzung

### Motivation

- Paketvermittlung des Internet geht von stationären Rechnern aus, die weder ihre Netzwerkadresse ändern, noch zwischen verschiedenen Subnetzen wandern
- Bei der Konzeption des Transportprotokoll Transmission Control Protocol (TCP) wurde davon ausgegangen, dass Pakete selten verloren gehen.

### Verfahren zur Mobilität im Internet

- Dynamic Host Configuration Protocol (DHCP)
  - o DHCP geht auf BOOTP zurück, dass entwickelt wurde um festplattenlose Rechner in Netzwerke einzubinden ohne diese jedes Mal manuell zu konfigurieren. Der Rechner sucht sich einen Server im Netzwerk, der ihn im Hochlaufen mit den nötigen Parametern versorgt.
  - o DHCP konzentriert sich darauf, den Rechner mit den netzwerkspezifischen Parametern zu versorgen ist aber BOOTP-kompatibel.
  - o Eigenschaften:
    - Ein Rechner (DHCP-Client), der in ein Netzwerk eingebunden wird bekommt auf Anfrage automatisch eine freie IP-Adresse zugewiesen.
      - DHCP-Client wird physikalisch ins Netz eingebunden, da er noch keine Netzwerkparameter kennt sind seine Kommunikationsmöglichkeiten stark eingeschränkt
        - o Die Kommunikation baut auf dem unzuverlässigen Transportprotokoll User Datagram Protocol (UDP) auf.

- Üblicherweise werden Netzwerkparameter beim Booten des Clients gesetzt, damit nach dem Start alle Netzwerkfunktionen genutzt werden können. Dafür muss aber das Betriebssystem zu lassen, dass UDP-Nachrichten noch vor dem kompletten Rechnerstart versendet und empfangen werden können.
- In Client ohne IP-Adresse kann als Ziel nicht angesprochen werden. Ein Server, der dem Client eine IP-Adresse zuweisen möchte muss deshalb die Nachricht direkt an die MAC-Adresse senden.
- Relay Agents ermöglichen es DHCP-Anfragen aus Subnetzen ohne eigenen DHCP-Server an Subnetze mit DHCP-Server weiter zu leiten. (moderne Router können als Relay Agents verwendet werden.)
- Der Client gibt per Broadcast eine Suchmeldung nach einem DHCP-Server aus (DHCPDISCOVER)
- Der DHCP-Server sendet als Antwort eine mögliche Netzwerkkonfiguration (DHCPOFFER)
  - Manuell: Hierbei wird die DHCP-Anfrage automatisch an den Systemadministrator weitergeleitet, der manuell eine freie IP-Adresse aus einem dazu hinterlegten freien IP-Adressbereiches des Netzes (Scope/Range) vergibt.
  - Automatisch: Eine freie IP-Adresse wird auf unbegrenzte Zeit vom DHCP-Server automatisch vergeben
  - Dynamisch: Eine freie IP-Adresse wird automatisch für eine bestimmte Zeit zugeteilt (Lease). Nach Ablauf der Zeit muss die Anfrage erneut gestellt werden, sonst kann die IP-Adresse erneut frei vergeben werden.
    - Besonders für mobile Rechner geeignet, da diese sich häufig nicht aus dem nur kurzzeitig genutzten Netz abmelden.
    - Das Lease enthält 3 Zeiten:
      - Gültigkeit des Leases
      - T1: Zeit nach der der Lease über eine erneute DHCPREQUEST zu erneuern ist.
      - T2: Zeit nach der die erneute DHCPREQUEST für den Lease vom DHCP-Server positiv quittiert worden sein muss, sonst muss ich der Client einen neuen Lease besorgen, wenn er über die Gültigkeit des aktuellen Lease hinaus im Netz bleiben will.
  - Der Rechner wird mit zusätzlichen Informationen über das Netzwerk versorgt (Subnetmask, Dynamic Name Server (DNS)-Adresse, Router-Adresse)
  - Optional werden Informationen zu weiteren Servern des Netzes übertragen (Mailserver, Webserver,..)
- Nimmt der Client die Netzwerkkonfiguration an, sendet er dem Server eine Anfrage über IP (DHCPREQUEST), mit der er explizit einwilligt, die angebotene Netzwerkkonfiguration zu nutzen
- Die Übertragung der Informationen, sowie die Einstellung der Parameter auf dem Rechner erfolgt vollständig ohne manuelle Konfiguration durch einen Benutzer

## Zusammenfassung Mobile Computing (1679)

- Ein mobiler Rechner muss lediglich in physischen Kontakt mit einem Netzwerk kommen, dass DHCP unterstützt um ihn analog einem stationären Rechner in dieses Netzwerk einzubinden
- Sicherheitsaspekt
  - Die automatische Vergabe von IP-Adressen an fremde Rechner ist sicherheitstechnisch problematisch, da Rechnern aus dem eigenen Netz in der Regel höhere Zugriffsrechte und Privilegien zu stehen, als Rechnern aus anderen Subnetzen, möchte man in der Regel nicht jedem fremden Rechner eine Subnetzadresse zuweisen.
  - Umgekehrt sind sich einbindende Rechner auf die Vertrauenswürdigkeit des DHCP-Servers angewiesen, damit er sie nicht anweist, Nachrichten über nicht vertrauenswürdige Rechner zu leiten.
  - Lösungsansatz ist die gegenseitige Identifizierung von Client und Server vor Vergabe der IP-Adresse. Hierzu sind jedoch MAC-Adressen nur bedingt geeignet, da sie leicht gefälscht werden können.
- Mobile IP
  - Bietet ein mobiler Rechner selber Dienste an reicht es nicht ihn über DHCP- in ein fremdes Subnetz einzubinden, da er für Dienstonutzer erstmal nicht unter dieser neuen IP-Adresse bekannt und damit unauffindbar ist.
  - Bei Mobile IP bekommt ein mobiler Rechner deshalb eine IP-Adresse zugewiesen, die er auch in fremden Netzwerken behält. Er ist damit stets unter einer festen Adresse erreichbar.
  - Rechnerarten im Konzept von MobileIP:
    - Mobile Host: Der mobile Rechner, der sich zwischen verschiedenen Subnetzen bewegt und dabei durch eine eindeutige IP identifiziert wird.
    - Corresponding Host: Kommunikationspartner, der Rechner der Kontakt zum mobilen Rechner aufnehmen will.
    - Home Agent: Der Heimagent ist der Rechner im Heimatnetzwerk (Heimnetz) des mobilen Rechners, der den mobilen Rechner dort vertritt, so lange sich der mobile Rechner nicht in seinem ursprünglichen Subnetz aufhält. Der Home Agent ist ständig über den aktuellen Aufenthaltsort des mobilen Rechners informiert.
    - Foreign Agent: Der Fremdagent befindet sich im aktuellen Subnetz (Fremdnetz (Visiting Network)) des mobilen Rechners und leitet eingehende Pakete an den mobilen Rechner weiter.
  - 2 Adressen pro mobilem Rechner:
    - Heimadresse: Adresse unter der der mobile Rechner permanent erreichbar ist.
    - Care-of-Adresse: IP-Adresse, die der mobile Rechner in fremden Netzen verwendet
      - Foreign-Agent-Care-of-Adresse: Ein Fremdagent übernimmt die Weiterleitung ankommender Pakete an den mobilen Rechner. Mehrere mobile Rechner können die gleiche Foreign-Care-of-Adresse nutzen
      - Collocated-Care-of-Adresse: Netzwerkadresse des mobilen Rechners im Fremdnetz wird direkt dem Heimagenten als Weiterleitungsadresse übermittelt. Es gibt keinen Fremdagenten. Die Collocated-Care-of-Adresse ist für jeden mobilen Rechner im Fremdnetz verschieden.
  - Arbeitsweise / Verfahren
    - Agent Discovery

- Über Agent Discovery ermittelt der mobile Rechner zunächst, ob er sich im Heimnetz oder einem Fremdnetz befindet. Gleichzeitig ermittelt er welcher Rechner im Subnetz der Heim-/Fremdagent ist.
  - Agent Advertisement: Die Agenten senden periodisch Broadcastnachrichten an alle Rechner des Subnetzes. Rechner die den Netzwerkverkehr mit hören, können so die Agenten identifizieren
  - Agent Solicitations: Der mobile Rechner sendet eine Aufforderung an alle Rechner des Subnetzes ein Agent Advertisement durchzuführen und erzwingt damit eine Verkürzung der Wartezeit.
  - Wird kein Advertisement empfangen geht der mobile Rechner erstmal davon aus, dass er sich im Heimnetzwerk befindet und der Heimagent gestört ist.
    - Er versucht dann den Router des Heimnetzwerkes zu erreichen um diese Annahme zu bestätigen.
      - Befindet er sich nicht im Heimnetzwerk versucht er daraufhin einen DHCP-Server zu erreichen um eine Subnetzadresse zu erhalten, die er so dann als collocated-care-of-Adresse an seinen Heimagenten weiterleitet.
    - An Hand der Advertismentnachrichten kann der mobile Rechner seinen Standort feststellen, insbesondere kann er feststellen, ob sich sein Standort seit dem letzten Advertisment verändert hat.
- Registrierung
  - Hat der mobile Rechner eine Care-of-Adresse (über Fremdagent oder eigen), nimmt er zu seinem Heimagenten Kontakt auf und teilt ihm die aktuelle Care-of-Adresse mit. (Registration Request)
  - Der Heimagent führt eine Liste die jedem von ihm vertretenen Mobilien Rechner die jeweils aktuelle Care-of-Adresse zuordnet. Er bestätigt den aktualisierten Eintrag. (Registration Reply)
  - Da theoretisch jeder beliebige Rechner sich als mobiler Rechner ausgeben könnte und so alle Pakete an sich umleiten könnte wird der Registrierungsdialog über einen gemeinsamen geheimen Schlüssel (Message Digest) abgesichert.
  - Kehrt ein mobiler Rechner in sein Heimnetzwerk zurück deregistriert er sich beim Heimagenten und übernimmt seine Datenpakete wieder direkt selber.
  - Eine Deregistrierung ist auch beim Verlassen eines fremden Netzes erforderlich, wenn der mobile Rechner anschl. für eine bestimmte Zeit unerreichbar ist, damit der Heimagent entsprechend reagieren kann.
  - Da Rechner häufig einfach ausgeschaltet werden ohne die entsprechende Deregistrierung vorzunehmen, können Registrierungen für eine bestimmte Zeit vorgenommen werden, sie sind dann vor Zeitablauf für eine weitere Periode zu bestätigen, sonst werden sie automatisch gelöscht.
- Tunneling
  - Pakete legen auf dem Weg zum mobilen Rechner einen Umweg über den Heimagenten zurück.

## Zusammenfassung Mobile Computing (1679)

- Der Kommunikationspartner kennt ja ausschließlich die Heimadresse des mobilen Rechners.
- Befindet sich der mobile Rechner in einem Fremdnetz, nimmt der Heimagent das Paket für ihn entgegen und kapselt es mit einem weiteren Paket,
- das er an die aktuelle Care-of-Adresse weiterleitet (IP-Tunneling).
- Beim Empfänger wird das ursprüngliche Paket wieder entpackt und dem Empfänger übergeben.
  - Bei Foreign-Care-of wird das entpacken vom Fremdagenten durchgeführt.
  - Beim Collocated-Care-of durch den mobilen Rechner selbst.
- Das Antwortpaket des mobilen Rechners selbst, kann direkt an den Kommunikationspartner versandt werden, vorausgesetzt die Router des Fremdnetzes lassen den Versand von IP-Paketen mit fremden Absenderadressen aus dem lokalen Netz zu. Ist dies nicht der Fall wird auch die Antwort wieder über den Heimagenten getunnelt (Reverse Tunneling). Hierbei packt der Heimagent das Tunnelpaket aus und verschickt das reine Antwortpaket an den Kommunikationspartner.
- Durch das Tunnelverfahren brauchen bestehende Implementierungen nicht geändert zu werden.
- Zukunftsaussichten
  - Das Verfahren ist auf Grund der zahlreichen erforderlichen Zusatzrechner unter IPv4 noch relativ aufwendig, deshalb werden unter IPv6 folgende Vereinfachungen direkt eingearbeitet:
    - Es gibt nur noch collocated-Care-of-Adressen. Der Fremdagent wird damit überflüssig
    - Die Funktionalität des Heimagenten wird in den Heimrouter eingearbeitet, damit entfällt der Heimagent als eigenständiger Rechner.
    - Mobile Rechner informieren involvierte Router, wenn sie sich in ein neues Netzwerk begeben. Das aufwendige Routen über den Heimagenten kann damit entfallen.
- Cellular IP
  - Bei MobileIP ist bei jedem Zellenwechsel eine neue Registrierung notwendig. Für cellulare Netze, in den Rechner häufig die Zelle wechseln (z.B. Mobilfunknetze) ist Mobile IP deshalb ungeeignet.
  - CellularIP bietet deshalb einen zweistufigen Ansatz:
    - Ein MobileIP-Netzwerk vermittelt Pakete an den mobilen Rechner nur grob an das Netzwerk in dem sich der mobile Rechner aktuell befindet.
    - Erst innerhalb der Netzwerkes werden die Pakete über cellularIP an den mobilen Rechner vermittelt.
    - Der Heimagent wird in der Regel nicht von einem Zellenwechsel informiert, solange sich der mobile Rechner innerhalb eines einzigen Zugriffsnetzwerkes aufhält, müssen nur die Routingtabellen des Zugriffsnetzwerkes angepasst werden.
    - Nur beim Wechsel in ein anderes Zugriffsnetzwerk wird der Heimagent informiert.
    - Die Verbindung von Zugriffsnetzwerk und MobileIP-Netzwerk erfolgt über einen Gatewayrechner, dessen Adresse als foreign-care-of-adresse von den mobilen Rechnern genutzt wird.

## Zusammenfassung Mobile Computing (1679)

- Routing
  - Gatewayrechner sendet periodisch Beacon-Nachrichten im Zugriffsnetzwerk aus, die über Fluten verteilt werden.<sup>1</sup>
  - Jeder Rechner merkt sich im Routing Cache von welchem Rechner er die Beacon-Nachricht erhalten hat, damit kennt er den nächsten Nachbarn in Richtung Gateway.
  - Sendet umgekehrt ein mobiler Rechner Pakete zum Gateway, merkt sich jeder Rechner auf der Route die Adresse des Vorgängers.
    - Mobile Rechner die länger keine Nutzdaten verschicken halten die Route durch RouteUpdate-Nachrichten für das Gateway aktuell
  - mit Hilfe der RoutingCaches wird so eine Route vom/zum Mobilien Rechner erstellt.
  - Einträge im RoutingCache werden nach der Zeitspanne RoutingTimeOut gelöscht, damit ist gewährleistet, dass alte Routingeinträge für längst wieder abgewanderte mobile Rechner den RoutingCaches nicht belasten.
- Handover (Handoff)
  - Wird vom mobilen Rechner durchgeführt, wenn die Signalstärke zu stark absinkt.
  - 2 Verfahren
    - Hard Handoff: der mobile Rechner sendet beim Zellenwechsel ein Routeupdate zur neuen Basisstation. Alle Rechner auf der Strecke zum Gateway ändern dadurch ihren Eintrag.
      - Rechner die nicht auf der Route liegen insbesondere die alte Basisstation löschen den Eintrag erst nach Routetimeout
    - Semisoft Handoff: der Rechner schaltet nicht direkt hart zur neuen Basisstation um, sondern empfängt eine zeitlang noch Pakete von beiden Basisstationen, um Paketverluste zu vermeiden, bis das RouteUpdate das Gateway erreicht hat. Erst danach werden nur noch Pakete der neuen Basisstation empfangen.
- Paging:
  - Inaktiver Zustand während dem mobile Rechner nicht mehr an der Kommunikation teilnehmen um Batteriestrom zu sparen, in dem die Funkschnittstelle außer Betrieb genommen wird.
  - Der inaktive Rechner sendet jedoch periodisch Page-Update-Nachrichten zum Gateway um die Routinginformationen im PageCache der Rechner auf der Route aktuell zu halten.
  - Page Einträge sind jedoch wesentlich länger gültig als Routeeinträge und müssen deshalb wesentlich seltener versendet werden.
  - Mit Page Paketen meldet ein Gateway einem inaktiven Rechner, dass für ihn Datenpakete vorliegen. Der inaktive Rechner reagiert darauf mit einem Routeupdate und die Datenpakete können zugestellt werden.
- Mobilität auf Transportebene
  - Das Transmission Control Protocol (TCP) wurde für drahtgebundene Netze entwickelt um eine zuverlässige Ende-zu-Ende-Verbindung herzustellen. Im Gegensatz zu drahtgebundenen Netzen treten in drahtlosen Netzen Bitfehler relativ häufig auf. Die Eigenschaft von TCP auf Bitfehler mit einer verringerten Pakethäufigkeit zu reagieren (Überlastungssteuerung) ist in drahtlosen Netzen kontraproduktiv und führt zu einer miserablen Performance.
  - Lösungsidee: Aufteilung der Strecke in 2 Teilstrecken
    - Drahtgebunden vom stationären Rechner bis zur Basisstation
    - Drahtlos von der Basisstation zum mobilen Rechner

---

<sup>1</sup> Fluten: Beim Fluten werden Nachrichten an alle Nachbarn weitergeleitet, außer an den von dem die Nachricht gekommen ist.

- Eine weitere drahtlose Zwischenstrecke ist bei den folgenden Lösungsansätzen nicht vorgesehen.
- Split-Connection-Verfahren (Hauptvertreter Indirect TCP (I-TCP))
  - Auf der drahtgebundenen Strecke wird TCP unverändert eingesetzt.
  - Die zweite Verbindung ist speziell für den drahtlosen Verkehr entwickelt
  - Die Basisstation verwaltet beide Verbindungen und übergibt die Nachrichten einer Verbindung jeweils an die andere Verbindung.
  - Vorteile
    - Überlastungskontrolle kann für den jeweiligen Abschnitt optimiert werden.
      - Drahtgebunden Verbindung Herabsetzung der Paketrate
      - Drahtlose Verbindung schnelles Nachsenden defekter Pakete
    - Die drahtlose Verbindung kann zusätzliche Funktionen integrieren ohne die stationäre Gegenstelle damit zu belasten:
      - Verbindungsabbrüche
      - Bewegen des Rechners im Raum
      - Reduktion verfügbarer Bandbreite
    - Die Basisstation kann für den mobilen Rechner Verwaltungsaufgaben für die Verbindung übernehmen.
      - Z.B. kann ein vereinfachtes Transportprotokoll zwischen mobilem Rechner und Basisstation, damit der mobile Rechner nicht den kompletten TCP-Protokollstapel beherrschen muss, obwohl der stationäre Sender sein gewohntes TCP-Protokoll verwendet.
        - MobileTCP verwendet beispielsweise zwischen Basisstation und mobilem Rechner kein Sendefenster, sondern ein einfaches Quittungsverfahren und spart zusätzlich durch ein Kompressionsverfahren, dass redundante Informationen aus Paketköpfen eliminiert Bandbreite ein.
  - Wechselt ein mobiler Knoten die Basisstation sind davon auch laufende Verbindungen betroffen. I-TCP löst dieses Problem im Bereich der Transportschicht
    - Die Verbindungsrelevanten Daten (Verbindungsparameter, Status der Sendepuffer,...) werden von der alten Basisstation an die neue übergeben. Dadurch muss keine neue Verbindung aufgebaut werden.
  - Nachteile von Split-Connection-verfahren:
    - 2 facher Verwaltungsaufwand der Basisstation, durch 2 Verbindungen.
    - Verletzung der Ende zu Ende Semantik von TCP, da die Basisstation die TCP-Quittung ausstellt ist nicht wirklich garantiert, dass die Pakete auch die mobile Station fehlerfrei erreicht haben.
- Snoop-Protokoll
  - Arbeitet auf der Vermittlungsschicht und Kombiniert Automatic Repeat Request (ARQ)-Verfahren mit der Sendewiederholung auf Transportebene.
  - Die Basisstation schreibt ein sogenannter SnoopAgent alle Pakete die die Basisstation auf dem Weg zum mobilen Rechner passieren in einen Puffer mit.
  - Gleichzeitig wird der Quittungsverkehr in Richtung des stationären Rechners vom SnoopAgent abgehört.

## Zusammenfassung Mobile Computing (1679)

- Pakete für die positive Quittungen vorliegen werden vom SnoopAgenten aus dem Puffer gelöscht
- Fehlt jedoch laut Quittung ein Paket beim mobilen Rechner fängt der SnoopAgent die negative Quittung ab und sendet das fehlende Paket aus seinem Puffer nach.
- Vorteile:
  - Keine Änderung des TCP-Kommunikationsprotokolls in den Endpunkten.
  - Ende zu Ende Semantik von TCP bleibt erhalten. Bestätigte Pakete sind auch wirklich angekommen
  - Geht der Zustand der Basisstation durch Ausfall verloren wird schlimmstenfalls direkt auf das klassische TCP-Verfahren zurückgegriffen es kommt also höchstens zu Performanceverlusten.
  - Vereinfachter Wechsel der Basisstation der Snoop-Puffer muss nicht zwingend übertragen werden und die neue Basisstation muss nicht zwingend das Snoop-Protokoll beherrschen.
- Problem: verschlüsselte Übertragung
  - Hier werden ggf. auch die Kopfinformationen des Paketes, sowie Quittungen verschlüsselt, damit kann der SnoopAgent nicht mehr die Sequenznummern der Pakete mitlesen die für ein erneutes Senden erforderlich sind.
    - Der Ausweg die Basisstation mit den Schlüsseln auszustatten setzt hohes Vertrauen in die Basisstation voraus.
- Fast Retransmission
  - Bei der Umstellung zwischen den Basisstationen kann es zu Verlusten von Quittungen des mobilen Rechners kommen, die zu einer Herabsetzung der Paketübertragungsrate im reinen TCP führen würden.
  - Deshalb sendet beim fast retransmission verfahren die mobile Station direkt nach der Umstellung auf die neue Basisstation eine Folge von positiven Quittungen über bisher erhaltene Pakete, damit wird die Eigenschaft von TCP ausgenutzt, bei positiven Quittungen über eine reduzierte Anzahl Pakete die fehlenden Pakete nach zu senden ohne die Paketrate zu reduzieren.
  - Vorteile:
    - Kombinierbar mit anderen Verfahren
    - Nur das Verhalten des mobilen Knotens muss modifiziert werden.
- Selektive Quittung
  - Standard mäßig werden bei TCP nur ununterbrochene Folgen korrekt empfangener Pakete quittiert. Fehlt ein einzelnes Paket werden auch alle vielleicht schon korrekt übertragenen Folgepakete noch mal gesendet.
  - Selective Acknowledgments (SACK) erweitern den Quittungsmechanismus von TCP so, dass erfolgreich empfangen Blöcke jeweils spezifiziert durch Anfang und Ende quittiert werden und so nur diejenigen Pakete wiederholt werden müssen, die tatsächlich fehlen.
- Explizit Loss Notification (ELN)
  - Expliziter Hinweis an den Sender auf einen speziellen Paketverlust erleichtern das schnelle Nachsenden der erforderlichen Information.
  - Der Paketverlust ist auf Empfängerseite jedoch relativ schlecht feststellbar, so dass keine ELN generiert werden kann.
- Remote-Socket-Architektur
  - Verwendet nur zwischen Basisstation und stationärem Sender TCP, zum mobilen Rechner wird ein spezielles Last Hop Protocol (LHP) gefahren.

## Zusammenfassung Mobile Computing (1679)

- Die Basisstation dient aus Sicht des stationären Rechners als Stellvertreter für den mobilen Rechner.
- User Datagram Protocol (UDP)
  - Unzuverlässiger verbindungsloser Datentransport
  - Keine Garantien, keine Überlastungskontrolle
  - Keine Ansätze zur Verbesserung
  - Probleme verursachen Anwendungen die UDP nutzen, aber von der fast fehlerfreien Übertragung in drahtlosen Netzen ausgehen und deshalb Übertragungsfehler nicht in der Anwendung auffangen

## Verfahren zum Routing in AdHocNetzen

- Klassifikation von Routingverfahren
  - Adaptive Verfahren automatische Reaktion auf Netzwerkveränderungen - Nicht adaptive Verfahren Routing anhand fester Tabellen (nicht für adHocNetze geeignet)
  - Proaktive Verfahren halten Routingtabellen zu sämtlichen Rechnern im Netz vor, selbst wenn noch nie ein Paket geschickt wurde – reaktive Verfahren ermitteln Routen bei Bedarf, d.h. wenn ein Paket versandt werden soll.
  - Distance-Vector-Verfahren Knoten tauscht nur mit seinem Nachbarknoten Distanzinformationen über Knoten aus, die sich nicht in der Nachbarschaft befinden – Link State Verfahren übermittlung der Distanzinformationen zum unmittelbaren Nachbarn wird über das gesamte Netzwerk verteilt.
    - Link-State-Verfahren
      - suchen von Nachbarknoten über „Hello“-Pakete. Nachbarn beantworten Hello-Pakete und werden so erkannt.
      - Echo-Pakete messen die Distanz zu den Nachbarn, da diese die Echopakete sofort beantworten müssen. (Verwendet man nur die Anzahl der Zwischenschritte als Distanz kann die Versendung von Echo-Paketen unterbleiben)
      - Topology control Message (TC) werden periodisch oder bei Veränderungen der Distanzinformationen erzeugt und enthalten neben der Knotenadresse und der Sequenznummer eine Liste der Nachbarn mit den entsprechenden Distanzen
      - Versenden des TC an alle Knoten des Netzwerkes mittels fluten
        - Hat ein Knoten ein bestimmtes TC-Paket schon mal erhalten und weitergeleitet wird es von ihm vernichtet.
      - Aus den gesammelten Distanzinformationen kann sich jeder Knoten ein Abbild des Netzwerkes erstellen und z.B. mit dem algorithmus von Dijkstra Tabellen für die Wegeauswahl generieren.
- Besonderheiten AdHocNetzwerke
  - Keine feste Infrastruktur die mit vorgegebenen Netzwerkadressen das Routing unterstützt.
  - Sehr dynamische Struktur, die Rechner bewegen sich, die Wegeauswahl muss häufig angepasst werden.
  - Keine ausgezeichneten Router vorhanden, jeder Rechner muss Pakete weiterleiten können.
- Destination Sequenced Distance Vector (DSDV)
  - Proaktives, distance-Vektorverfahren
  - Geht zurück auf Distributed Bellman Ford (DBF)
    - Jeder Knoten im Netz hat Routingtabelle mit Angaben zum Zielknoten, nächsten Nachbarknoten auf dem Weg zum Ziel (Hop) und Gesamtdistanz zum Ziel (Metrik) für jeden Knoten im Netzwerk.
    - Knoten a will an d senden. Bei knoten a steht dafür als nächster Zwischenschritt Knoten b eingetragen, dass Paket geht an Knoten b, der

## Zusammenfassung Mobile Computing (1679)

wiederum in seiner Routingtabelle c als nächsten Zwischenschritt ausmacht. So geht es weiter, bis schließlich das Paket bei d ankommt.

- Die Routingtabellen werden aufgebaut, in dem jeder Knoten mit seinen direkten Nachbarknoten Distanzvektoren austauscht.
- Die Routingtabellen werden mit den ausgetauschten Informationen angepasst.
  - Die Distanz (Metrik) zu den über den Nachbarknoten erreichbaren Knoten ist für den aktuellen Knoten jeweils um 1 länger, als für den Nachbarn, die weil ja der Nachbar als zusätzlicher Hop gilt.
  - Ist für einen Zielknoten dieser neue Wert kleiner, als der bisher vorhandene Metrikwert, wird der neue Wert eingesetzt und der 1.Zwischenhop durch den Nachbarn ersetzt.
  - Nach jeder Änderung der Routingtabelle werden die geänderten Informationen an alle direkten Nachbarn übertragen
- In einem neuen Netz liegen zunächst keine Routingtabellen vor.
- Die Knoten ermitteln zunächst ihre nächsten Nachbarn und legen dafür Tabelleneinträge an. Durch die Verbreitung dieser Informationen an die jeweiligen Nachbarn verbreiten sich nach und nach die Distanzinformationen über das gesamte Netz.
- Problem unterbrochene Verbindungen:
  - Kann ein Knoten seinen Nachbarn nicht mehr erreichen setzt er die Metrik automatisch auf unendlich.
  - Beim anderen Nachbarn steht sie jedoch noch auf 2, so dass der Knoten den unendlichen Wert auf 3 korrigiert, der Nachbar korrigiert daraufhin auf 4 usw. der korrekte unendlich Wert wird jedoch nie erreicht.
- Periodisch bzw. immer wenn ein Knoten eine Topologieänderung erkannt hat, werden Distanzinformationen an die Nachbarn versendet. Entweder einzeln oder als Full Dump aller Einträge
- Erweiterung der Routingtabelle aus dem DBF-Verfahren um die Spalte Sequenznummer, zur Kennzeichnung der Aktualität der Nachricht.
  - Sie wird von dem Knoten vergeben, zu dem die Distanz gemessen wurde und bei jedem Verbreiten der Distanzinformation um 2 erhöht.
- Empfängt ein Knoten eine neue Distanzinformation zu einem Knoten, so wird der Eintrag nur aktualisiert, wenn die Sequenznummer höher ist, als die Sequenznummer des alten Eintrages oder die Sequenznummer gleich geblieben ist, aber sich die Distanz gegenüber dem alten Eintrag verringert hat.
- Nach jeder Verbreitung an alle Nachbarn erhöht der Knoten die eigene Sequenznummer um 2
- Das Verfahren setzt voraus, dass alle Verbindungen bidirektional sind, was in AdHocNetzen nicht immer der Fall ist.
- Unterbrochene Verbindung
  - Stellt ein Knoten eine Verbindungsunterbrechung fest, setzt der den Eintrag bzw. die Einträge zum entsprechenden Knoten auf unbekannt und die Distanz auf unendlich. Außerdem erhöht er die Sequenznummer des „verlorenen“ Knotens um 1.
  - Damit ist sichergestellt, dass sich die Information auf Grund der höheren Sequenznummer im Netz verbreitet.
  - Gleichzeitig wird verhindert, dass ein ggf. neuer Pfad zum ehemaligen Nachbarknoten überschrieben wird, da dieser ja mit einer um 2 gegenüber dem letzten Eintrag erhöhten Sequenznummer durchs Netz verbreitet wird.
- Nachteil: hohe Netzwerklast durch ständigen Versand der Routingtabellen, die dazu bei vielen Knoten recht groß werden.

## Zusammenfassung Mobile Computing (1679)

- Dynamic Source Routing (DSR)
  - o Reaktives Verfahren
  - o Route Discovery: ermittelt möglichst optimalen Weg zum Zielknoten.
    - Liegt für den gewünschten Zielknoten kein Eintrag im Cache vor. Wird eine Nachricht an alle Nachbarn versandt, ob diese den Zielknoten kennen, zusammen mit einer Wegeliste, in der der Anfragende Knoten als Initiator schon eingetragen ist.
    - Die Nachbarn tragen sich selber auf der Liste als Folgeknoten ein und überprüfen ob sie schon einen Pfad zum Ziel kennen oder selbst das Ziel sind.
      - Kennen sie den Pfad zum Ziel, hängen sie ihn an die Wegeliste an und schicken sie auf dem umgekehrten Weg zurück zum anfragenden Knoten (Route Reply)
        - o Gibt es unidirektionale Verbindungen, ist der direkte Rückweg ggf. nicht möglich.
        - o Der Rücksender erstellt dann ein RouteDiscoveryPaket zum ursprünglichen Anfrager und hängt das RouteReplyPaket als Information an, damit ist sichergestellt, dass die Antwort ankommt, vorausgesetzt es gibt einen Rückweg.
      - Kennen sie das Ziel nicht, schicken sie die verlängerte Anfrage an alle ihre Nachbarn mit Ausnahme desjenigen von dem die Anfrage gekommen ist.
      - Existieren zu einem Ziel schon viele Cacheeinträge kann es zu einem Ansturm von Route-Reply-Paketen kommen, dies kann vermieden werden, indem ein Knoten vor Weiterleitung eines Routereplypaketes einige Zeit wartet bevor er das Paket weiterleitet und derweil darauf achtet, ob Reply-Pakete mit kürzerer Route unterwegs sind.
  - o Route Maintenance überwacht den einmal entdeckten Pfad zum Ziel
    - Kann ein Paket auf dem einmal erstellten Pfad nicht versandt werden. sendet der Knoten, der den Fehler feststellt ein Errorpaket an den Absender.
      - Jeder Knoten der das Errorpaket weiterleitet, löscht den entsprechenden Routeneintrag in seinem Cache und guckt, ob ihm evtl. schon eine alternative Route bekannt ist, dann könnte das ursprüngliche Paket über den alternativen Weg geschickt werden
      - Ein Knoten, der einen kürzeren Weg für ein von ihm weitergeleitetes Paket kennt kann unaufgefordert einen Route-Reply an den Sender schicken, dass den kürzeren Weg enthält.
- Optimized Link State Routing (OLSR)
  - o Link-State-Verfahren
  - o Basiert auf Multipoint-Relays, d.h. ausgewählten Nachbarknoten, die besondere Aufgaben bei der Weiterleitung von Kontrollpaketen übernehmen
  - o Bei geschickter Auswahl kann insbesondere der Aufwand beim fluten von Kontrollpaketen stark herabgesetzt werden
  - o Jeder Knoten der vom Ursprungsknoten eine Distanz von 2 hat muss eine Verbindung zu einem Multipointrelay der Distanz 1 haben.
  - o Auswahlverfahren für Multipointrelays
    - Beginne mit einer leeren Menge
    - Füge die Nachbarknoten hinzu, die eine einzige Verbindung zu einem Knoten mit der Distanz 2 darstellen
    - Solange es noch Knoten mit der Distanz 2 gibt, die nicht erreicht werden können,

- Wähle den Nachbarknoten, der die meisten Knoten mit der Distanz 2 abdeckt.
- Decken mehrere Knoten die gleiche Zahl ab, wähle den Knoten mit den meisten Nachbarknoten und füge ihn der Menge N hinzu
- Wenn es einen Knoten in der Menge der Multipointrelays gibt, so dass ohne ihn immer noch alle Knoten erreicht werden können lösche ihn aus der Menge der Multipointrelayknoten
- Kontrollnachrichten und ge“Flutete“ Nachrichten werden nur noch über die Multipointrelays verbreitet, die Netzwerklast sinkt
- Berechnung des kürzesten Weges zu einem Knoten
  - Beginne mit einer leeren Routingtabelle
  - Füge für den Knoten selbst einen Eintrag mit der Distanz 0 ein und für jeden Nachbarknoten einen Eintrag mit der Distanz 1
  - Durchlaufe die Routingtabelle und vergleiche sie mit der Topologietabelle
  - Gibt es einen Eintrag in der Topologietabelle für dessen Selektor in der Routingtabelle ein Zieleintrag ist, lösche den Eintrag aus der Topologietabelle
  - Ist die Topologietabelle leer, ist die Routingtabelle fertig
  - Sonst durchlaufe die Topologietabelle und zeilenweise teste dabei für alle Zeilen, ob es in der Routingtabelle einen Eintrag für den Zielknoten gibt dem Knoten in der Topologietabelle entspricht und dessen Metrik = der aktuellen Hopanzahl ist, dann füge eine entsprechende Zeile in die Routingtabelle ein.
  - Erhöhe den Hopzähler um 1 und fahre beim durchlaufen der Routingtabelle fort.
- Link-Reversal-Routing (LRR)
  - Ermittelt überhaupt einen Weg muss nicht optimal sein.
  - Weginformation wird mit Hilfe eines gerichteten Azyklischen Graphen repräsentiert (DAG)
    - Jedes Paar von Knoten, die sich in gegenseitiger Kommunikationsreichweite befinden, wird durch eine gerichtete Kante verbunden
    - Der Graph ist frei von Zyklen
    - Eine Kante von i nach j wird als Upstream von j und als downstream von i bezeichnet.
    - Unterteilung:
      - Zielorientierte DAG : Der festgelegte Zielknoten ist der einzige im Netz ohne Downstreams.
      - zieldisorientierte DAG Der festgelegte Zielknoten ist der NICHT einzige im Netz ohne Downstreams.
        - Ein disorientierter DAG kann durch umdrehen einiger Kanten in einen orientierten DAG umgeformt werden.
  - Für jeden Zielknoten wird ein eigener zielorientierter DAG aufgebaut. Der Knoten, der ein Paket senden will, wählt den entsprechenden DAG aus und sendet das Paket über einen beliebigen Downstream. Wegen der Zielorientierung kann das Paket nicht in einer Sackgasse landen und erreicht irgendwann das Ziel.
  - Verfahren bei Topologieänderungen, wenn ein Knoten alle Downstreams verloren hat, der nicht der Zielknoten ist:
    - Full-Reversal-Verfahren
      - Umkehrung der Orientierung aller Kanten zu allen Nachbarn. Ggf. „in Serie“ über mehrere Knoten, bis wieder ein zielorientierter DAG entstanden ist.
    - Partial-Reversal-Verfahren

## Zusammenfassung Mobile Computing (1679)

- Wie Full-Reversal, jedoch merkt sich der 2.Knoten von welchem Nachbarn die Änderung kam und dreht diese Kante ggf. nicht direkt wieder zurück, wenn andere zur Verfügung stehen. Stehen keine nicht gedrehten Kanten zur Verfügung werden doch wieder alle gedreht.
- Höhen basiertes Partial-Reversal
  - Jeder Knoten erhält „Höhe“ Daten fließen wie Wasser von oben nach unten. Der Ausgleich erfolgt über „Höhenveränderungen“. Das Verfahren terminiert für zusammenhängende Netzwerke in endlicher Zeit. Zerfällt das Netzwerk in zwei Teile, terminiert das Verfahren nur in dem Teil, in dem sich der Zielknoten befindet.
- Lightweight-Mobile-Routing (LMR)
  - Zusätzliche Benutzung ungerichteter Kanten. Nur die direkten Nachbarn des Zielknoten haben gerichtete Kanten. Erst wenn ein Knoten ein Paket senden möchte wird eine Route zum Ziel berechnet und die Kanten entsprechend gerichtet.
    - Anfragepakete (Query) werden verteilt und weitergeleitet bis ein Knoten eine Route zum Ziel kennt und die Anfrage mit einem
    - Replypaket auf umgekehrtem Weg beantwortet. Transportiert eine Kante ein Replypaket, bekommt sie eine Richtung zum Sender des Replypaketes.
  - Bei Verlust einer Kante werden Failure-Query-Pakete von einem Knoten an alle Nachbarn versandt, die Kanten verlieren daraufhin ihre Richtung.
    - Knoten die durch den Wegfall der Kante keinen Downstream mehr haben senden ihrerseits Failure-QueryPakete
    - Knoten, die noch einen Downstream haben, senden Reply-Pakete und erstellen so eine neue gerichtete Kante.
- Temporary Ordered Routing Algorithm (TORA)
  - Erweiterung des höhenbasierten Partial-Reversal-Verfahrens mit Behandlung des Problems partitionierter Netze. Durch die Einführung zweier zusätzlicher Merkmale Originator (Auslöserknoten der Änderung) und Reflexion (wird gesetzt, wenn die Änderung an einen Knoten gelangt, der ausschließlich downstreams hat, erhält ein Knoten dieselbe Höheninformation ein 2.Mal und ist Reflexion gesetzt kann der Knoten davon ausgehen, dass der Weg zum Zielknoten unterbrochen wurde.)

## Verfahren zur Dienstsuche und Dienstvermittlung in mobilen Umgebungen

- generelles Vorgehen
  - Dienstanbieter registriert Dienst bei lokalem Dienstvermittler
  - Dienstsucher ermittelt alle Dienstvermittler in der Umgebung
  - Dienstsucher fragt bei jedem lokalen Dienstvermittler auf jedem Gerät an, ob ein entsprechender Dienst vorhanden ist.
    - Nur für kleine Netze geeignet, da Dienstsuche sehr aufwendig.
    - In großen Netzen gibt es deshalb einen zentralen Dienstvermittler, auf den alle Geräte für die Registrierung bzw. Suche zugreifen.
  - Der Dienstvermittler der den entsprechenden Dienst anbieten kann, teilt dem Dienstsucher die entsprechenden Modalitäten mit.
- Service Location Protocol (SLP)
  - Ergänzung der zentralen Dienstvermittlung um 3 Arten von Agenten:

## Zusammenfassung Mobile Computing (1679)

- User Agents: sind Prozesse, die auf dem Rechner des Dienstanbieters laufen, sie leiten Suchanfragen weiter und nehmen Suchergebnisse entgegen
- Service Agents: laufen auf dem Rechner des Dienstvermittlers und sorgen für die Registrierung der angebotenen Dienste beim Vermittler
- Directory Agents: laufen auf dem Rechner des Dienstvermittlers, sie nehmen die Registrierungen und Suchanfragen entgegen.
  - Suche nach Directory Agents:
    - Suche per Multicast-Paket, Directory Agent meldet sich daraufhin beim Absender des Paketes
    - Directory Agent sendet periodisch Broadcastnachricht über seine Existenz
    - Mitteilung des Directory Agents im Rahmen der vom DHCP-Server bei der Anmeldung verteilten Informationen.
- Skalierbarkeit
  - In kleinen Netzen können Service Agents so programmiert werden, dass sie auch als Directory Agents für den eigenen Rechner arbeiten.
  - In großen Netzen können mehrere Directory Agents so zusammengeschlossen werden, dass sie ihre Einträge abgleichen
  - Alternativ können in großen Netzen sogenannte Scopes (Dienstgruppen) eingerichtet werden
    - Administrative Scopes: werden automatisch vom Netzwerk vergeben, der Dienstanbieter hat hierauf keinen Einfluss
    - Wählbare Scopes können vom Benutzer ausgewählt werden. (Kann aus Liste verfügbarer Scopes ausgewählt werden.)
- Aufbau von Anfragen und Resultaten
  - Schema ähnlich Internet URLs  
service:<Diensttyp>://<Adressespezifikation>
  - Dienste können nach Spezifikationsmerkmalen gesucht werden:  
lpr//(&(SEITEN\_PRO\_MINUTE==12)(STANDORT==3.ETAGE))
- Java Intelligent Network Infrastruktur (Jini)
  - Auf Java basierende Dienstinfrastuktur
  - Java Virtuell Machine erforderlich und nur von Javaprogrammen aus zugreifbar
  - Verwendet Java Object Serialization und Remote Methode Invokation (Entfernten Methoden Aufruf) aus der Javafunktionalität
  - Verfahren
    - Dienstanbieter führt Discovery durch um mindestens einen Lookupdienst (Dienstvermittler) zu ermitteln.
    - Join des Dienstanbieters beim Lookupdienst trägt Dienst in Lookup ein. (Dienstkennung, Dienstinterface und ggf. weitere Attribute die den Dienst genau beschreiben)
    - Dienstanbieter ermittelt über Discovery mindestens einen Lookupdienst
    - Über einen Lookup (Dienstanfrage) spezifiziert er den benötigten Dienst, als Ergebnis können mehrere Dienste zurückgegeben werden, von denen sich der Nutzer einen aussuchen kann
    - Eigentliche Dienstanfrage erfolgt unabhängig vom Lookupdienst mit den von diesem übermittelten Dienstinterface
  - Verfahren für Dienstsuche (Discovery) entweder über Multicast Request Protocol durch den Sucher oder mittels Multicast Announcement Protocol durch den Lookup Dienst über entsprechende Multicast Nachrichten. Für bekannte Weit entfernte Lookup-Dienste mit bekannter Adresse besteht die Möglichkeit des Unicast Discovery, d.h. der direkten Anwahl des entsprechenden Lookupdienstes.
- Weitere Systeme zur Dienstvermittlung
  - In wireless personal Networks:

## Zusammenfassung Mobile Computing (1679)

- Information Access Services (IAS) IrDA (siehe dort)
- Service Discovery Protocol (SDP) Bluetooth (siehe dort)
- Universal Plug and Play (UPnP)
  - Simple Service Discovery Protocol verwendet so genannte Control Points um die Verwaltung der Netzwerkdienste zu übernehmen.
- Secure Service Discovery Service (SSDS)
  - Neben Dienstvermittlung erfolgt Authentifizierung des Dienstanwenders und Diensteanbieters um Missbrauch zu vermeiden.
  - Hierzu wird zusätzlich eine Certification Authority eingeführt, die die Zertifikate der Kommunikationspartner verwaltet und ein Capability Manager, der die Zugriffsberechtigungen den einzelnen Teilnehmern verwaltet.

## KAPITEL 7: Positionsbestimmung

### Context Awareness?

- Kontext ist jede Information, die die Situation einer Einheit charakterisieren kann, dass in relevanten Bezug zur Interaktion zwischen dem User und der Anwendung dient.

### Location Awareness?

- Eigenschaft von Anwendungen Positionsdaten zu berücksichtigen

### Welche Verfahren/Basistechniken gibt es?

- Cell of Origin (COO)
  - Drahtlose Übertragungssysteme haben nur eine beschränkte Reichweite. Ausgestrahlte Signale können nur in bestimmten Bereichen (Zellen) wahrgenommen werden. Aus der Identifikation der Zelle kann man Rückschlüsse auf die Position ziehen
- Time of Arrival (TOA) / Time Difference of Arrival (TDOA)
  - Elektromagnetische Signale bewegen sich mit Lichtgeschwindigkeit. Die Laufzeit kann mittlerweile präzise bestimmt werden. Ermittelt man den Zeitunterschied zwischen Aussenden und Empfang eines Signals, kann auf die Entfernung geschlossen werden.
- Angle of Arrival (AOA)
  - Werden Antennen mit Richtungscharakteristik verwendet, kann ermittelt werden aus welcher Richtung ein bestimmtes Signal eintrifft.
- Signalstärke
  - Aus der Signalstärke kann auf den Abstand zum Sender geschlossen werden, da die Signalstärke mit dem Quadrat des Abstands vom Sender abnimmt. (Wird allerdings durch äußere Einflüsse ungenau.)
- 

### Satellitenavigation erklären.

- Verfahren mit 3 Satelliten
  - 3 Satelliten mit bekannter Position erforderlich
  - Abstand von den 3 Satelliten wird ermittelt
    - Satellit sendet ein Signal, das den Zeitpunkt des Aussendens ( $t_S$ ) codiert enthält.
    - Der Empfänger vergleicht diesen Zeitpunkt mit der internen Uhr zum Zeitpunkt des Empfangs ( $t_E$ ).
    - Für die Entfernung  $r$  vom Satelliten gilt dann:  $r = c \cdot (t_E - t_S)$ , wobei  $c$  für die Lichtgeschwindigkeit (300.000 km/s) steht
  - terrestrischer Schnittpunkt der 3 Kugeln = Position des Empfängers
  - Kritischer Punkt exakte Zeitmessung Fehler von  $1\mu s$  führt zu 300m Entfernungsdifferenz.
  - Die exakte Uhrzeit des ganzen Navigationssystems wird als Systemzeit bezeichnet.
  - Benutzung von Atomuhren in den Satelliten
  - Hinzuziehung eines weiteren 4. Satelliten zur Steigerung der Genauigkeit
    - Sei  $t'_S = t_S + dt_S$  (unbek. Abweichung der Satellitenzeit zur Systemzeit)
    - analog sei  $t'_E = t_E + dt_E$  (unbek. Abweichung des Empfängers zur Systemzeit)
    - $dt = t'_E - t'_S$  exakte Laufzeit des Signals
    - $d't = t'_E - t'_S$  ermittelte Laufzeit des Signals
    - Berechnet wird stets nur die Pseudoentfernung  $p = c \cdot d't = r + c \cdot (dt_E - dt_S)$
    - Sei nun  $dt_S = 0$ , da die Satelliten ja über genau gehende Atomuhren verfügen, die ständig überwacht und synchronisiert werden.
    - $R$  wird über die Position des Empfängers und des Satelliten in einem kartesischen Koordinatensystem ausgedrückt..

## Zusammenfassung Mobile Computing (1679)

- Für die Pseudoentfernung  $p$  gilt dann:  $p = r + c \cdot dtE = \sqrt{(sx - ex)^2 + (sy - ey)^2 + (sz - ez)^2} + c \cdot dtE$
- Die Gleichung enthält 4 Unbekannte, deshalb ist zur exakten Positionsbestimmung der 4. Satellit erforderlich. Das resultierende Gleichungssystem aus 4 Gleichungen mit 4 unbekanntem ist nicht linear. Die Lösung erfolgt bspw. über iterative Näherungslösungen, die auf Taylor-Reihen basieren.

### Wie funktioniert Global Positioning System (GPS)

- 24 Satelliten befinden sich auf 6 Bahnen mit je 4 Satelliten pro Bahn im Umlauf um die Erde im Abstand von ca. 20200km (zeitweise sind aus Ersatz/Reservegründen sogar bis zu 28 Satelliten auf den Umlaufbahnen unterwegs.)
- Die Satelliten sind so angeordnet, dass von jedem Punkt der Erde aus mindestens 5 und maximal 11 jederzeit über dem Horizont „sichtbar“ sind. Durch Gebäude oder andere Abschattungen kann es sein, dass nicht stets alle „sichtbaren“ Satelliten auch erreichbar sind, aber die benötigte Anzahl von 4 ist in aller Regel verfügbar.
- 2 Dienste zur Positionsbestimmung:
  - Precise Positioning Service (PPS) mit einer Genauigkeit von 22m in der Horizontalen und 27,7 m in der Vertikalen.
    - Der Dienst ist verschlüsselt und kann nur von den Streitkräften der USA und NATO entschlüsselt werden.
  - Standard Positioning Service (SPS) ist für zivile Nutzer verfügbar und verfügt über eine Genauigkeit von 25m in der Horizontalen und 43m in der Vertikalen.
    - Der Dienst wurde bis Mitte 2000 künstlich durch Selective Availability (SA) verfälscht, dass die Uhrzeiten der Satelliten zufällig veränderte und die Bahninformationen verfälschte, so dass die Genauigkeit auf 100, in der Horizontalen und 156m in der Vertikalen beschränkt war.
  - Frequenz 1575,42 Mhz für PPS und SPS bzw. 1227,6 MHz nur für PPS
  - Erkennung der Satellitensignale über CodeDivisionMultipleAccessverfahren.
    - Jeder Satellit hat ein eigenes Pseudo-Random-Noise-Signal (PRN)
    - Der Empfänger kennt alle PRN-Signale und kann so aus den überlagerten Signalen aller Satelliten einzelne Satelliten herausfiltern.
  - Messung der Signallaufzeit mit PRN
    - Der Empfänger verschiebt das ihm bekannte PRN-Signal solange auf der Zeitachse, bis es exakt mit dem vom Satelliten empfangenen Signal übereinstimmt. Aus der Verschiebung kann er dann die Laufzeit des Signals berechnen.
- Aufteilung in Segmente
  - Benutzersegment = Endgeräte zur Positionsbestimmung,
    - können teilweise auch zur Geschwindigkeitsmessung herangezogen werden
      - Zeit zwischen zwei Positionsmessungen messen und den Abstand zwischen den beiden Positionen durch diese Zeit teilen.
      - Dopplereffekt nutzen: Bewegte Objekte erfahren eine Frequenzverschiebung der empfangenen Signale, die Größe der Verschiebung ist ein Maß für die eigene Geschwindigkeit
    - Ablesen der genauen Uhrzeit
    - Nicht möglich ist jedoch die Messung der Ausrichtung (aktueller Winkel des Gerätes) hierzu sind andere Verfahren nötig.
  - Kontrollsegment = Territoriale Kontrollstationen
    - Verwaltung der Satelliten und Korrektur der Satelliten eigenen Daten (Systemzeit, Position, Bahndaten)
    - Monitorstationen berechnen Korrekturdaten, die an die Master Control Station (MCS) weitergeleitet werden.
    - Aufgaben der Master Control Station
      - Sammeln der Korrekturdaten von den Monitorstationen
      - Berechnung von Korrekturinformationen für die Satelliten
      - Übertragung der Bahn- und Positionsinformationen an die Satelliten.
      - Korrektur der Atomuhren der Satelliten
      - Einrichten neuer Satelliten
  - Raumsegment = Satelliten
    - Autonome Energieversorgung über Sonnensegel
    - 16MHz CPU
    - Programmiert in ADA

## Zusammenfassung Mobile Computing (1679)

- Fehlerquellen
  - o Uhrenfehler
  - o Schwankungen in der Umlaufbahn, denn die Gravitationskräfte von Sonne und Mond stören die Umlaufbahnen
  - o Störungen der Atmosphäre
  - o Störungen der Ionosphäre
  - o Multipath-Fehler (reflektierte Signale in der Umgebung des Empfängers)
- Verfahren zur Genauigkeitserhöhung
  - o Differential Global Positioning System (DGPS)
    - Einrichtung zusätzlicher Basis- (Korrektur-)Stationen auf der Erde, deren Position bekannt ist.
    - Die Basisstationen führen für sich selbst Positionsbestimmungen via Satellit durch, da die Positionsbestimmung fehlerbehaftet ist, ergeben sich Differenzen zur tatsächlichen Position
    - Anhand der Differenzen werden Korrekturdaten ermittelt, die den Benutzern im Umkreis der Basisstation mitgeteilt werden, da davon ausgegangen wird, dass bei Ihnen sehr ähnliche Fehler vorliegen.
    - Voraussetzung:
      - Die Entfernung zwischen Empfänger und Korrekturstation ist nicht zu groß
      - Die Korrekturen werden zeitnah übertragen.
      - Die Station und der Benutzer nutzen dieselbe Satellitenauswahl zur Positionsbestimmung (Korrekturdaten stimmen nur für bestimmte Konstellation) Umgehung:
        - o für jeden Satelliten werden Korrekturdaten zur Pseudoentfernung ermittelt und verteilt, so dass die Auswahl der Satellitenkombination keine Rolle mehr für den Korrekturwert spielt.
    - Die Genauigkeit erhöht sich hierdurch auf 1-3m
  - o Wide Area Augmentation System (WAAS)
    - Im Gegensatz zu DGPS wird die Verteilung der von den Monitorstationen ermittelten Korrekturdaten nicht direkt über terrestrische Sender durchgeführt, sondern mit Hilfe geostationärer Satelliten.
- Bildung des Korrekturfaktors Satelliten weise, was wird eigentlich genau korrigiert?
  - o der Abweichungsfaktor der Pseudoentfernung

## Positionsbestimmung in Gebäuden

- Infrarotbaken
  - o Benutzer trägt Active Badge (kleinen Infrarotsender) offen sichtbar an der Kleidung
  - o In den Räumen installierte Infrarotsensoren registrieren die individuellen Signale der Badges und leiten die Positionsinformation über ein Netzwerk an einen zentralen Locationserver weiter.
- Wireless Indoor Positioning System
  - o Umgekehrtes Infrarotverfahren zu den Infrarotbaken.
  - o Diesmal senden die Infrarotbaken die Signale, und der von der Person getragene Active Badge leitet die empfangenen Signale per WLAN an den Location Server weiter, der daraus die Position errechnet und sie dem Badge zurück übermittelt.
- Funkbaken
  - o Ähnlich Infrarotbaken jedoch über Abwicklung über Funkstrahlen statt über Infrarot.
  - o Sicht Hindernisse stören nicht mehr, jedoch Positionsberechnung genau deshalb komplizierter, da mehrere Sensoren gleichzeitig, das Signal empfangen. Genauigkeit deshalb nur bei +/- 3 m
- Radiofrequenzidentifikation (RFID)
  - o Variante der Funkbaken, die active Badges (in diesem Fall RFID-Transponder) haben keine eigene Stromversorgung, sondern beziehen ihre Energie aus den empfangenen Funksignalen, mit denen Verfehle übersandt werden, die entweder Daten in den Speicher laden oder in den Speicher schreiben oder als Antwort zurück funken lassen.
  - o Einsatz zur Verfolgung von Objekten während der Produktion.
- Ultraschallverfahren
  - o Genauigkeit von 10cm
  - o Active Bat gibt auf Anforderung eines Servers kurze Ultraschallimpulse ab, die von Ultraschallsensoren aufgenommen werden, die ihre Empfangsinformationen wiederum an den Location Server weiterleiten. Der berechnet aus diesen Daten die Position des Active

## Zusammenfassung Mobile Computing (1679)

Bat ähnlich der Berechnung bei der Satellitennavigation, jedoch entfällt auf Grund der kurzen Entfernung der Korrekturfaktor für den Zeitversatz.

- Cricket
  - o Dreht die Funktion von Empfänger und Sender im Ultraschallverfahren um. Die fest installierten Baken senden die Ultraschallsignale aus, die von den mobilen Badges empfangen werden.
  - o Das System kommt ohne Server aus
  - o Im Vordergrund steht allerdings auch nicht die genau Positionsbestimmung, sondern die Übermittlung von örtlichen Dienstdaten.
- Visuelle Positionsbestimmung
  - o Auswertung von Videodaten
  - o Ggf. vereinfacht durch spezielle visuelle Tags
- Netzwerkgestützte Positionsbestimmung im GSM-Netz
  - o Durch die Einteilung des Netzwerkes in Zellen ist schon eine grobe Positionsbestimmung durch die Kenntnis der aktuellen Zelle gegeben (Cell Global Identity), die jedoch bei teilweise bis zu 35km großen Zellen für die meisten Anwendungen viel zu ungenau ist.
  - o Besitzt die Basisstation Richtungsantennen, kann darüber der Winkelbereich eingeschränkt werden in dem sich das Mobiltelefon zur Basisstation befindet.
  - o Timing Advance: Aus dem Zeitversatz der Zeitschlitz zwischen Basisstation und mobilem Endgerät lässt sich auf die Entfernung von mobilem Endgerät zur Basisstation in Schritten von ca. 550m schließen
  - o Uplink-Time of Arrival: Befindet sich das Gerät in Reichweite von mindestens 4 Basisstationen kann über eine Laufzeitmessung des Signals zum mobilen Endgerät die Position ähnlich der Satellitennavigation auf 50-150m genau bestimmt werden.
- Netzwerkgestützte Positionsbestimmung bei WLAN
  - o Alle Basisstationen messen Signalstärke des bewegten Rechners
  - o Jeder Punkt im Raum hat x,y Koordinaten, zusätzlich kann auch noch die Ausrichtung d als Winkel zu einer bestimmten Wand angegeben werden.
  - o Lernsystem: Tabelle bekannter Wegepunkte mit entsprechenden Signalwerten muss angelegt werden
  - o Anschließend erfolgt die Ermittlung der jeweiligen Position durch Vergleich der Messdatentabelle mit den aktuell gemessenen Werten der einzelnen Basisstationen.

## Geografische Adressierung

- nicht netzwerkspezifische Adresse dient zur Identifikation des Rechners, sondern geografische Position
- derzeitige Netzwerkadressen sind mit 4 Byte erheblich zu kurz um genaue Positionen zu codieren, dafür wären je nach Genauigkeit bis zu 10 Byte (1,8m Genauigkeit) erforderlich.
- Rechner muss seine geografische Position kennen, bei stationären Rechnern könnte man die fest programmieren, mobile Rechner ändern jedoch ständig ihre Position
- Aktuell werden für die Rechneradressierung die Netzwerktopologien beachtet jedoch nicht die geografische Position.
- Adressierung durch zusätzliches Feld im Paketkopf ist nicht mit existierenden Netzwerkprotokollen kompatibel.
- Einführung von neuen Internetadressen mit IPv6 bietet die Möglichkeit mit einem relativ kleinen Adressanteil von 80 Bit (der 128 Bit großen Adressen) jeden Kubikzentimeter der Erde dreidimensional von 100 km über der Meeresoberfläche bis 10km unter der Meeresoberfläche zu adressieren.
- Außerhalb von Gebäuden könnten auch eingebaute GPS-Empfänger die Positionsbestimmung erleichtern.
- Da geografische Adressierung z.Zt. nicht in den Netzwerkprotokollen integriert ist, muss das Problem mit überlagerten Protokollen gelöst werden:
  - o Geo-Routing-Ansatz
    - Geografische Adressierung der Erdoberfläche in 2 Dimensionen
    - Absender gibt als Zieladresse ein geschlossenes Polygon oder einen Kreismittelpunkt mit gewünschtem Radius an. (beispielsweise über Markierung in einer eingeblendeten Karte)
    - Hierarchisch angeordnete Georouter (Georouter Land, Region, Stadt) leiten das Paket in den entsprechenden Zielbereich weiter, dabei kennt jeder Router die Fläche, die er betreut..
    - Erhält er ein Paket, dass in seinen Servicebereich fällt, leitet er es an die untergeordneten Router weiter, liegt das Ziel (teilweise) außerhalb seines Servicebereiches leitet er es an den nächst höheren Router weiter.

## Zusammenfassung Mobile Computing (1679)

- Den Georoutern sind Geo Nodes untergeordnet, die die Nachricht zwischenspeichern und periodisch versuchen sie im Gültigkeitszeitraum über Basisstationen an alle Geräte (Geo Host) im Servicebereich weiterzuleiten.
- Geonodes, die nicht im exakten Zielbereich liegen verwerfen die erhaltenen Pakete.
- Verbesserungsmöglichkeiten
  - Einmal bekannte Schnitte werden zwischengespeichert, so dass die aufwendigen Schnittoperationen bei bekannten Zielen entfallen können
  - Querverlinkung der Georouter einer Ebene, so dass ggf. eine Hochleitung der Daten entfallen kann.
- Multicast-Ansatz
  - Atome sind die kleinsten adressierbaren Flächen
  - Partitionen sind größere geografische Bereiche (Städte, Regionen, Länder), die aus Partitionen oder Atomen aufgebaut sind
  - Jedes Atom und jede Partition erhält eine eigene Multicast-Gruppen-Adresse
  - Basisstationen werden Mitglied in sämtlichen Multicastgruppen, die in Ihrem Reichweitenbereich liegen.
  - Sender bestimmt Zielpolygon, das kann über Atomgrenzen hinaus gehen.
  - Es wird die kleinste Partition bestimmt, in der das Zielgebiet vollständig eingebettet ist und das Paket an diese adressiert.
  - Die Empfänger kennen ihre eigene Position und verwerfen das Paket, falls sie zwar in der Partition aber nicht im Zielgebiet liegen.
  - Probleme:
    - Verfügbarkeit der MulticastIP-Adressen unter IPv4 erzeugt sehr große Atome
    - Multicastgruppen erfordern in den involvierten Routern einen hohen Ressourcenaufwand
- Geografische Adressierung mit Hilfe von Domain-Name-Servern (DNS)
  - Geografische Informationen zu Rechnern werden als Zusatzinfo in Domain-Name-Servern hinterlegt und können von allen bisher vorgestellten Verfahren zur Adressierung verwendet werden
  - Alternativ können neue Namen definiert werden, die mit geografischen Adressen verknüpft sind: PC1.InformatikZentrum.Ferruni-Hagen.NRW.DE.geo, so dass statt Netzwerkdomänen geografische Domänen verwendet werden.
  - DNS Dienst müsste allerdings angepasst werden, damit ggf. statt der bisher üblichen einer IP-Adresse als Antwort auch Listen von IP-Adressen verarbeitet werden können.

## KAPITEL 8: Sicherheit in Mobilendgeräten

### Grundlagen kryptografischer Verschlüsselung

- symmetrische Verfahren
  - auf Sender und Empfängerseite wird identischer geheimer Schlüssel zur Ver- und Entschlüsselung verwendet
- asymmetrische Verfahren (public-key-Verfahren)
  - Schlüsselpaar aus öffentlichem (bekanntem) und privatem (nur 1 Person bekanntem geheimen) Schlüssel.
  - Spezielle Algorithmen stellen sicher, dass der öffentliche Schlüssel allein nutzlos ist um Daten zu entschlüsseln.
- Hashfunktionen bilden Daten unterschiedlicher Länge auf Zahlen fester Länge ab.
- Sicherheit sollte nie darauf beruhen, dass der Algorithmus selbst geheim bleibt, bei aktuellen Verfahren ist in der Regel der Algorithmus zur Kritik und Analyse offen gelegt, die Sicherheit beruht allein auf der Geheimhaltung der aktuell verwendeten Schlüssel.
- Data Encryption Standard (DES)
  - Symmetrisches Verschlüsselungsverfahren
  - Ein 56 Bit Schlüssel wird 16fach auf die 64 Bit Klartextblöcke angewendet, wobei die Ergebnisse Permutationen unterzogen werden, so dass nachher jedes Bit des Ergebnisses von jedem Bit des Schlüssels und des Klartextes abhängt.
  - Auf der Empfängerseite wird mit dem entsprechenden Schlüssel ein entsprechendes Entschlüsselungsverfahren angewandt, das wieder den Klartext ergibt.
- Triple Data Encryption Algorithmus (TDEA)
  - Weiterentwicklung von DES ein 168 Bit Schlüssel wird in 3 Teile geteilt und der Klartext mit je einem dieser Teilschlüssel verschlüsselt, entschlüsselt, verschlüsselt.
  - Dies soll durch erhöhte Rechenkapazitäten möglich gewordene Brute Force Angriffe verhindern helfen.

## Zusammenfassung Mobile Computing (1679)

- Advanced Encryption Standard (AES) Rijndael-Algorithmus
  - o Günstigeres Laufzeitverhalten als DES und TDEA mit 128-256 Bit Schlüssel
  - o Feste Transformation des Klartextes wird mit dem Schlüssel per XOR verknüpft.
  - o Es werden 10 Runden aus Transformationen und XOR-Verknüpfungen durchgeführt.
- RSA (Rivest, Shamir und Adleman)
  - o Public-Key-Verfahren
  - o Öffentlicher Schlüssel  $e$  und  $n$
  - o Privater Schlüssel  $d$  und  $n$
  - o Verschlüsselung  $C = M^e \bmod n$
  - o Entschlüsselung  $M = C^d \bmod n$
  - o Text wird als Zahl dargestellt und verschlüsselt. Ggf. muss der Text in Blöcke aufgeteilt werden, wenn der Nummernkreis nicht ausreicht.
  - o  $e, d$  und  $n$  werden dabei aus 2 Primzahlen  $p$  und  $q$  ermittelt.
    - $n = p * q$
    - $e$  mit  $\text{ggT}(e, (p-1)*(q-1))=1$
    - $d$  mit  $1 = d * e \bmod ((p-1)*(q-1))$
  - o Wichtig ist es große Primzahlen  $p$  und  $q$  zu verwenden.
  - o Üblich sind heute Schlüssellängen von ca. 300 Dezimalziffern. (1024 Bit)
- Diffie-Hellmann-Schlüsselaustausch
  - o Nur Austausch eines geheimen Schlüssels für die weitere Kommunikation über unsichere Leitung (Anfällig gegen Man in the Middle-Angriff beim Schlüsselaustausch)
  - o Der Datenaustausch selber findet mit Hilfe des Schlüssels über ein beliebiges symmetrisches Verfahren statt.
  - o Zwei Teilnehmer einigen sich auf eine Primzahl  $q$  und eine dazugehörige Primitivwurzel  $a$ , so dass  $a \bmod q, a^2 \bmod q, a^3 \bmod q, \dots, a^{q-1} \bmod q$  jeweils unterschiedlich sind.
  - o  $A$  und  $B$  wählen jeweils privat einen eigenen Wert  $x_a$  aus mit  $x_a < q$  und berechnen  $y_a = a^{x_a} \bmod q$
  - o  $Y_a$  bzw.  $Y_b$  wird jeweils an den Partner übermittelt.
  - o  $A$  und  $B$  berechnen damit identisches  $K$  zu  $K = y_b^{x_a} \bmod q = y_a^{x_b} \bmod q$ ,

Authentifizierung nur ganz grob.

- Zweifelsfreie Feststellung, dass der Kommunikationspartner auch der Kommunikationspartner ist, für den er sich ausgibt.
  - o Pro Nachricht
    - Unterzeichnung mit privatem Schlüssel  $\Rightarrow$  Nachricht kann Absender eindeutig zu geordnet werden.
  - o Pro Verbindung
  - o Über Schlüsselnutzung und über Zertifikate, die Echtheit des Schlüsselseinsetzers dokumentieren.

## Wireless Transport Layer Security (WTLS)

- o Asymmetrisches Verschlüsselungsverfahren (Diffie-Hellmann oder RSA) für die Vereinbarung eines geheimen Schlüssels
- o Anwendungsnachrichten werden symmetrisch verschlüsselt (DES, TDEA,...)
- o Authentifizierung über Hashfunktionen (MD5 oder SHA-1)
- Sitzungszustand:
  - o Sitzungskennung (vom Server willkürlich gewählte Nummer, die die Sitzung identifiziert)
  - o Zertifikat des Kommunikationspartners soweit vorhanden
  - o Gemeinsame Komprimierungsmethode
  - o Hashfunktion zur Bildung authentifizierter Nachrichten
  - o Gemeinsames Geheimnis „Master Secret“ für die Schlüsselbildung
- 3 Protokolle zur Herstellung des Sitzungszustandes
  - o Handshakeprotokoll verabredung der verwendeten Verfahren und Schlüssel und Austausch von Zertifikaten
  - o Change-Cipher-Protokoll. Bestätigungsnachricht für die für die folgende Kommunikation die ausgewählten Verfahren bestätigt, aber nicht mehr zum Handshakeprotokoll gehört.
  - o Alert-Protokoll ermöglicht die Behandlung auftretender sicherheitsrelevanter Fehler während der Sitzung. Führt ggf. zum Abbruch der Kommunikationsverbindung
- Master-Secret:
  - o Grundlage für die Schlüssel, die für den Nachrichtenauthentifizierungscode und den geheimen Schlüssel der symmetrischen Verfahren verwendet werden
  - o Zuerst Berechnung der Vorstufe (pre-Master-Secret)
    - Vereinbarung des preMasterSecrets über Diffie Hellmann Verfahren

## Zusammenfassung Mobile Computing (1679)

- Über RSA: Client verschlüsselt geheimen Wert (preMasterSecret) mit öffentlichem Schlüssel des Servers und sendet diesen an den Server, dieser entschlüsselt ihn mit seinem privaten Schlüssel.
- Aus preMasterSecret, der Zufallszahl aus dem Client Hello und der Zufallszahl aus dem Serverhello wird so dann von Client und Server mit Hilfe eines Pseudozufallszahlengenerators das gemeinsame Master-Secret berechnet.

### "Challenge Response Verfahren"

- Digest-Challenge (Frage) und Digest-Response(Antwort)-Nachrichten System
- Nur wenn die Antwort zur Frage passt, gilt der Partner als authentifiziert.
- Gerät 1 berechnet einen einmal Schlüssel (Pseudozufallszahl bspw. Aus Zeitstempel und privatem Schlüssel verschlüsselt diesen mit einer Hashfunktion (MD5) und schickt dies zusammen mit der Benutzerinformation (Realm) zur Authentifizierungsanfrage an Gerät 2
- Gerät 2 ermittelt die zur Realm gehörige Information (z.B. Kennwort) verschlüsselt diese seinerseits zusammen mit dem Einmalschlüssel und schickt die Antwort an Gerät1
- Gerät 1 seinerseits kennt die Antwort auf die Frage (Kennwort. Zur BenutzerID) und berechnet selber mit dem Einmalschlüssel und dem Kennwort die Hashfunktion (MD5) stimmt das Ergebnis von Gerät 1 mit dem von Gerät 2 übermittelten Ergebnis überein, Gilt Gerät 2 als Authentifiziert.

### GSM-Authentifizierung und Verschlüsselung

- Sicherheitsziele:
  - Schutz vor nicht autorisiertem Telefonieren
  - Schutz vor Abhören einer Sprach oder Datenverbindung (durch 3.)
  - Schutz vor der Bestimmung des Aufenthaltsortes durch 3. (Der Mobilfunkbetreiber muss die Zelle ja kennen.)
- 3 kryptografische Funktionen (A3,A5 und A8), davon 2 (A3 und A8) auf der SIM-Karte und einer (A5) im Mobiltelefon gespeichert.
- 2 Schlüssel (Ki [Identifikation/SIM-Karte]) und Kc [Verschlüsselung])
- Challenge-Response-Verfahren
  - Mobilfunkbetreiber sendet Zufallszahl (128Bit) an Mobiltelefon
  - Mobiltelefon und Betreiber wenden A3 zusammen mit dem gemeinsam bekannten Schlüssel Ki (128Bit) auf die Zufallszahl an.
  - Das Mobiltelefon schickt sein Ergebnis (32 Bit) an den Betreiber
  - Der vergleicht und gibt die Verbindung frei, wenn die Authentifizierung stimmt.
- Aus der Identifizierung (Ki) und der Zufallszahl wird mit Hilfe der Funktion A8 ein gemeinsamer geheimer Schlüssel für die Verbindung (Kc) von Mobilfunkbetreiber und Mobiltelefon berechnet.
- Die Nutzdaten werden dann über die Funktion A5 mit dem Schlüssel Kc für die Übertragung über die Luftschnittstelle verschlüsselt.
  - Es handelt sich um eine Stromchiffre, d.h. jedes Bit der Nutzdaten wird mit genau einem Bit des Schlüssels mittels XOR verknüpft.
- Sicherheit und Roaming
  - Beim Roaming wird die Identifikation durch den Mobilfunkbetreiber des Heimatnetzes durchgeführt, d.h. die Zufallszahl, das Ergebnis der Authentifizierung und Kc (64 Bit) werden beim jeweiligen Heimatmobilfunkbetreiber angefragt.
  - A5 ist einheitlich über Betreibergrenzen hinweg spezifiziert, die Verschlüsselung ist somit kompatibel.
- Anonymität
  - GSM verwendet nach erfolgreicher Authentifizierung nicht die weltweit eindeutige IMSI (International Mobile Subscriber Identity), sondern eine jeweils Temporär vergebene TMSI (Temporary Mobile Subscriber Identity), die zusammen mit der Local Area Identity (LAI) dem Mobilfunkbetreiber eine eindeutige Identifikation ermöglicht, die sich aber bei jedem Zellwechsel ändert.
- Kritik am Sicherheitskonzept
  - Die Funktionen für die Berechnung der Schlüssel sind nicht offen gelegt und können deshalb nicht wissenschaftlich untersucht werden.
  - A5 ist mittlerweile rekonstruiert und die Verschlüsselung zumindest theoretisch gebrochen
  - A3 und A8 verwenden den Algorithmus COMP128, der Schwächen hat, so kann der Schlüssel Ki aus einer Reihe von Authentifizierungsanfragen an eine SIM-Karte berechnet werden, die danach dupliziert werden könnte.
  - Kc ist zu kurz um Brute-Force-Angriffen zu widerstehen.
  - Die Basisstation identifiziert sich nicht gegenüber dem Mobiltelefon, nur umgekehrt erfolgt eine Authentifizierung

## Zusammenfassung Mobile Computing (1679)

### WLAN Verschlüsselung

- Vereinbarung von
- 3 Sicherheitskonzepte
  - o Authentifizierung mittels Zugriffslisten
    - Nur Rechner mit hinterlegter Rechneradresse können zugreifen
    - Problem, Rechneradressen können problemlos geändert werden
  - o Gemeinsames Kennwort für alle Access Points und Stationen über die dann jede Station jede Station authentifizieren kann (Test ob sie im Besitz des Kennwortes ist)
  - o Stationen und Access Points verschlüsseln alle Pakete mit Hilfe des gemeinsamen Kennwortes
    - Verschlüsselung über Wired Equivalent Privacy (WEP)
      - Jeder Teilnehmer im Netz erhält über einen sicheren Pfad einen geheimen Schlüssel
      - Aus dem geheimen Schlüssel wird eine Pseudozufallsfolge generiert, die mit den Daten im Rahmen einer Stromchiffre mit XOR verknüpft wird.
      - Jedes zu sendende Paket wird mit dem Schlüssel symmetrisch verschlüsselt.
      - Da der Empfänger über dieselbe Pseudo-Zufallsfolge verfügt, kann er durch nochmaliges Anwenden der XOR-Verknüpfung die Daten wieder herstellen.
      - Der geheime Schlüssel wird relativ selten geändert. Zur Erschwerung der Analyse wird deshalb zusätzlich zum geheimen Schlüssel ein sogenannter Initialisierungsvektor (IV), der bei jedem Paket verändert werden muss im Klartext dem Paket beigefügt.
      - 2 Schlüssellängen
        - o 40 Bit fester Schlüssel und 24 Bit Initialisierungsvektor
        - o 104 Bit fester Schlüssel und 24 Bit Initialisierungsvektor
      - Der geheime Schlüssel und der Initialisierungsvektor werden verkettet und dienen als Eingabe für den Pseudozufallszahlengenerator (Pseudo Random Number Generator, PRNG), der mit dem Verfahren RC4 aus der Eingabe eine scheinbar zufällige Folge von Bits berechnet.
      - Den Nutzdaten wird zur Überprüfung der Integrität der Daten auf der Empfängerseite noch eine Cyclic Redundancy Check (CRC)-Prüfsumme angehängt. (Integrity Check Value ICV), bevor die Daten verschlüsselt werden.
      - Auf der Empfängerseite wird nach Übertragung der Daten und der Entschlüsselung der ICV neu gebildet und überprüft, stimmt er nicht, wird das Paket verworfen.
      - Identifikation kann vor dem Nachrichtenaustausch im Rahmen Challenge-Response-Verfahren erfolgen.
        - o Dem zu identifizierenden Teilnehmer wird einen 128 Bit Zufallsfolge unverschlüsselt geschickt.
        - o Diese muss vom Empfänger mit WEP-Verschlüsselt zurückgesandt werden.
        - o Nur wenn nach der WEP-Entschlüsselung die ursprüngliche Folge wieder erhalten wird, gilt der Kommunikationspartner als identifiziert
      - Kritik an WEP
        - o Alle Teilnehmer gelten als Vertrauenswürdig, kein Schutz vor Angreifern, die selbst am drahtlosen Netz teilnehmen dürfen
        - o Der kurze 40 Bit Schlüssel bietet keinen Schutz vor Brute-Force-Angriffen.
        - o Einige WLAN\_Karten ändern den Initialisierungsvektor gar nicht bzw. nicht häufig genug
        - o Algorithmus RC4 gilt mittlerweile als nicht mehr sicher, da bei „schwachen“ Schlüsselkombinationen die Kenntnis nur weniger Schlüsselbits genügt um auf die gesamte Ausgabe zu schließen.
        - o 24 Bit Initialisierungsvektor ist zu kurz um ausreichend viele Permutationen zu zulassen, wenn mit hoher Netzlast gearbeitet wird.
        - o CRC—Verfahren ist ungeeignet die Integrität der Pakete zu sichern, da CRC linear ist, kann ein Angreifer einige Bits des Originalpaketes ändern und eine neue CRC-Summe berechnen, ohne den kompletten Klartext des Paketes zu kennen.

Bluetooth Sicherheitskonzept

- 3 Modi
  - o Keine Sicherheit
  - o Sicherheit auf Dienstebene (nach Aufbau einer Verbindung)
    - Authentifikation und Autorisation erforderlich
    - Authentifikation erforderlich
    - Allgemein zugängliche Dienste
    - Über Dienst und Gerätedatenbanken
  - o Sicherheit auf Verbindungsebene (Beim Aufbau einer Verbindung)
    - Mit verschiedenen Funktionen werden aus verschiedenen Angaben Schlüssel gebildet, mit deren Hilfe die Verbindung abgesichert wird.
    - Datenverschlüsselung erfolgt anschließend mittels einer Stromchiffre

**KAPIEL 9: Mobile Endgeräte**

Kategorien mit Beispielen

	Universalgeräte: sind vom Hersteller nicht für einen bestimmten Zweck vorgesehen und erlauben die Installation beliebiger Anwendungen	Spezialgeräte werden für einen bestimmten Einsatzzweck hergestellt und optimiert. Ein anderweitiger Einsatz ist oft nicht möglich
mobile Standardcomputer mit nahezu der gleichen Leistungsfähigkeit wie stationäre Endgeräte	Notebook	Spezielle Computer z.B. in der Vermessungstechnik
Bordcomputer: hochspezialisierte Endgeräte in Fahrzeugen, Flugzeugen, Schiffen etc. die dort festinstalliert sind.	-	Bordcomputer in Fahrzeugen und Flugzeugen
Handhelds: Kleine mobile Computer die gegenüber Standardgeräten über eine stark eingeschränkte Leistungsfähigkeit verfügen. Sie können in einer Hand gehalten und mit der anderen Hand bedient werden	PDA	Nicht programmierbarer elektronischer Kalender, Mobiltelefon, GPS-Empfänger, Digicam,..
Wearables: Endgeräte die am Körper getragen werden (Armband, Kopfbefestigung oder in Kleidung integriert.	Programmierbares Wearable	Armbanduhr, Pulsmesser
Chipkarten: kein selbständiges Endgerät, da Lesegerät für Einsatz benötigt wird, können jedoch teilweise programmiert werden.	Smart Card	SIM-Karte, EC-Karte mit Geldchip, Telefonkarte,..

## Zusammenfassung Mobile Computing (1679)

### Eigenschaften von PDA-Betriebssystemen

- Texteingabe über Graffiti oder eingeblendete Tastatur
- Datenspeicherung und Verwaltung im lokalen Speicher
- Datenübertragung über Infrarot/Bluetooth-Schnittstelle
- Datenabgleich mit „zentral“ Rechner
- Unterstützung mehrerer Anwendungen
  - o Kalender
  - o Adressverwaltung
  - o ToDo-Listen
  - o Notizen
  - o Frei programmierte Anwendungen
  - o Alarmmöglichkeit und Überwachung
- Starten und Beenden von Anwendungen
- PalmOS
  - o Single—Threaded, d.h. keine parallele Programmausführung immer genau eine Anwendung aktiv
  - o Steuerung über Ereignisse die vom Betriebssystem an die Anwendung weitergeleitet werden.
  - o Kontrolle erfolgt ausschließlich über das Betriebssystem
  - o Bis 4.0 kein hierarchisches Dateisystem, ab 4.0 rudimentäres Dateisystem Virtual File System (VFS)
  - o Anwendungen nutzen als Entsprechung zu Dateien Ressourcen (ausführbare Anwendungen, Bilder , Texte und Dialoge der Anwendung) und Datenbanken (Daten der Anwendung)
  - o Zugriff auf die gespeicherten Daten erfolgt satzweise es stehen jedoch bei weitem nicht die Zugriffsmethoden einer relationalen SQL-Datenbank zur Verfügung
  - o Betriebsmodi
    - Ausgeschaltet = Sleep mode = Nur überwachung ein/aus-Schalter und „Alarmergebnisse“ aus den Anwendungen (Erinnerung Kalendereintrag)
    - Eingeschaltet - Running = Bearbeite Ereignis
    - Eingeschaltet - Doze = Warte auf Ereignis
  - o Handschrifterkennung über Graffiti
- Windows CE
  - o Oberfläche an Desktop Windows angelehnt ⇒ Look and Feel eines Desktopcomputers
  - o Erheblich höhere Hardwareausstattung als bei PalmOS erforderlich
  - o Verbesserte Handschrifterkennung durch Programme von drittanbietern möglich
  - o Handheld PCs, HandheldPCs Pro und PocketPCs
  - o Threadfähig
  - o W32-API vorhanden, identisch mit Desktop PC
    - Im günstigsten Fall muss Desktop Anwendung nur neu für den Prozessortyp übersetzt werden, jedoch häufig nicht sinnvoll, da spezielle Anforderungen von HandheldPCs dann nicht unterstützt werden.

## **KAPITEL 9: Datenübertragung in mobilen Umgebungen**

### Object Exchange Protokoll (OBEX)

- Datenaustausch zwischen mobilen Geräten über IrDA oder Bluetooth
- Es können beliebige Objekte ausgetauscht werden, da vor dem Objekt jeweils Daten zum Objekt übertragen werden, damit die empfangende Stelle weiss, wie die empfangenen Daten einzusetzen sind.
- Objektmodell legt fest, wie Informationen über ein Objekt, sowie Objekthinhalte dargestellt werden

## Zusammenfassung Mobile Computing (1679)

- Sitzungsprotokoll legt fest, wie und in welcher Reihenfolge die Informationen über das Objekt zwischen den Kommunikationspartnern übertragen werden
  - o Request-Response-Paradigma
  - o Sitzung= Zeitraum der für eine komplexe Operation aus Benutzersicht benötigt wird, dabei können mehrere Nachrichten ausgetauscht werden
  - o Connect-Nachricht initialisiert OBEX Sitzung
  - o Positive Quittung für alle Nachrichten Success
  - o Put überträgt Daten, get fordert Daten an
  - o Continue quittiert und wartet auf Fortsetzung der Übertragung
  - o Disconnect beendet die Sitzung
  - o Jede Put/Get Nachricht enthält unter Nachrichten (Header)
    - Wie viele Objekte insgesamt übertragen werden
    - Wie der Name des einzelnen Objektes lautet
    - Wie der Typ des Objektes ist
    - Binärdaten des Objektes
    - Eigentlicher Inhalt wird im Header Body übertragen, der mit End of Body abgeschlossen wird.
- Anwendungsmodell gibt an, wie Anwendungen mit Hilfe von OBEX beliebige Daten miteinander austauschen können.
  - o OBEX-Client und OBEX-Server
  - o In der Inbox werden ankommende Objekte abgelegt bzw. liegen Objekte zur Abholung für andere Geräte bereit.
- Authentifizierung auf Basis Challenge-Response-Nachrichten für Sitzungen nicht für einzelne Nachrichten

## SyncML

- Synchronisation von Datenbeständen zwischen stationären Netzwerken und mobilen Geräten
- Synchronisationsprotokoll SyncML Sync Protocol dient der Verständigung der an der Synchronisation beteiligten Partner über die Synchronisation
- Repräsentationsprotokoll SyncML Representation Protocol spezifiziert, wie Daten für den Transport codiert werden und welche Grundoperationen für die Datensynchronisation existieren.
- Initiierung der Synchronisation geht im allgemeinen vom Client aus
- Synchronisationsarten:
  - o 2 Wege Synchronisation: Client und Serverdaten werden durch Austausch der Änderungen seit der letzten Synchronisation miteinander abgeglichen
    - Client sendet seine Änderungen an Server
    - Server sendet seine Änderungen an Client
    - Client sendet seine IDs für neue Servereinträge an Server
    - Server quittiert die Synchronisation
  - o Langsame Synchronisation: Abgleich der Client und Serverdaten, bei der alle Daten übertragen und Feld für Feld miteinander verglichen werden
  - o Einweg-Synchronisation Client: Client sendet alle Änderungen an den Server nicht umgekehrt
  - o Einweg-Synchronisation Server: Server sendet alle Änderungen an den Client nicht umgekehrt
  - o Erneuerungssynchronisation Client: Der Client sendet alle Daten an den Server, der alle Daten überschreibt
  - o Erneuerungssynchronisation Server: Der Server sendet alle Daten an den Client der alle Daten überschreibt
  - o Serverinitiierte Synchronisation Der Server initiiert eine Synchronisation beliebigen Typs
- Die eigentlichen Nachrichten sind in XML aufgebaut

## Zusammenfassung Mobile Computing (1679)

- Ändern Server und Client den gleichen Datensatz, kann es zu Konflikten kommen, diese werden vom SynchEngine behandelt bzw. von diesem zur Lösung an den Benutzer weitergeleitet, wenn eine automatische Lösung nicht durchführbar ist.
- Authentifizierung über Challenge-Response-Verfahren möglich

## vCard

- elektronische Visitenkarte
- Textobjekte aus Tupeln von
  - o Eigenschaftsnamen, [Parameter(n)] und Werten
- Je Eintrag eine Zeile, sind in Ausnahmefällen Zeilenumbrüche erforderlich müssen diese extra gekennzeichnet sein „\“ oder „=0D=0A“ Einzelne Felder innerhalb eines Wertes werden durch ; getrennt
- Vorgesehene Eigenschaften u.a.:
  - o Name der Anzeige
  - o Name (Familienname;Vorname; zusätzlicher Name; Titel; nachgestellter Teil)
  - o Geburtstag
  - o Adresse
  - o Telefon (Fax, Telefon, Mobil)
  - o Email
  - o Zeitzone

## vCalendar

- elektronischer Kalendereintrag
- Textobjekte aus Tupeln von
  - o Eigenschaftsnamen, [Parameter(n)] und Werten
- Je Eintrag eine Zeile, sind in Ausnahmefällen Zeilenumbrüche erforderlich müssen diese extra gekennzeichnet sein „\“ oder „=0D=0A“ Einzelne Felder innerhalb eines Wertes werden durch ; getrennt
- Vorgesehene Eigenschaften:
  - o Startdatum und Uhrzeit
  - o Endedatum und Uhrzeit
  - o Beschreibung
  - o Ggf. Alarm
  - o Wiederholungstermine möglich dazu spezielle Formatangaben täglich, wöchentlich, monatlich, jährlich begrenzt/unbegrenzt
  - o Kategorie
  - o Ort

## **KAPITEL 11: Plattformen und höhere Dienste**

### Grundlagen von WAP

- wireless application protocol (WAP)
- für Zugriff auf das Internet von mobilen Endgeräten vorwiegend Mobiletelefonen aus.
- Spezialisierte Anzeigeformate und Steuerung kaum Übernahme nicht speziell entwickelter HTML-Seiten sinnvoll
- Keine aktiven Komponenten wie javascript oder javaapplets möglich
- Spezieller WAP-Proxy vermittelt zwischen Internet und Mobilfunknetz
- Die „Eingangsdateien für WAP sind WML-Dateien. HTML-Dateien können über einen Filterrechner in beschränktem Masse automatisch übertragen werden.
- Die Ausgangsdateien zum Mobilenden Gerät sind WBXML (binäre XML) Dateien
- Endgeräte müssen über integrierten WML-Browser verfügen
- Sichere Verbindungen über WTLS auf der Luftschnittstelle bzw. SSL/TSL auf der Internetseite möglich. Risikofaktor WAP-Proxy, hier liegen die Inhalte kurze Zeit unverschlüsselt vor.

## Zusammenfassung Mobile Computing (1679)

- WML ähnliche HTML jedoch eingeschränkter Funktionsumfang, da auf mobile Endgeräte zugeschnitten
- Unterscheidung in Karten (Seiten) und Kartenstapel (mehrere Seiten zwischen denen der Nutzer navigieren kann)
- Datenübertragung nur bei Aufruf eines neuen Kartenstapels

## Forschungsplattformen Coda, Rover und Quickstep

- Coda
  - o Spezielles Netzwerkdateisystem für Einsatz mit mobilen Rechnern
  - o Mehrere Server stehen mit unterschiedlichen Verbindungen und identischen Daten/Diensten bereit
  - o Arbeitet ein Client an einer Netzwerkdatei wird diese automatisch auf die lokale Platte übertragen
  - o Bei Unterbrechung der Netzwerkverbindung zu allen Servern, kann der Client auf der lokalen Datenkopie normal weiterarbeiten
  - o Liegt wieder eine Netzwerkverbindung vor, werden die Änderungen an den Server übertragen
  - o Benutzer können Dateien explizit für den lokalen Cache auswählen, so können auch seltener benutzte Dateien im lokalen Cache gehalten werden bzw. ein Client auf eine drohende Trennung vorbereitet werden.
  - o Evtl. durch parallele Änderungen auf verschiedenen Rechnern entstandene Konflikte müssen je nach Art ggf. manuell gelöst werden
- Rover
  - o Nicht erfolgte Dateimodifikationen werden übertragen, sondern die Operation die zur Modifikation führte wird übertragen und am Server nachvollzogen
  - o 2 wesentliche Mechanismen
    - RDO Relocatable Dynamic Objects Verschiebbare Objekte, die auf verschiedenen Rechnern lauffähig sind und ihren internen Datenzustand speichern und rekonstruieren können
    - QRPCs Queued Remote Procedure Calls nicht blockierende Aufrufe die die Kommunikation zwischen Rechnern herstellen. Da sie nicht blockieren kann am aufrufenden Rechner auch bei Verbindungsunterbrechung sofort weitergearbeitet werden. Eine asynchrone Callback-Prozedure wird beim Eintreffen des Ergebnisses aufgerufen.
  - o Jedes RDO hat einen „Original“ Home Server.
  - o Die Anwendung selbst ist in 2 Teile aufgeteilt
    - Auf dem Server laufen die Anteile die viel Ressourcen benötigen bzw. eine ständige Netzwerkverbindung zu weiteren Rechnern benötigen
    - Auf dem Client läuft zumindest die Benutzerschnittstelle. Aus performance Gründen können auch weitere Anteile auf den Client verlegt werden.
    - Konflikte müssen durch die einzelne Anwendung gelöst werden.
- Quickstep
  - o Speziell für mobile Geräte mit reduzierten Fähigkeiten entwickelt.
  - o Datenaustausch zwischen mobilen Endgeräten über einen zwischengeschalteten Server (z.B. öffentliche Terminkalender)
  - o Satzorientierte Datenbankschnittstelle, wie sie auf Handhelds und Palm PDAs verwendet wird.
  - o Ein Datenbankproxy repräsentiert die Summe aller verbundenen Datenbanken mit denen die jeweiligen lokalen Datenbanken kommunizieren können
  - o Ein anonymisierer befreit z.B. kalendereinträge von persönlichen Daten vor der Veröffentlichung
  - o Die Lebenszeitüberwachung löscht überholte Datensätze aus dem System

## Zusammenfassung Mobile Computing (1679)

- Nur Eigentümer des Datensatzes kann Datensatz ändern, dadurch keine Konflikte möglich