Diplomarbeit

Technische Grundlagen des Nomadic Computing

vorgelegt von

Ralf Staudemeyer

am Institut für Informatik
der Humboldt-Universität zu Berlin

betreut durch

Prof. Dr. Alexander Reinefeld
Hubert Busch

Berlin, den 5. Mai 2002

Danksagung:

Mein Dank gilt Prof. Dr. Alexander Reinefeld, Leiter des Bereichs Computer Science am Konrad-Zuse-Zentrum für Informationstechnik Berlin, und meinem Betreuer Hubert Busch für die Unterstützung beim Entstehen dieser Arbeit. Desweiteren danke ich Anja Weigel für die tatkräftige Hilfe beim Überarbeiten der im Dokument enthaltenen Abbildungen. Außerdem danke ich Bert Staudemeyer und Gregor Baudis für die stetige Motivation und Überarbeitung diverser Fassungen. Ich will mich an dieser Stelle auch bei meinen Freunden für die vielen Diskussionen und die daraus resultierenden Ratschläge bedanken, die dem Vorankommen der Arbeit oft dienlich waren.
Nicht zu vergessen danke ich den Entwicklern von TEX und LATEX, wodurch meine Arbeit in dieser Form präsentiert werden kann. Letztendlich danke ich auch der Open-Source Gemeinde und insbesondere den vielen Entwicklern von Linux, ohne das ein effizientes Arbeiten kaum möglich gewesen wäre.

Inhaltsverzeichnis

1 Einleitung

NOMADISMUS

> ... in wüstenhaften und halbwüstenartigen Gebieten verbreitete Wirtschafts- und Gesellschaftsform, ... die mit nichtseßhafter Lebensweise verbunden ist.

(Meyers Lexikon - Das Wissen von A-Z)

Innerhalb der sich immer schneller entwickelnden Informationsgesellschaft sind die meisten Menschen Nomaden. Wir bewegen uns zwischen unserem Arbeitsplatz und unserem Zuhause mit dem Auto, der Bahn oder dem Flugzeug, sind auf Geschäftreisen oder Kongressen. Doch meist sind unsere Arbeitsrechner an festen Orten, wie an unserem Arbeitsplatz und in unserem Arbeitszimmer. Diese sind dann permanent oder zumindestens zeitweilig durch ein Netzwerk mit einem Server verbunden, der an einem sicherem Ort untergebracht ist.
Oft sind die klassischen Arbeitsplätze in Form von standortfesten, drahtgebundenen Endgeräten nicht verfügbar. Uns umgibt eine neue Arbeitsumgebung, die aus mobilen Endgeräten wie Laptops, Subnotebooks, Handhelds und Mobiltelefonen besteht. Die Eigenschaften dieser Geräte unterscheiden sich partiell sehr stark. So variieren sie hinsichtlich Leistungfähigkeit, genutzter Netzwerkschnittstelle und Qualität der Ein- und Ausgabegeräte.
Wichtigster Aspekt ist dabei der ortsunabhängige und kontinuierliche Zugriff auf benötigte Ressourcen. Dies wird möglich durch die Nutzung drahtloser Kommunikationstechnik.

1.1 Aufgabenstellung

Durch die Nutzung mobiler Endgeräte lässt sich mehr Flexibilität erreichen. Solche Geräte sind klein und leicht, so dass sich überall mit ihnen arbeiten lässt.
Es sind allerdings eine Reihe von Problemen abzusehen, die sowohl die mobile Nutzung drahtloser Kommunikationsnetze, als die von Applikationen betreffen. Diese Arbeit soll klären, wie sich die im verdrahteten Bereich problemlose Kommunikation im entsprechenden Einsatz bei drahtlosen Verbindungen verhält.
Folgende Fragen sollen dabei beantwortet werden:

1. Welche drahtlosen Anbindungsmöglichkeiten gibt es gegenwärting beziehungsweise befinden sich im Aufbau?
   Welche Vor- und Nachteile ergeben sich seitens der Infrastruktur, angebotener Bandbreiten und vorhandener Sicherheitsverfahren?

2. Netzwechsel sollten idealerweise transparent für Nutzer und Applikationen möglich sein. Welche Probleme ergeben sich für das Vermittlungsprotokoll IP, die bei stationären, drahtgebundenen Geräten nicht auftauchen?
   Das Transportprotokoll TCP wurde weder für drahtlosen Umgebungen noch auf Netzwechsel hin ausgelegt. Welche Probleme bestehen und welche Lösungsansätze gibt es?

1.2 Mobile Computing

Beim *Mobile Computing* kommen leichte, portable Geräte zum Einsatz. Dies können Laptops, Subnotebooks, Handhelds, sowie Mobiltelefone mit PDA-Funktionen sein.
Die Geräte sind abhängig von der Stromversorgung. Batteriekapazität ist in mobilen Endgeräten nur in begrenzter Menge vorhanden. Dies macht ein Management gegen Engpässe in der Stromversorgung notwendig. Dabei müssen das Betriebssystem und die genutzten Applikationen Funktionen unterstützen, die die Wiederaufnahme von Sitzungen unterstützen.
Bedingt durch die kleinen Abmessungen und begrenzte Versorgungsenergie haben mobile Geräte schwächere Rechenleistung als stationäre. Sie besitzen langsamere Speichermedien mit geringerer Kapazität. Außerdem verfügen sie über kleine Displays mit zur Zeit aus kostengründen geringerer Darstellungsqualität.
Mobile Computer können viel leichter als stationäre in fremde Hände gelangen. Deshalb sind sie besonders gut gegen unbefugten Zugang und damit gegen Zugriff auf die darauf gespeicherten Daten zu schützen.
Der Zugriff auf notwendige Daten kann aus technischen Gründen (begrenzter Speicherplatz, Diskonnektivität) nicht immer gewährleistet werden. Es müssen lokale Kopien angefertigt und zu gegebener Zeit mit den Originaldaten synchronisiert werden. Um ein kontinuierliches Arbeiten in Zeiten hoher Diskonnektivität zu gewährleisten, sind vorausschauende Replikationsverfahren einzusetzen.
Die Benutzerschnittstellen mit ihren kleinen Abmessungen führen zu einer Reihe ergonomischer Probleme in der Informationsvermittlung vom und zum Endgerät. Besonders interessant wird *Mobile Computing*, wenn die Geräte trotz ihrer Ortsunabhängigkeit vernetzt werden sollen: beispielsweise über das Internet als *Backbone*.
Nomadic Computing ermöglicht es, dass sich jede Aufgabe an jedem beliebigen Ort und auch unterwegs lösen lässt.
Idealerweise sollte es möglich sein, beliebige Kommunikationsverfahren einzusetzen. Drahtgebundene und drahtlose Kommunikationsverfahren mit den unterschiedlichen Übertragungstechniken sollten dabei kein Hindernis sein.
Durch die Mobilität der Teilnehmer entstehen neue Herausforderungen an die Technik im Vergleich zur ortsgebundenen Festnetzkommunikation:

- Die Bandbreite der Luftschnittstelle ist schmal und zudem störanfälliger als die Leitungen des Festnetzes. Zeitweilige Diskonnektivitätsphasen führen möglicherweise zum Abbruch der Kommunikation und müssen ausgeglichen werden. Übertragungsprotokolle und Anwendungen sollten sich der sich ständig ändernden Übertragungsqualität anpassen. Soweit wie möglich müssen Übertragungsfehler, schwankende Bandbreiten und Latenzzeiten sowie Netzwechsel systemseitig gehandhabt werden.

- Vermittlungs- und Transportprotokolle sind nicht auf die Mobilität und die Eigenschaften drahtloser Kommunikationsverbindungen ausgelegt. Der TCP/IP-Protokollstack ist ein zentraler Bestandteil heutiger Kommunikationsnetze. Durch die Erweiterung Mobile IP lässt sich das IP-Protokoll durch eine Mobilitätsunterstützung ergänzen. Änderungen der IP-Adresse werden hier vor der Transportschicht versteckt. So wird Transparenz

auf der Ebene des Transportprotokolls TCP erreicht. TCP-Verbindungen können so Netzwechsel erfolgreich überstehen. Es entstehen hier allerdings neue Probleme, auf die in dieser Arbeit hingewiesen wird.

- Die Luftschnittstelle bietet leichte Angriffsmöglichkeiten. Daten können leicht gestört, verändert und mitgelesen werden. Aus Datenschutzsicht sollte insbesondere das Abhören durch den Einsatz von Authentifizierungs- und Verschlüsselungstechnologien verhindert werden. Verschlüsselungsverfahren werden zunehmend eingesetzt, sind aber meist noch nicht standardmäßig in den Geräten vorhanden.
  Ein weiterer Aspekt ist der Schutz der Privatheit von Lokalitätsinformationen.

- Auch die genutzten Applikationen müssen mit den divergierenden Eigenschaften des Übertragungskanals sowie mit Verbindungsabbrüchen umgehen. Hierzu ist eine zusätzliche Applikationsunterstützung seitens einer *Middleware* notwendig.
  Bei *Middleware* handelt es sich in diesem Zusammenhang um mobilitätsunterstützende Software, die über der verteilten Systeminfrastruktur und unter den Applikationen liegt.

1.3 Anwendungsbeispiel

Typische Routenplanungssysteme, wie sie heute bereits in Fahrzeugen eingesetzt werden, arbeiten auf der Basis einer statischen Datenbank, die zum Beispiel auf einer CD die relevanten Stadtpläne und Landkarten enthält. Ein großer Nachteil bei diesen Systemen ist, dass aktuelle Informationen, die die Streckenführung beeinträchtigen, nicht zur Verfügung stehen. Solche Informationen können Daten über gegenwärtige Baustellen, Verkehrsdichte oder Staus sein. Da sich diese Informationen ständig ändern, ist ein Zugriff auf eine dynamische Datenbank sinnvoll, auf die die Software im Fahrzeug zugreifen kann. Auf Grund der Mobilität des Fahrzeuges ist es naheliegend, dass eine Anbindung des mobilen Systems an ein Verkehrsleitsystem über die Luftschnittstelle erfolgt. Über diese könnten dem Fahrzeug beziehungsweise dessen Führer natürlich noch weitere Informationen zukommen. Denkbar wären zunächst Informationen über das Wetter und aktuelle Verkehrsnachrichten, aber auch Informationen über lokale Dienstleister erscheinen schlüssig:

- Eine in der Nähe befindliche Tankstelle könnte über Ihre Preise informieren.

- Eine Kfz-Werkstatt könnte mitteilen, ob sie eine nötige Reparatur am Fahrzeug durchführen kann und ob Ersatzteile vorrätig sind.

- Eine mobile Pannenhilfe könnte berechtigt werden, Statusinformationen über das plötzlich defekte Fahrzeug einzuholen und entsprechend zu reagieren.

- Ein nahes Hotel könnte über freie Plätze zur Übernachtung informieren und eine Buchung durchführen.

- Geschäfte könnten über ihre Öffnungszeiten und Restaurants über ihre Speisenkarte berichten.

- Selbst die Polizei könnte bei Bedarf auf Informationen über das Fahrzeug zugreifen oder für den Fahrer bereitstellen.

Software im Fahrzeug könnte diese Informationen entsprechend verarbeiten und aufbereiten. Hier liegt ein typisches Anwendungsbeispiel für einen nomadischen Client vor: Die angesprochenen Anwendungen benötigen über die Luftschnittstelle eine relativ hohe Datenübertragungsrate. Um eine ständige Aktualität der Informationen zu gewährleisten, ist eine möglichst lückenlose Anbindung des mobilen Clients an die dynamischen Nachrichten der Umgebung nötig.
Für die personalisierten Dienste ist eine Identifizierung des Clients angebracht. Die übertragenen Daten müssen einem gewissen Sicherheitsanspruch genügen und entsprechend verschlüsselt gesendet werden. Auch ist ein Rückkanal für Daten vom Client notwendig, denn Broadcast-Lösungen reichen für einige der Anwendungen nicht aus.
Um ein solches Szenario zu realisieren, wird eine entsprechende Infrastruktur gebraucht, wie sie heute noch nicht vorliegt. Die bereits existierenden drahtlosen Kommunikationsnetze bieten zwar eine nahezu flächendeckende Anbindung, allerdings fehlt es an nötigen breitbandigen Zugangsbereichen. Die Infrastruktur umfasst auch den wesentlichen Aspekt, dass der Zugriff auf ein einheitliches Datennetz, an das alle potentiellen Kommunikationspartner angebunden sind, wie zum Beispiel das auf TCP/IP basierende Internet, zur Verfügung steht.

2 Drahtlose Kommunikationstechnik

Drahtlose Kommunikationstechnik ist eine der Grundvorraussetzungen für *Nomadic Computing*. Der Netzzugang ist hier nicht mehr auf einen Punkt festgelegt, sondern in einem geographischen Bereich, wo der Netzzugang möglich ist. Diese Bereiche werden als Kommunikationszellen bezeichnet. Die drahtlose Verbindung innerhalb der Zellen erfolgt dabei über Funksignale. Für sehr kleine Zellen lassen sich auch optische Übertragungsverfahren nutzen.
Im Folgenden sollen, nach einer kurzen Einführung in die Grundlagen drahtloser Kommunikationstechnik, aktuelle drahtlose Kommunikationsverfahren hinsichtlich ihrer Tauglichkeit für das *Nomadic Computing* untersucht werden.
Jedes Verfahren wird hinsichtlich der vorhandenen Infrastruktur, der möglichen Bandbreiten und der vom System aus angebotenen Sicherheitsverfahren hin betrachtet.

2.1 Grundlagen drahtloser Kommunikationstechnik

2.1.1 Welleneigenschaften

Bewegende Elektronen erzeugen elektromagnetische Wellen, die sich frei im Raum ausbreiten. Die Zahl der Schwingungen pro Sekunde ist die Frequenz f mit der Einheit Hertz. Der Abstand zwischen zwei Maxima ist die Wellenlänge Lambda λ.
Wellen von 1 MHz haben eine Länge von etwa 300 Metern, Wellen von der Länge eines Zentimeters haben eine Frequenz von 30 GHz.
Elektromagnetische Wellen pflanzen sich im Vakuum mit Lichtgeschwindigkeit fort. Die Ausbreitungsgeschwindigkeit in der Atmosphäre entspricht in etwa der im Vakuum. Dies ist ein absoluter Grenzwert. Je nach Übertragungsmedium verändert sich die Fortpflanzungsgeschwindigkeit.
Der mathematische Zusammenhang zwischen einer Frequenz f, der Wellenlänge λ und der Ausbreitungsgeschwindigkeit c lautet

$$f * \lambda = c$$
$$(\text{mit } c = 2.99778 * 10^8 m/s \approx 3 * 10^8 m/s)$$

Eine drahtlose Übertragung des Digitalsignals erfordert die Umsetzung des Basisbandes in eine höhere Frequenzlage durch Modulation einer Trägerschwingung (Abbildung 1).
Der sinusförmige Träger kann dabei in einem oder mehreren seiner Parameter von dem zu übertragenden Digitalsignal beeinflusst werden. Das modulierte Signal wird dann über eine Senderantenne abgestrahlt. Der Empfänger demoduliert das empfangene Hochfrequenzsignal und das Basisband liegt wieder in der ursprünglichen Form vor.
Es gibt viele verschiedene Modulationsverfahren mit unterschiedlicher Bandbreiteneffizienz und Robustheit gegenüber Störungen des Signals. Die Signalausbreitung einer Welle bei drahtloser Übertragung erfolgt gradlinig in alle Richtungen, sofern sich keine Materie im Ausbreitungsbereich befindet.
Bei Rundstrahlung nimmt die Stärke des Signals quadratisch mit dem Abstand zum Sender ab. Innerhalb eines gewissen Abstands um den Sender ist eine Datenübertragung möglich.

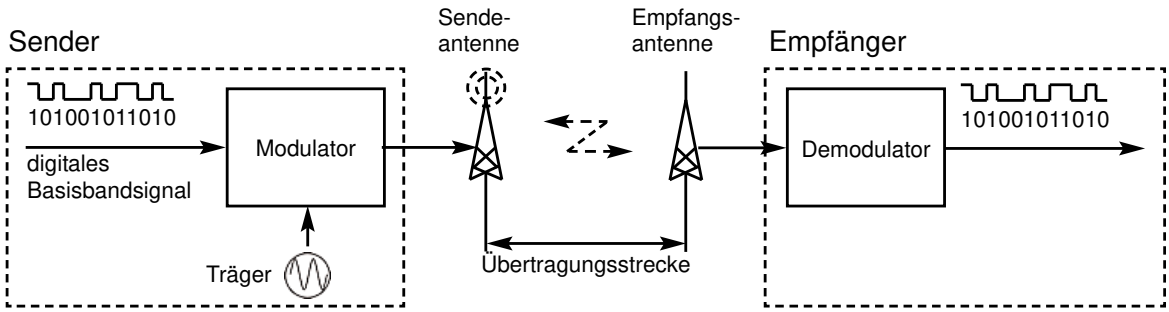


Abbildung 1: Drahtlose Übertragung von digitalen Daten

Dies ist abhängig von der Sendeleistung, der Empfängerempfindlichkeit und von dem Störeinfluß auf die Übertragungsstrecke. Mit zunehmender Entfernung nimmt die Fehlerrate zu, bis eine Rekonstruktion der Daten nicht mehr möglich ist.
Unter realen Bedingungen werden die elektromagnetischen Wellen von der Umwelt in ihrem Ausbreitungsbereich stark beeinflusst. Wellen können an Objekten reflektiert, gebeugt, gebrochen, absorbiert oder gestreut werden. Dadurch kann es zu Mehrwegeausbreitung kommen, und somit zu Interferenzen innerhalb des Übertragungsbereichs. Regen, Schnee, Nebel und Luftverunreinigungen absorbieren die Hochfrequenzenergie. Der Ausbreitungsbereich ist also nie konstant.
Abhängig von der Frequenz der Funkwellen können diese Objekte durchdringen. Bodenoberflächenwellen können dies besser als Direktwellen.
Bodenoberflächenwellen ($\leq$ 3 MHz) breiten sich der Erdkrümmung folgend aus. Sie können auch noch in großer Entfernung, im Tunnel oder unter Wasser empfangen werden.
Wellen höherer Frequenz (3 MHz - 3 GHz) werden als Raumwellen bezeichnet. Langwellige Raumwellen reflektieren an der Ionosphäre und lassen sich für Weitverkehrverbindungen einsetzen. Kurzwellige Raumwellen können noch nichtmetallische Objekte durchdringen, sind aber in ihrer Ausbreitung auf den Horizont beschränkt.
Wellen mit einer Frequenz von über 3 GHz breiten sich als Direktwellen aus. Ihre Ausbreitung ist auf den geometrischen Horizont begrenzt. Mit zunehmender Frequenz werden ihre Eigenschaften denen des Lichtes immer ähnlicher.
[34] [37]

2.1.2 Radiofrequenzen und ihre Regulierung

Radiofrequenzen sind eine begrenzte Ressource. Aus diesem Grund gibt es nationale und internationale Vereinbarungen, um die Nutzung von Frequenzen zu regulieren.
Die ITU-R (International Telecommunication Union - Radiocommunication Sector) übernimmt weltweit diese Aufgabe. Die Empfehlungen der ITU-R sind jedoch nicht bindend, so dass zwischen der europäischen Gemeinschaft, den USA und Japan Unterschiede bestehen.
Die Regulierungen betreffen den Frequenzbereich von 9 kHz bis 275 GHz. Insbesondere die Regulierung niedriger Frequenzbereiche ist aufgrund ihrer großen Reichweiten sehr wichtig.

Ein Überblick auf die vorhandenen Frequenzbänder und die für die Funkübertragung wesentlichen Frequenzbereiche ist in Abbildung 2 dargestellt.
Für Frequenzregulierung ist die Welt ist in drei Regionen unterteilt worden: Europa, Nordamerika und der ostasiatische Kontinent.
Innerhalb der Regionen sind Organisationen für die weitere Regulierung zuständig. Dies ist beispielsweise die CEPT (European Conference for Posts and Telecommunications) innerhalb Europas und die FCC (Federal Communications Commission) in den USA.
Für Standardisierung von Kommunikationstechniken gibt es weitere Organisationen. So werden in Europa fast alle Standards von der ETSI (European Telecommunications Standards Institute) und in den USA von der IEEE (Institute of Electrical and Electronics Engineers) erarbeitet.
Für die Nutzung der meisten Frequenzbänder müssen Lizenzen erworben werden. Drahtlose Kommunikationsnetze nutzen die sogenannten ISM-Bänder (Industrial, Scientific, Medical), welche vorrangig in lizenzfreien Frequenzbereichen arbeiten und weltweit ähnlich angelegt sind. Eines liegt knapp unter 1 GHz, das verbreitetste ISM-Band bei 2.4 GHz.
Zwei weitere befinden sich bei 5.2 und 5.8 GHz, welche allerdings in vielen Ländern noch nicht freigegeben sind.

2.1.3 Mehrfachzugriff auf das Medium

Die Mehrfachnutzung des nur einmal vorhandenen Übertragungsmediums durch mehrere Teilnehmer wird durch Multiplexverfahren möglich. Der Signalraum lässt sich so in mehrere Kanäle aufteilen. Dabei sollen sich verschiedene Teilnehmer möglichst wenig gegenseitig beeinflussen. Die Aufteilung findet in vier Dimensionen statt: Raum, Frequenz, Zeit und verwendeter Code. Die daraus resultierenden Verfahren werden in der Praxis meist miteinander kombiniert.

Raummultiplexing: Beim Raummultiplexing (Space Division Multiplexing, SDM) werden Sender, die die gleiche Frequenz benutzen, unterschiedlichen geographischen Bereichen zugeordnet. So kann gleichzeitig auf derselben Frequenz kommuniziert werden, ohne dass es zu Überlagerungen kommt. Im Abschnitt zum Zellularkonzept wird näher darauf eingegangen.

Frequenzmultiplexing: Durch Frequenzmultiplexing (Frequency Division Multiplexing, FDM) lässt sich das zur Verfügung stehende Frequenzband partitionieren. Diese Einteilung kann statisch oder dynamisch sein. Eine statische Einteilung weist einem Kanal eine Frequenz, wie beim Radio, fest zu. Bei dynamischer Einteilung ist die Frequenz nicht von vornherein festgelegt. In jedem Fall kann ein Sender auf seiner Frequenz ununterbrochen senden. Ein weiterer Sender innerhalb desselben geographischen Bereichs sendet auf einer anderen Frequenz.

Zeitmultiplexing: Zeitmultiplexing (Time Division Multiplexing, TDM) teilt den Signalraum in disjunkte Zeitschlitze. Auch hier kann die Einteilung vorab festgelegt oder anforde-

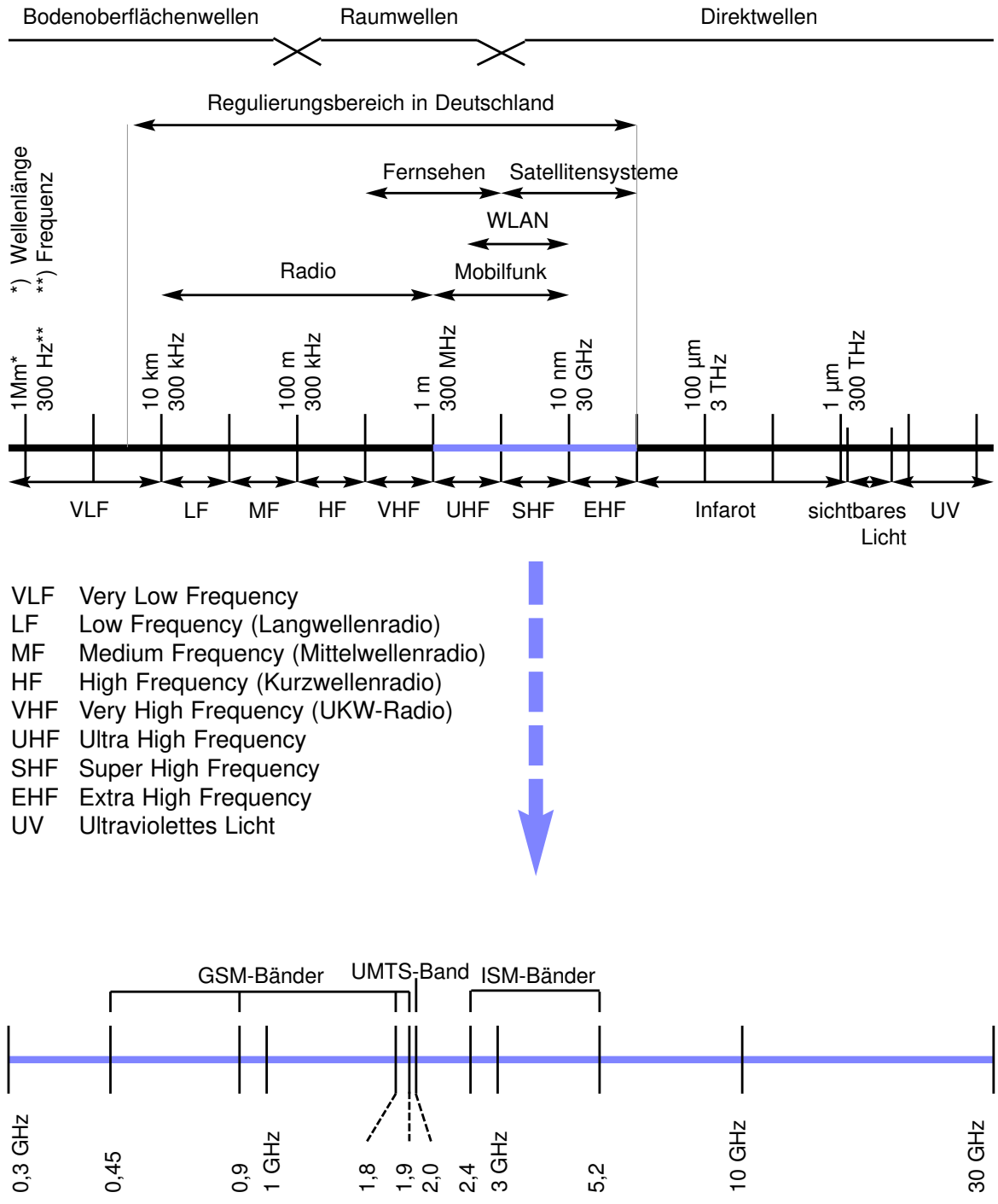


Abbildung 2: Vorhandene Frequenzbänder und für die Funkübertragung wesentliche Frequenzbereiche

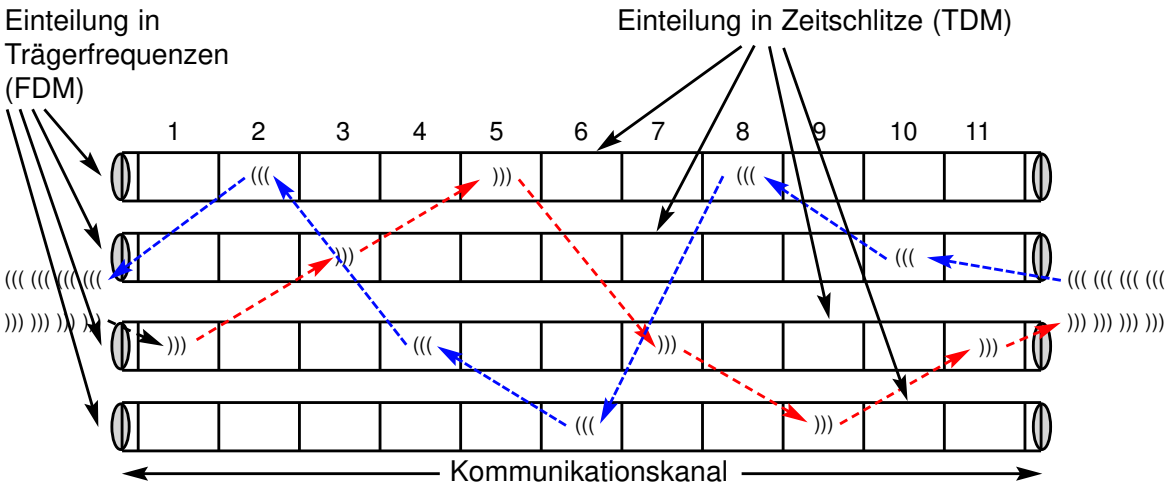


Abbildung 3: Frequenzsprungverfahren

rungsgesteuert sein. Sender auf derselben Frequenz sind hier nur kurze Zeit innerhalb ihres zugewiesenen Zeitschlitzes aktiv.

Codemultiplexing: Bei Codemultiplextechniken (Code Division Multiplexing, CDM) werden die Signale vom Sender mit individuellen Codesequenzen codiert und können vom Empfänger durch auf dem Code basierende Filtertechniken wieder herausgefiltert werden.
Typische Codemultiplexverfahren sind die auf Bandspreiztechnik basierenden FHSS (Frequency Hopping Spread Spectrum) und DSSS (Direct Sequence Spread Spectrum).
Bei FHSS (Abbildung 3) wechselt der Sender nach kurzer Zeit die von ihm genutzten Frequenzen, wobei jeder Sender innerhalb eines Sende- und Empfangsbereichs eine andere Folge von Frequenzwechseln haben muss.
Bei DSSS wird das schmalbandige Signal durch eine geeignete Codiervorschrift auf einen größeren Frequenzbereich gespreizt. Die so erhaltenen Signale lassen sich zeitgleich mit denen anderer Sender im gleichen Frequenzband übertragen. Der Empfänger, dem die Codiervorschrift des Senders bekannt ist, kann das Signal rekonstruieren.
Durch diese Verfahren wird die Übertragung weniger anfällig für die meist schmalbandigen Störungen.
Codemultiplexbasierende Techniken haben den Vorteil, dass alle Sender dasselbe Frequenzband nutzen können. Die entstehenden Zellen verfügend über eine sogenannte weiche Kapazitätsgrenze. Mit zunehmender Teilnehmerzahl erhöht sich der Rauschpegel und es verringert sich die räumliche Ausdehnung des Bereichs, in dem eine Signalrekonstruktion möglich ist. Bei abnehmender Teilnehmerzahl innerhalb der Zelle verhält es sich umgekehrt. Die daraus entstehenden Zellen werden als „atmende Zellen“ bezeichnet.
CDM spielt eine Schlüsselrolle in aktuellen Standards wie beispielsweise UMTS, IEEE 802.11x und HiperLAN2.
Codemultiplexing bietet Sicherheit gegen einfaches Mithören. Wenn der Code nicht bekannt

ist, lässt sich das Signal kaum rekonstruieren[49].

Ein weiteres ergänzendes Verfahren ist das bei neueren Übertragungstechniken eingesetzte OFDM (Orthogonal Frequency Division Multiplexing). Dabei handelt es sich um ein Mehrträgerverfahren.

Der Unterschied zu Einträgerverfahren besteht im zeitgleichen Einsatz von mehr als einer Trägerfrequenz zur Übertragung. Für jeden Teilkanal kann ein eigenes Modulationsverfahren verwendet werden. Dies kann in Abhängigkeit vom Störanteil jedes einzelnen Kanals erfolgen.

In Kanälen mit einem geringeren Störanteil lassen sich mehr Bits pro Hertz codieren, als in Kanälen mit hohem Störanteil. Das verfügbare Frequenzband lässt sich damit nahezu optimal ausnutzen.

OFDM basierende Übertragungsverfahren werden anhand der eingesetzten TDM-, FDM- und CDM- Verfahren unterschieden.

2.1.4 Zellularkonzept

Drahtlose Netze nutzen Raummultiplexing. Das Versorgungsgebiet wird hier in sogenannte Zellen aufgeteilt. Jede Zelle repräsentiert dabei das Sende- und Empfangsgebiet einer Basisstation.

Basisstationen können durch eine auf Richtfunk basierende oder auch drahtgebundene Infrastruktur miteinander verbunden sein. Die Station befindet sich meist im Zentrum der Zelle.

Der Radius entspricht der Sendereichweite. Durch an die Zellgröße angepasste Sendeleistung und geschickte Verteilung von Frequenzbändern ist es möglich, diese mehrfach zu nutzen.

Wie in Abbildung 4 dargestellt, werden Zellen in Clustern zusammengefasst. Dabei soll der Abstand zwischen zwei Zellen mit gemeinsamen Frequenzband maximal werden. Dadurch werden Interferenzen vermieden. Die Zuweisung von Frequenzen und Kanälen auf Cluster oder einzelne Zellen hat wesentlichen Einfluss auf die Netzkapazität und Dienstqualität.

Moderne Systeme wie UMTS umgehen das Problem der Frequenzverteilung durch den Einsatz von Codemultiplexing mit den dadurch entstehenden „atmenden Zellen“. Dies hat den Vorteil, dass die Zelldichte kontinuierlich erhöht werden kann, ohne dass Optimierungsprobleme bezüglich der Frequenzverteilung entstehen.

Zellen lassen sich nach ihrem Radius unterscheiden. Innerhalb von Gebäuden haben sogenannte Pikozellen einen Radius von etwa 10 Metern. Mikrozellen haben außerhalb von Gebäuden Zellgrößen bis zu mehreren 100 Metern. Makrozellen dehnen sich im Kilometerbereich aus. Zellen mit der größten Ausdehnung werden von Satellitensystemen gebildet.

Ein spezieller Typ von Zellen sind sogenannte Umbrellazellen. Diese stellen übergeordnete Zellen dar, die wiederum Zellen enthalten. Umbrella-Zellen dienen insbesondere dazu, die Zahl der Handovervorgänge bei Teilnehmern mit hoher Reisegeschwindigkeit zu verringern [53] [49].

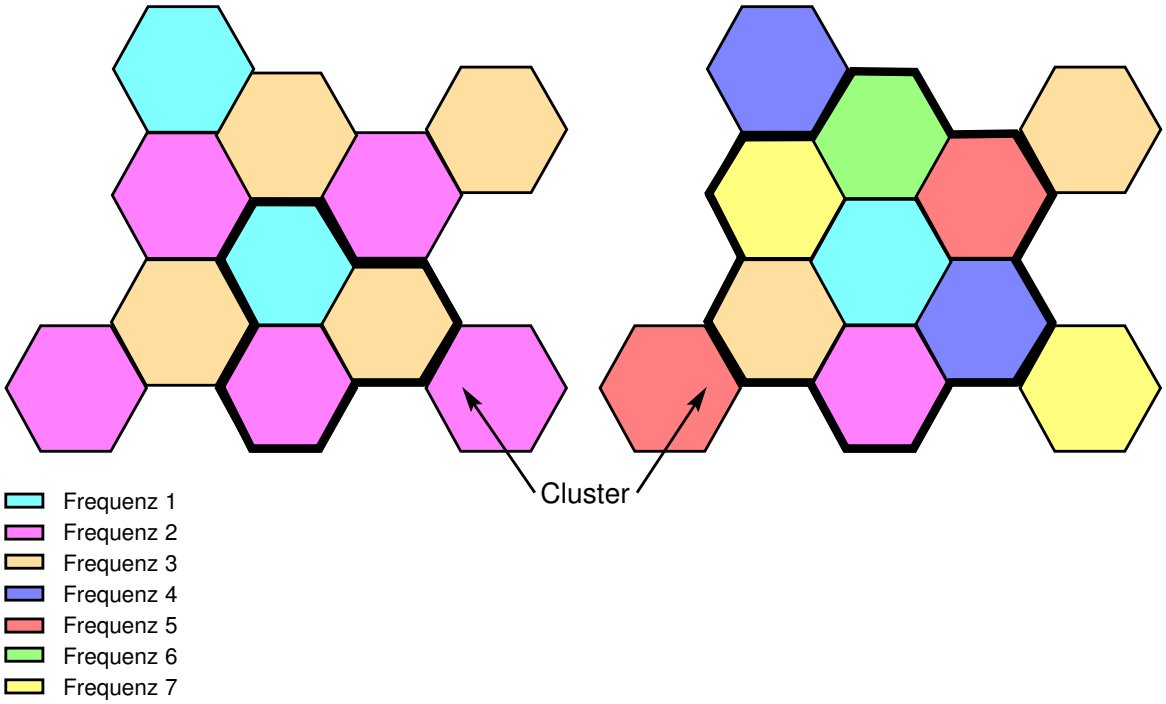


Abbildung 4: Frequenzverteilung beim Raummultiplexing in zellbasierten Funksystemen mit 3er- und 7er-Clustern

2.1.5 Roaming

Durch die Signaldämpfung ist die Reichweite innerhalb einer Zelle eingeschränkt. Wenn ein mobiler Teilnehmer sich in den Bereich einer anderen Zelle bewegt, muss der Netzzugangspunkt gewechselt werden. Solch ein Wechsel des drahtlosen Dienstzugangspunktes, möglichst ohne Störung der Verbindung, wird als *Roaming* bezeichnet.
In Mobilfunknetzen gibt es für die Verbindungsübergabe auch die Bezeichnung *Handover*.
Wenn die Signalstärke innerhalb einer Zelle zu schwach wird, muss das mobile Endgerät eine Suche nach einem neuem Zugangspunkt durchführen. Dabei kann je nach unterstützten Netztypen die Suche aktiv oder passiv sein. Eine passive Suche beschränkt sich auf das Hineinhören in die Luftschnittstelle.
Bei aktiver Suche werden vereinbarte Signale auf allen verfügbaren Kanälen gesendet und auf eine Antwort gewartet. Die Antworten enthalten dann alle notwendigen Informationen, um eine Verbindung mit den neuen verfügbaren Dienstzugangspunkten aufzunehmen.
Auswahlkriterium kann dabei der Sender mit der größten Signalstärke oder die kostengünstigste Übertragungstechnologie sein. Der mobile Teilnehmer schickt dann eine Anfrage zur Aufnahme an den neuen Netzzugangspunkt. Bei negativer Antwort wird eine Alternative probiert, oder die Suche fortgesetzt. Bei positiver Antwort sendet der Dienstzugangspunkt einer zentralen Instanz im Netz den neuen Aufenthaltsort der Station zu.
Netzseitig findet meist eine Aktualisierung innerhalb einer Aufenthaltsortdatenbank statt.

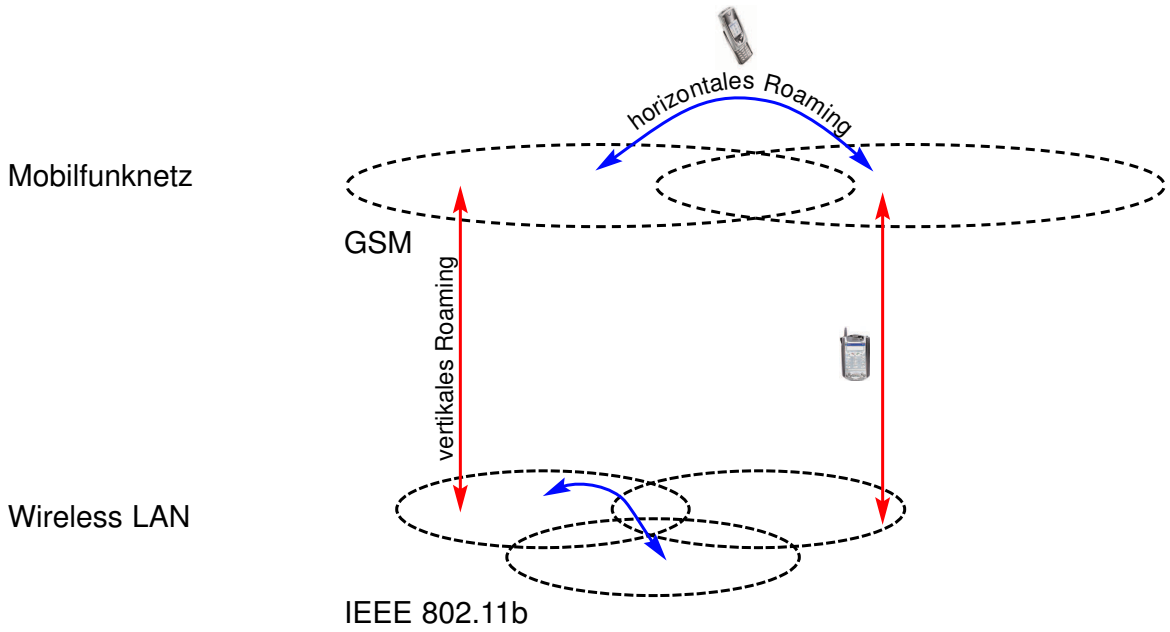


Abbildung 5: Roaming in Mobilfunk- und drahtlosen Kommunikationsnetzen

Es wird zwischen horizontalem und vertikalem Roaming unterschieden. Die beiden unterschiedlichen Verbindungsübergaben sind in Abbildung 5 dargestellt.
Das horizontale Roaming bezeichnet die Intra-Systemübergabe zwischen zwei Zellen, die derselben Netztechnologie angehören.
Das vertikale Roaming ist die Inter-Systemübergabe zwischen zwei unterschiedlichen Netztechnologien. Es ist dabei notwendig, dass alle beteiligten Netztechnologien über ein Netzwerk miteinander verbunden sind [49].

2.1.6 Sicherheit in drahtlosen Netzen

Drahtlose Netze stellen besondere Anforderungen an die eingesetzten Sicherheitsmechanismen. Bei herkömmlichen Netzen muss physikalisch in die Verkabelung oder in einzelne Netzelemente eingegriffen werden, um den Netzverkehr abzuhören. Auch lassen sich Eindringlinge aus anderen Netzen durch einen *Firewall* am Zugang hindern.
Die Ausbreitung der Funkwellen ist jedoch nicht auf das Netzwerk beschränkt. Jeder potentielle Empfänger kann das Medium abhören.
Im Rahmen dieser Arbeit muss deshalb auf zwei Dinge besonders geachtet werden:

1. Authentifizierung
   Es muss sichergestellt werden, dass die Kommunikationsteilnehmer wirklich diejenigen sind, als die sie sich ausgeben.

   Für die Authentifizierung werden meist *Challenge-Response*-Verfahren eingesetzt. Dazu denkt sich das Zielsystem eine Zeichenfolge (Challenge) aus und überträgt diese an

den Kommunikationspartner. Nun müssen beide Seiten mit Hilfe eines passenden Verfahrens, auf Basis der *Challenge*, die *Response* berechnen. Schließlich vergleicht das Zielsystem die vom Kommunikationspartner berechnete *Response* mit der selber berechneten. Sind beide identisch erfolgt die Authorisierung.

Challenge-Response-Verfahren haben herkömmlichen Passwörtern voraus, dass einem potentiellen Angreifer das Mithören nichts nutzt.

2. Vertraulichkeit und Integrität der Kommunikationsinhalte
   Übertragene Daten müssen gegen Abhören durch dritte geschützt werden. Sowohl das Lesen, als auch das Kopieren oder Verändern der Inhalte darf nicht möglich sein. Dies lässt sich durch Verschlüsselung der Daten erreichen. Dabei sollte Verschlüsselung immer mehrseitig sicher sein. D.h. es erfolgt zwischen den Kommunikationsteilnehmern eine Ende-zu-Ende-Verschlüsselung und zusätzlich eine Verschlüsselung während der Funkübertragung durch das gewählte Übertragungsverfahren.

   Bei Verschlüsselungsverfahren wird zwischen symmetrischen und asymmetrischen Methoden unterschieden:

   Bei symmetrischen Methoden arbeiten Sender und Empfänger mit dem selben Schlüssel. Dabei ist es ein Problem, dass der Schlüssel vor der sicheren Kommunikation zwischen Sender und Empfänger bereits ausgetauscht sein muss. Vorteil symmetrischer Kryptographie ist deren hohe Geschwindigkeit beim Ver- und Entschlüsseln von großen Datenmengen.

   Bei der asymmetrischen Verschlüsselung besitzt jeder Kommunikationspartner einen privaten und einen öffentlichen Schlüssel. Zur Verschlüsselung einer Nachricht wird der private Schlüssel des Senders und der öffentliche Schlüssel des Empfängers benötigt, für die Entschlüsselung der private Schlüssel des Empfängers und der öffentliche des Senders.

   Asymmetrische Verschlüsselung ist wesentlich sicherer als symmetrische, jedoch 10 bis 1000 mal langsamer. Alle hier vorgestellten drahtlosen Kommunikationstechniken setzen symmetrische Verschlüsselung ein.

[11]

2.2 Mobilfunknetze

Es werden einige der wichtigsten drahtlosen Kommunikationsnetzwerke vorgestellt. Diese lassen sich grundsätzlich in zwei Klassen unterteilen. Die eine Klasse stammt aus dem Bereich der digitalen Mobilfunkkommunikation. Sie ist aus dem analogen Mobilfunksystem entstanden, das ursprünglich nur die leitungsorientierte Übertragung von Sprache vorgesehen hatte. Das andere System stammt aus dem Bereich der drahtlosen Rechnernetzwerke. Hier wurde von Anfang an der Schwerpunkt in der paketorientierten Datenübertragung gelegt.
Das erste öffentliche Mobilfunknetz war das 1958 eingeführte, mit analoger Übertragungstechnik arbeitende A-Netz. Es verwendete eine Trägerfrequenz von 160 MHz. Gespräche wa-

ren nur innerhalb des A-Netzes möglich und *Handover* war auch innerhalb des Systems nicht vorgesehen. Bis 1971 erreichte das A-Netz eine Flächendeckung von etwa 80%.
In den weiteren Jahren folgten die zellularen B- und C-Netze.
Das B-Netz ermöglichte die Durchstellung von Anrufen in das Festnetz. Anrufe aus dem Festnetz in das B-Netz waren jedoch nur dann möglich, wenn der Aufenthaltsort des mobilen Teilnehmers bekannt war.
Das 1986 folgende C-Netz nutzte einen Träger von 450 MHz. Hier wurden auch die ersten Datendienste eingeführt.
1982 wurde mit der Entwicklung eines europäischen, digitalen Mobilfunkstandard begonnen. Zehn Jahre später ist die erste Version des GSM-Standards (Global System for Mobile Communication) in Betrieb genommen worden. Das GSM-Mobilfunknetz arbeitete anfangs auf 900 MHz, später auch auf 1800 und 1900 MHz.
GSM bietet:

- internationales Roaming
- automatische Teilnehmerlokalisierung
- Authentifizierung von Geräten und Teilnehmer
- Verschlüsselung der Luftschnittstelle
- Integration zusätzlicher Telefonsysteme
- bessere Sprachqualität gegenüber den analogen Mobilfunknetzen
- Kurznachrichtendienst (Short Message Service, SMS)
- Fax- und Datendienste mit einer Bandbreite bis zu 9,6 Kbit/s

Das digitale GSM-System bildet zusammen mit diversen folgenden Trägerdiensten die zweite Mobilfunkgeneration. Ziel der weiteren Modifikation durch Trägerdienste war in erster Linie die Vergrößerung der verfügbaren Bandbreite für Datendienste.
Mit UMTS (Universal Mobile Telecommunication System) wird der Schritt in die dritte Mobilfunkgeneration vollzogen. Ziel von UMTS ist die Umstellung vom verbindungsorientierten Betrieb auf einen vollständig paketorientierten, die Einführung weiterer, leistungsfähiger Datendienste und die Zusammenführung diverser sich stark unterscheidender drahtloser Kommunikationstechniken.
In Abbildung 6 sind die einzelnen Generationen der Mobilfunksysteme dargestellt.

2.2.1 GSM

GSM ist der europäische Mobilfunkstandard und das weltweit erfolgreichste Mobilfunksystem. Es handelt sich dabei um ein rein digitales System der zweiten Mobilfunkgeneration. Im folgenden wird GSM aufgrund seiner Bedeutung ausführlich behandelt. Wichtige Trägerdienste und Teile des Evolutionsprozesses zur dritten Mobilfunkgeneration basieren auf der vorhandenen GSM-Infrastruktur.

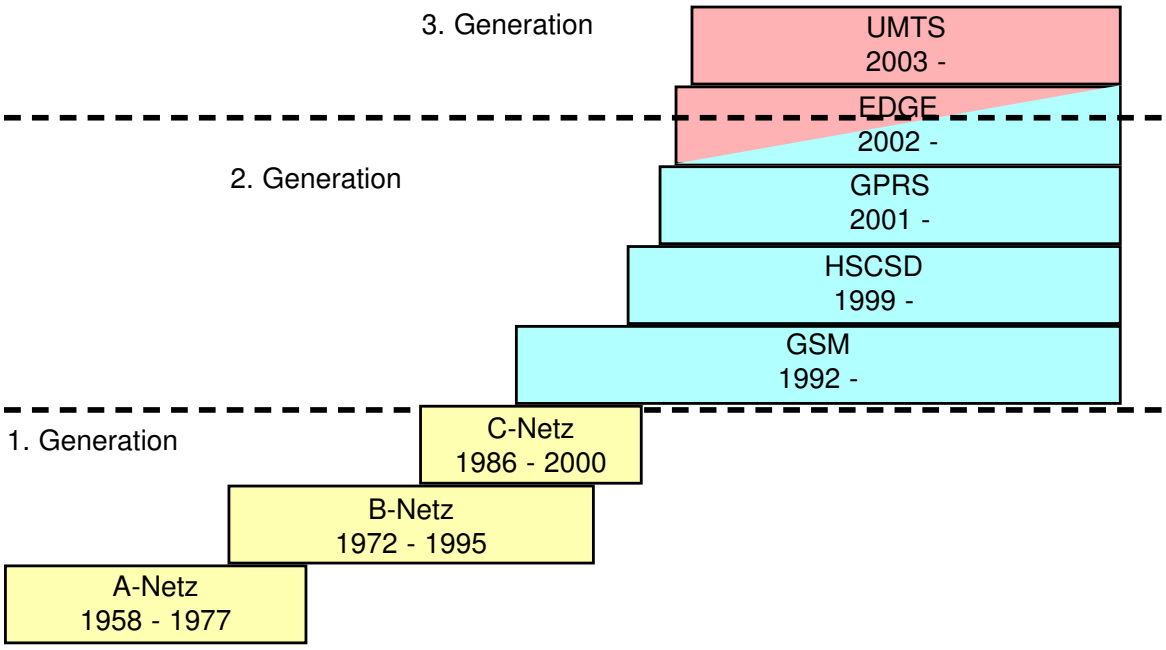
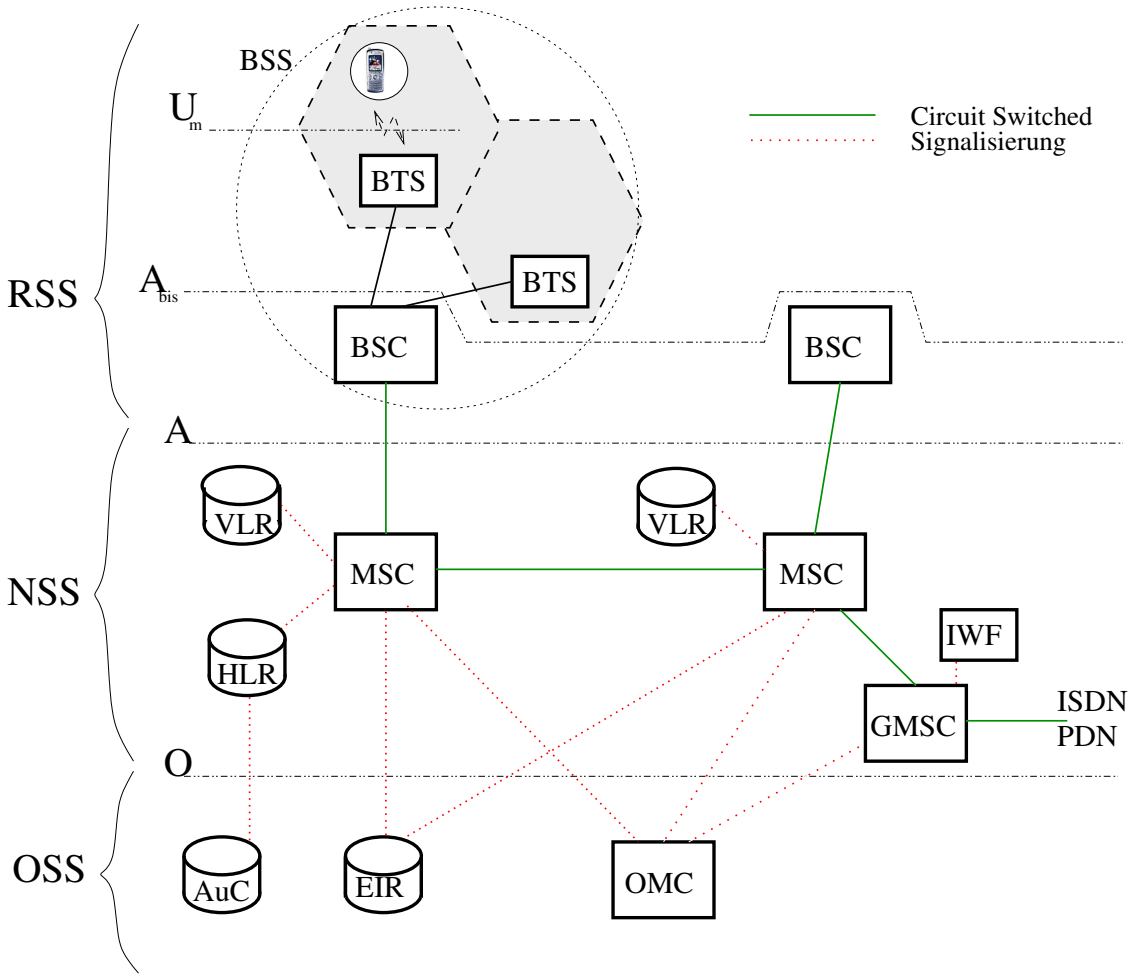


Abbildung 6: Generationen der Mobilfunksysteme

Infrastruktur: GSM lässt sich in drei Subsysteme unterteilen (Abbildung 7):

- das Funk-Feststationssystem RSS (Radio Subsystem)
- das Mobilvermittlungssystem NSS (Network and Switching System)
- das Betriebs- und Wartungssystem OSS (Operation Subsystem)

Das Funk-Feststationssystem besteht aus einer Menge von Feststationssystemen BSS (Base Station Subsystem), die jeweils von einer Feststationssteuerung BSC (Base Station Controller) gesteuert werden.
Eine Feststationssteuerung verwaltet mehrere Basis-Sende-Empfangsstationen BTS (Base Tranceiver Station) innerhalb des Feststationssystems.
Eine Basis-Sende-Empfangsstation bildet eine Funkzelle mit einem Radius von mehreren 100 Metern bis zu 35 Kilometer. Der Radius ist abhängig von der Umgebung, dem zu erwartenden Verkehrsaufkommen und vom Frequenzbereich.
Das mobile Endgerät besteht aus einer nutzerunabhängigen und nutzerspezifischen Komponente. Es besitzt eine eigene, einmalige Gerätekennung IMEI (International Mobile Equipment Identity) und ist nutzerunabhängig.
Außerdem enthält es ein Modul SIM (Subscriber Identity Module), dieses ist nutzerabhängig. Es enthält alle den Teilnehmer betreffenden Daten und muss in dem zu nutzenden GSM-Endgerät eingesetzt werden. Ohne SIM-Karte sind nur Notrufe möglich.



BTS – Base Transceiver Station
BSS – Base Station Subsystem
BSC – Base Station Controller
MSC – Mobile Switching Center
HLR – Home Location Register
VLR – Visitor Location Register
GMSC – Gateway Mobile Switching Center

IWF – Internet Working Funktions
ISDN – Integratet Services Digital Network
PDN – Public Data Networks
OMC – Operation and Maintenance
Auc – Authentification Centre
EIR – Equipment Identity Register

Abbildung 7: Referenzarchitektur von GSM

Die A-Schnittstelle verbindet das Mobilvermittlungssystem mit dem Funk-Feststationssystem. Hauptkomponente des Mobilvermittlungssystems sind die Dienstvermittlungsstellen MSC (Mobile Switching Center). Es handelt sich dabei um leistungsfähige Vermittlungsstellen. Sie bilden die GSM-Netzinfrastruktur und sind mit den Feststationssteuerungen und anderen Vermittlungsstellen verbunden.
Jede Dienstvermittlungsstelle verwaltet einen bestimmten Bereich. Sogenannte *Gateway* Dienstvermittlungsstellen (GMSC) bieten zusätzlich Verbindungen zum ISDN-Festnetz. GMSCs können aber auch mit Hilfe einer speziellen Erweiterung, den IWFs (Internetworking Functions), an IP-basierende Datennetze angeschlossen werden.
Das Mobilvermittlungssystem besitzt zwei Datenbanken: das Heimatregister HLR (Home Location Register) und das Besucherregister VLR (Visitor Location Register).
Das Heimatregister ist genau einmal vorhanden und speichert alle teilnehmerspezifischen Daten.
Das Besucherregister ist eine hochdynamische Datenbank, die alle relevanten Daten der Teilnehmer innerhalb eines von einer Vermittlungsstelle verwalteten Bereichs zwischenspeichert. Wechselt ein Teilnehmer die Dienstvermittlungsstelle, so werden die notwendigen Daten in das Heimatregister zurückkopiert und von der neuen Vermittlungsstelle wiederum von dort abgefragt. Durch diese Hierarchie wird die häufige Aktualisierung und somit die Belastung des Heimatregisters vermieden.
Das Betriebs- und Wartungssystem OSS dient der zuverlässigen Funktion und Wartung des GSM-Netzes. Das OSS ist über die O-Schnittstelle angebunden.
Die Systemüberwachung wird von der Betriebs- und Wartungszentrale OMC (Operation and Maintenance Center) übernommen. Die OMC-Zentrale übernimmt auch die Teilnehmerverwaltung und die Abrechnung.
Die Authentifizierungszentrale AuC (Authentification Center) sorgt zusammen mit den in dem Heimatregister gespeicherten personenbezogenen Daten für eine gesicherte Datenübertragung. Meist ist die Authentifizierungszentrale Teil des Heimatregisters.
Das Geräteidentifikationsregister EIR (Equipment Identity Register) speichert alle Gerätekennungen. Das EIR enthält eine „weiße Liste“ gültiger Kennungen, eine „schwarze Liste“ gesperrter Kennungen und eine graue Liste zur Kennzeichnung von Geräte mit Fehlfunktionen.
Das GSM-Funkschnittstelle U_m arbeitet in Europa auf Frequenzen im 900- und 1800-MHz-Band. Im nordamerikanischen Bereich wird auf 1900 MHz gesendet.
Geplant ist auch im 450-MHz-Band noch Frequenzen zu reservieren, die durch den Wegfall der analogen Telefondienste frei werden. Die Netze werden entsprechend der genutzten Frequenzen als GSM-450, GSM-900, GSM-1800 und als GSM-1900 bezeichnet.
GSM nutzt für den Mediumzugriff eine Kombination von Raum-, Frequenz- und Zeitmultiplex. Für die Übertragung vom mobilen Endgerät zur Funkstation werden im 900-MHz-Band die Frequenzen von 890 bis 915 MHz und in Rückrichtung von 935 bis 960 MHz verwendet. Die Frequenzbänder werden in 200 kHz breite Kanäle unterteilt, so dass für jede Senderichtung 124 Kanäle zur Verfügung stehen. Diese Kanäle werden als FDM-Kanäle bezeichnet.
Die von den Basis-Sende-Empfangsstationen gebildeten Zellen werden zu *Clustern* zusammengefasst, in denen jede Funkzelle bestimmte FDM-Kanäle exklusiv benutzt. Durch jeden FDM-Kanal werden acht physikalische TDM-Kanäle realisiert. Dazu wird durch Zeitmultiple-

max. Nutzdatenrate in Kbit/s	Bruttodatenrate in Kbit/s	FEC-Kosten in Kbit/s	Nettodatenrate in Kbit/s
2.4	22.8	19.2	3.6
2.4	11.4	7.8	3.6
4.8	22.8	16.8	6
4.8	11.4	5.4	6
9.6	22.8	10.8	12
14.4	22.8	5.4	17.4

Tabelle 1: Verfügbare Datenraten in GSM

xing jeder FDM-Kanal in TDMA-Rahmen (Time Division Multiple Access) unterteilt. Jeder Rahmen beinhaltet acht Zeitschlitze, die von jeweils einem TDM-Kanal genutzt werden.
Für die Verbindungsübergabe besitzt GSM vier verschiedene Verfahren. Die Intrazellenübergabe weist einer Verbindung eine neue Trägerfrequenz zu. Notwendig wird dies, wenn auf der genutzten Frequenz schmalbandige Störungen auftreten.
Wechselt das mobile Endgerät die Zelle, erfolgt eine Intra-BSC-Übergabe. Dann wird das Endgerät von der zuständigen Feststationssteuerung einer neuen Basis-Sende-Empfangsstation zugeordnet.
Sollte die zuständige Feststationssteuerung überlastet sein, oder liegt die neue Zelle außerhalb ihres Zuständigkeitsbereichs, so erfolgt eine Intra-MSC-Übergabe.
Eine weitere Möglichkeit ist schließlich die Inter-MSC-Übergabe zwischen zwei Dienstvermittlungsstellen. Diese erfolgt bei einer Übergabe zwischen zwei Zellen, die sich im Zuständigkeitsbereich von unterschiedlichen Vermittlungsstellen befinden.
Die Qualität einer Verbindung zwischen mobilen Endgerät und Basis-Sende-Empfangsstation wird im Halbsekundentakt von beiden Kommunikationspartnern gemessen und bewertet. Anhand der Signalstärke und deren Veränderung über einen längeren Zeitraum lassen sich Entscheidungen zwecks Übergabe treffen.

Übertragungsraten: Wie in Tabelle 1 dargestellt, bietet GSM Bruttotransferraten von 22.8 und 11.4 Kbit/s pro Übertragungskanal an. Abzüglich der Kosten für die Vorwärtsfehlerkorrektur FEC (Forward Error Correction) ergeben sich Nettotransferaten von 3.6, 6, 12 und optional auch 17.4 Kbit/s. Für den mobilen Teilnehmer ergeben sich Datenübertragungsraten von 2.4, 4.8, 9.6 und optional 14.4 Kbit/s.
Die maximale Reisegeschwindigkeit die dabei möglich ist beträgt 250 Km/h.
Durch die in den folgenden Abschnitten noch zu erklärenden GSM-Trägerdienste HSCSD (High Speed Cellular Switched Data), GPRS (General Paket Radio Services) und EDGE (Enhanced Data Rates for GSM Evolution) stehen größere Datenraten zur Verfügung.

Sicherheit: Die von GSM angebotenen Sicherheitsdienste basieren auf vertraulichen Daten, die in der SIM und der Authentifizierungszentrale gespeichert sind.

Erster Schritt ist immer die Authentifizierung des Benutzers gegenüber der SIM-Karte durch eine Geheimzahl. Diese ist auf der SIM gespeichert und muss vom Teilnehmer bei Aktivierung des Endgerätes eingegeben werden.
Die Authentifizierung des Endgerätes gegenüber der zuständigen Basisstation erfolgt mit einen *Challenge-Response*-Verfahren. Dieser Algorithmus verwendet einen auf der SIM-Karte und in der Authentifizierungszentrale gespeicherten 128-Bit-Schlüssel und eine ebenfalls 128 Bit lange Zufallszahl. Die Zufallszahl wird von der Basis-Sende-Empfangsstation ermittelt und unverschlüsselt zum mobilen Endgerät übertragen.
Funkstation und mobiles Endgerät wenden nun den Authentifizierungsalgorithmus an und erhalten als Ergebnis eine 32-Bit-SRES (Signed Response). Beide SRES werden an die Besucherdatenbank geschickt. Die Besucherdatenbank überprüft beide Werte auf Übereinstimmung. Sind beide identisch, so ist der Teilnehmer authentifiziert und es können weitere Transaktionen vorgenommen werden.
Alle teilnehmerbezogenen Informationen werden verschlüsselt über die Luftschnittstelle übertragen. Auch hier wird von der Sende- und Empfangsstation zuerst eine 128 Bit lange Zufallszahl generiert und dann an das mobile Endgerät übertragen. Ein weiterer Algorithmus erzeugt im Endgerät und in der Funkstation aus dem Authentifizierungsschlüssel und der Zufallszahl einen 64 Bit langen Übertragungsschlüssel. Dieser Schlüssel wird nicht über die Funkstrecke übertragen, sondern nach jeder Authentifizierung neu berechnet. Mithilfe des Übertragungsschlüssels werden die teilnehmerbezogenen Nutzdaten verschlüsselt.
[49] [11] [13]

Im Folgenden werden mit HSCSD, GPRS und EDGE verschiedene, sich teilweise ergänzende, Trägerdienste vorgestellt. Diese können zusammen mit dem vorhandene GSM-Netz innerhalb derselben Frequenzbänder koexistieren.

2.2.2 HSCSD

HSCSD (High Speed Circuit Switched Data) ist ein für GSM vorgesehener Trägerdienst. Zur Einführung von HSCSD ist lediglich eine Modifizierung von Endgeräten und Vermittlungsstellen notwendig. Dies ist meist durch ein Softwareupdate zu realisieren. Das Endgerät muss zeitgleich senden und empfangen können. Häufig schalten Endgeräte nur sehr schnell zwischen Senden und Empfangen um.
Durch HSCSD lassen sich mehrere GSM-Kanäle zusammenlegen und stellen somit eine höhere Bandbreite zur Verfügung. Ein mobiles Endgerät kann theoretisch einen gesamten TDMA-Rahmen mit allen 8 Zeitschlitzen anfordern. Aus frequenzökonomischen Gründen ist lediglich die Reservierung von bis zu 4 Zeitschlitzen in Auf- und Abwärtsrichtung vorgesehen.
Die damit maximale Datenübertragungsrate von 57.6 Kbit/s entspricht dann etwa der von einem heute typischen Modem (56 Kbit/s) oder ISDN (64 Kbit/s). Die zur Verfügung stehenden Zeitschlitze können beliebig auf die beiden GSM-Rahmen in Auf- und Abwärtsrichtung verteilt werden. Die Verteilung kann durchaus asymmetrisch sein. In der Tabelle 2 sind alle verfügbaren Datenraten aufgeführt.
HSCSD ist sehr gut geeignet, direkte Datenverbindungen aufzubauen, bei denen es um hohen

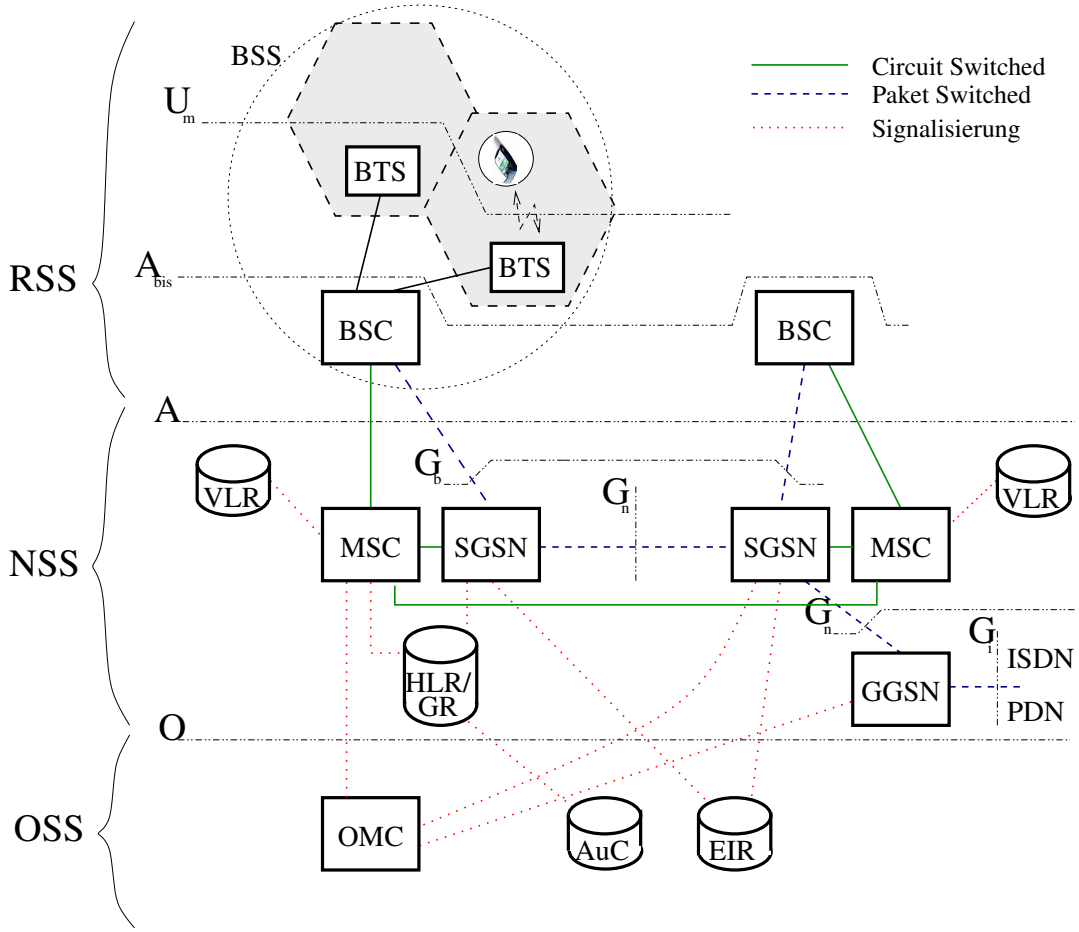
max. Datenrate in Kbit/s	Zahl der TDM-Kanäle	Datenrate pro TDM-Kanal in Kbit/s
4.8	1	4.8
9.6	1 / 2	9.6 / 4.8
14.4	1 / 2 / 3	14.4 / 9.6 / 4.8
19.2	1 / 2 / 3 / 4	19.2 / 14.4 / 9.6 / 4.8
28.8	2 / 3	14.4 / 9.6
38.4	4	9.6
43.2	3	14.4
57.6	4	14.4

Tabelle 2: Verfügbare Datenraten für HSCSD

Datendurchsatz geht. Jedoch werden hier Ressourcen der Luftschnittstelle verschenkt, da HSCSD immer noch verbindungsorientiert arbeitet. Außerdem entsteht durch die getrennte Signalisierung der Kanäle Mehraufwand beim Auf- und Abbau von Verbindungen.
Handovervorgänge gestalten sich aufgrund der hohen Anzahl zu migrierender Kanäle als außerordentlich schwierig und sind meist nicht erfolgreich.
[64] [65]

2.2.3 GPRS

GPRS (General Paket Radio Services) ist ein paketorientierter auf GSM-basierender Trägerdienst, durch den ebenfalls höhere Übertragungsraten mit GSM möglich werden. Der Netzanbieter ist hierbei gleichzeitig Internetprovider und das Endgerät ist ständig mit dem Netz verbunden. Ein Auf- und Abbau der Verbindung fällt vollständig weg. Die Abrechnung erfolgt in Abhängigkeit von der übertragenen Datenmenge.
Es wurden für GPRS zwei neue, das GSM-Netz ergänzende, Netzelemente eingeführt. Sie werden als GPRS *Support Nodes* (GSN) bezeichnet und sind in Abbildung 8 dargestellt.
Der GPRS *Gateway Support Node* (GGSN) ist die Verbindungseinheit zwischen dem vorhandenen GSM-Netz und dem externen paketorientierten Dienst. Es enthält Wegwahldaten, übernimmt die Adressumwandlung und die Tunnelung von Nutzdaten. Der GGSN ist über die G_i-Schnittstelle an das Festnetz angebunden.
Zweites zusätzliches unterstützendes Netzelement ist der *Serving* GPRS *Support Node* (SGSM). Es unterstützt das mobile Endgerät indirekt über die G_b-Schnittstelle durch das Feststationssystem. Der *Serving* GPRS *Support Node* erfragt Teilnehmeradressen aus dem GPRS Register (GR).
Das GR ist eine in das Heimatregister integrierte Datenbank, das alle GPRS-relevanten Daten speichert.
Wie bei HSCSD kann auch GPRS theoretisch bis zu acht Zeitschlitze innerhalb eines GSM-Zeitrahmens belegen. Die Belegung erfolgt hier jedoch anforderungsgesteuert. Alle Zeitschlitze können unter den aktiven Teilnehmern verteilt werden. Auf- und Abwärtsrichtung werden



BTS	–	Base Transceiver Station	SGSN	–	Serving GPRS Support Node
BSS	–	Base Station Subsystem	GGSN	–	GPRS Gateway Support Node
BSC	–	Base Station Controller	ISDN	–	Integratet Services Digital Network
MSC	–	Mobile Switching Center	PDN	–	Public Data Networks
HLR	–	Home Location Register	OMC	–	Operation and Maintenance
GR	–	GPRS Register	Auc	–	Authentification Centre
VLR	–	Visitor Location Register	EIR	–	Equipment Identity Register

Abbildung 8: Referenzarchitektur von GPRS

real. Datenrate in Kbit/s (4 Kanäle)	max. Datenrate in Kbit/s (8 Kanäle)	Datenrate pro TDM-Kanal in Kbit/s	Coding Scheme
36.2	72.4	9.05	CS1
53.6	107.2	13.4	CS2
62.4	124.8	15.6	CS3
85.6	171.2	21.4	CS4

Tabelle 3: Verfügbare Datenraten und Coding Schemes für GPRS

vollkommen getrennt behandelt.

Die Datenrate pro Zeitschlitz ist abhängig von der Güte der Übertragung. Sie wird in vier Stufen variiert.

Coding Scheme 1 (CS1) liefert die höchste Übertragungssicherheit mit der unter GSM üblichen Übertragungsrate von 9.05 Kbit/s. CS2 bietet 13.4 Kbit/s bei geringerer Zuverlässigkeit. CS3 (15.6 Kbit/s) und CS4 (21.4 Kbit/s) bieten noch größere Basis-Übertragungsraten (siehe Tabelle 3). Hier sind jedoch weitere Anpassungen zwischen Feststationssteuerung (BSC) und Basis-Sende-Empfangsstation (BTS) notwendig.

Die hohen Übertragungsraten lassen sich nur unter idealen Bedingungen erreichen, da sich mehrere Teilnehmer die Zeitschlitze teilen.

Die Verschlüsselung der paketorientierten Daten erfolgt bei GPRS zwischen mobilem Endgerät und SGSN.

[63] [66] [49] [59]

2.2.4 EDGE

EDGE (Enhanced Data-Rates for GSM Evolution) ist eine Weiterentwicklung des GSM-Standards. Es arbeitet mit neuen Modulationsverfahren, durch die sich HSCSD und GPRS ergänzen lassen. Diese werden dann als *Enhanced* HSCSD (ECSD) und *Enhanced* GPRS (EGPRS) bezeichnet.

Die in EDGE eingesetzten Modulationsverfahren sind anfälliger für Funkstörungen. So wird bei nicht ausreichender Verbindungsqualität wieder auf weniger anfälliges Verfahren zurückgeschaltet.

Für den Einsatz von EDGE muss ein Großteil der vorhandenen GSM-Vermittlungstechnik ausgetauscht werden. Fraglich ist, ob EDGE angesichts der notwendigen Investitionen in UMTS eingeführt wird.

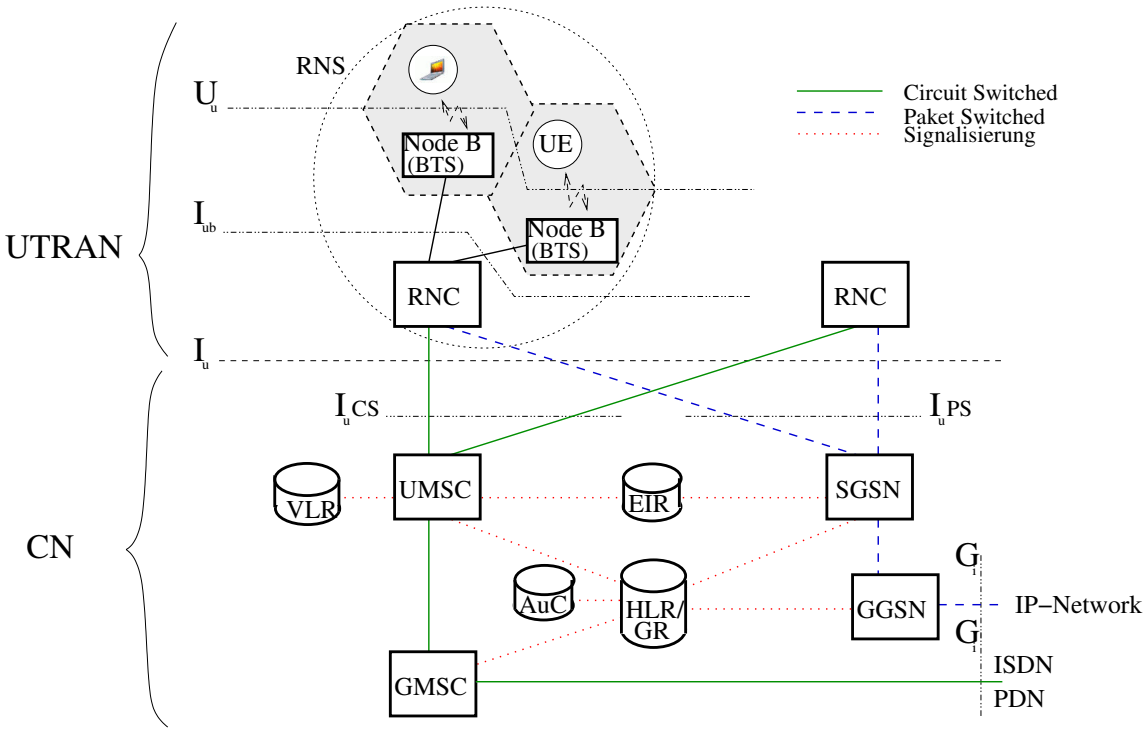
Die Nettoübertragungsrate eines GSM-Kanals lässt sich durch EDGE auf 48 Kbit/s erhöhen. So ist eine maximale Datenrate von 384 Kbit/s erreichbar. EDGE führt durch adative Codec-Auswahl AMR (Adaptive Multirate Codec) auch zu einer besseren Auslastung der normalen Telefonverbindungen. Innerhalb einer Funkzelle sind so mehr Gespräche vermittelbar.

[44] [59]

2.2.5 UMTS

UMTS (Universal Mobile Telecommunication System) ist der europäische Standard für die dritte Mobilfunkgeneration. Es ist Teil des internationalen Standards IMT-2000 (International Mobile Telecommunication) für Mobilfunknetze. Die derzeitigen Mobilfunknetze der zweiten Generation sollen durch IMT-2000 in einem Evolutionsprozeß abgelöst werden. UMTS bezieht sich ausschließlich auf die Erweiterungen für GSM-basierende Systeme.
Es handelt sich bei UMTS in vielen Teilen um eine komplett neue Basistechnologie, in der die Luftschnittstelle weitestgehend ausgetauscht und das Kernnetz durch neue Elemente ergänzt wird. Dabei wird der Ausbau von GSM zu UMTS in zwei Stufen erfolgen. In der ersten Stufe, dem *Release´99*, werden die Elemente der Luftschnittstelle installiert und das bereits GPRS-fähige Kernnetz beibehalten. Die zweite Ausbaustufe, das *Release 2000*, betrifft das Kernnetz. Hier wird der gesammte interne Transportweg auf IP und ATM-basierenden Paketbetrieb umgestellt. Somit sind keine getrennten Leitungen für Sprache und Daten mehr notwendig.
Im Folgenden wird in erster Linie auf die erste, die Luftschnittstelle betreffende, Ausbaustufe eingegangen.

Infrastruktur: Die in Abbildung 9 dargestellte UTMS-Architektur teilt sich in das Funknetz UTRAN (UMTS Terrestrial Radio Access Network) und das Kernnetz CN (Core Network) auf. Das Funknetz besteht aus einer Anzahl von Funkteilsystemen RNS (Radio Network Subsystem), die über die I_u-Schnittstelle mit dem Kernnetz CN verbunden sind.
Ein Funkteilsystem setzt sich aus einer Feststationssteuerung UTRAN RNC (UTRAN Radio Network Controller) und einer oder mehrerer zellbildender Basisstationen UTRAN Node B zusammen. Über die Luftschnittstelle U_u kommuniziert die Funkstation mit dem mobilen Endgerät UE (User Equipment).
Das Kernnetz muss die Daten vermitteln und an entsprechende externe Netze weiterleiten. Bei der Vermittlung wird zwischen verbindungsorientierten Daten CS (Circuit Switched) und paketorientierten Daten PS (Paket Switched) unterschieden.
Daten der *Circuit Switched Domain* (CSD) werden vom der UMTS-Dienstvermittlungsstelle UMSC (UMTS Mobile Switching Center) verarbeitet und, falls sich der Kommunikationspartner innerhalb eines anderen Netzes befindet, von der *Gateway*-Vermittlungsstelle GMSC (Gateway Mobile Switching Center) ausgekoppelt.
Die paketorientierte Daten der *Packet Switched Domain* (PSD) werden vom SGSN (Serving GPRS Support Node) und vom GGSN (Gateway GPRS Support Node) verarbeitet.
Die Mobilitätsverwaltung erfolgt, wie auch bei GSM, über ein Heimatregister und den UMTS-Dienstvermittlungsstellen zugeordneten Besucherregistern. Auch die Authentifizierungszentrale und das Geräteidentifikationsregister bleiben in bekannter Weise eingebunden.
Wie Abbildung 10 zeigt, soll der internationale Standard IMT-2000 eine Fülle von unterschiedlichen Übertragungsstandards unterstützen. UMTS-fähige Endgeräte sollen für alle Übertragungsstandards kompatibel sein.
Für UMTS sind die Technologien UTRA/FDD (UMTS Terrestrial Radio Access / Frequency Division Duplex) und UTRA/TDD (UMTS Terrestrial Radio Access / Time Division Duplex)



UTRAN – UTMS Radio Access System
RNC – Radio Network Controller
CN – Core Network
RNS – Radio Network Subsystem
UE – User Equipment
Node B – Base Transceiver Station
RNC – UTRAN Radio Network Controller
UMSC – UMTS Mobile Switching Center
GMSC – Gateway Mobile Switching Center
HLR – Home Location Register

GR – GPRS Register
VLR – Visitor Location Register
SGSN – Serving GPRS Support Node
GGSN – GPRS Gateway Support Node
ISDN – Integratet Services Digital Network
PDN – Public Data Networks
Auc – Authentification Centre
EIR – Equipment Identity Register
ILR – Internetworking Location Register

Abbildung 9: UMTS Referenzarchitektur

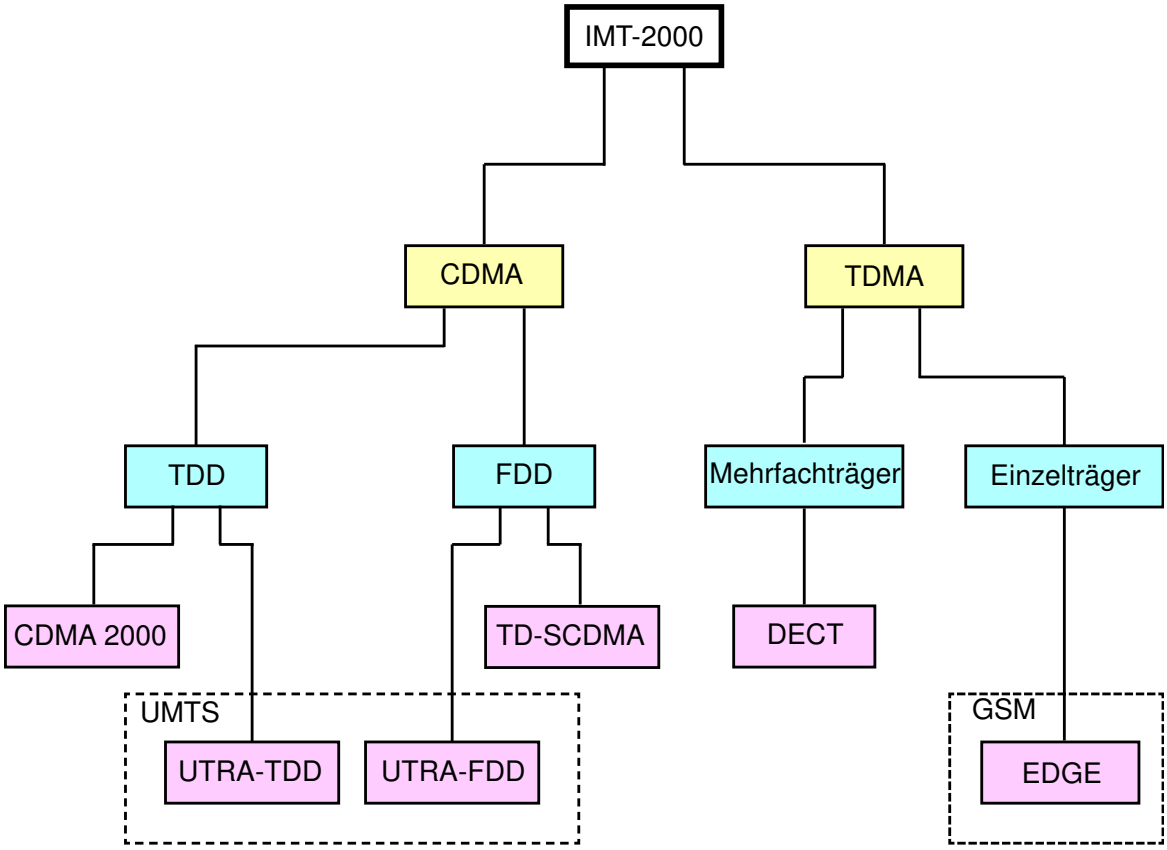


Abbildung 10: UMTS Kerntechnologien

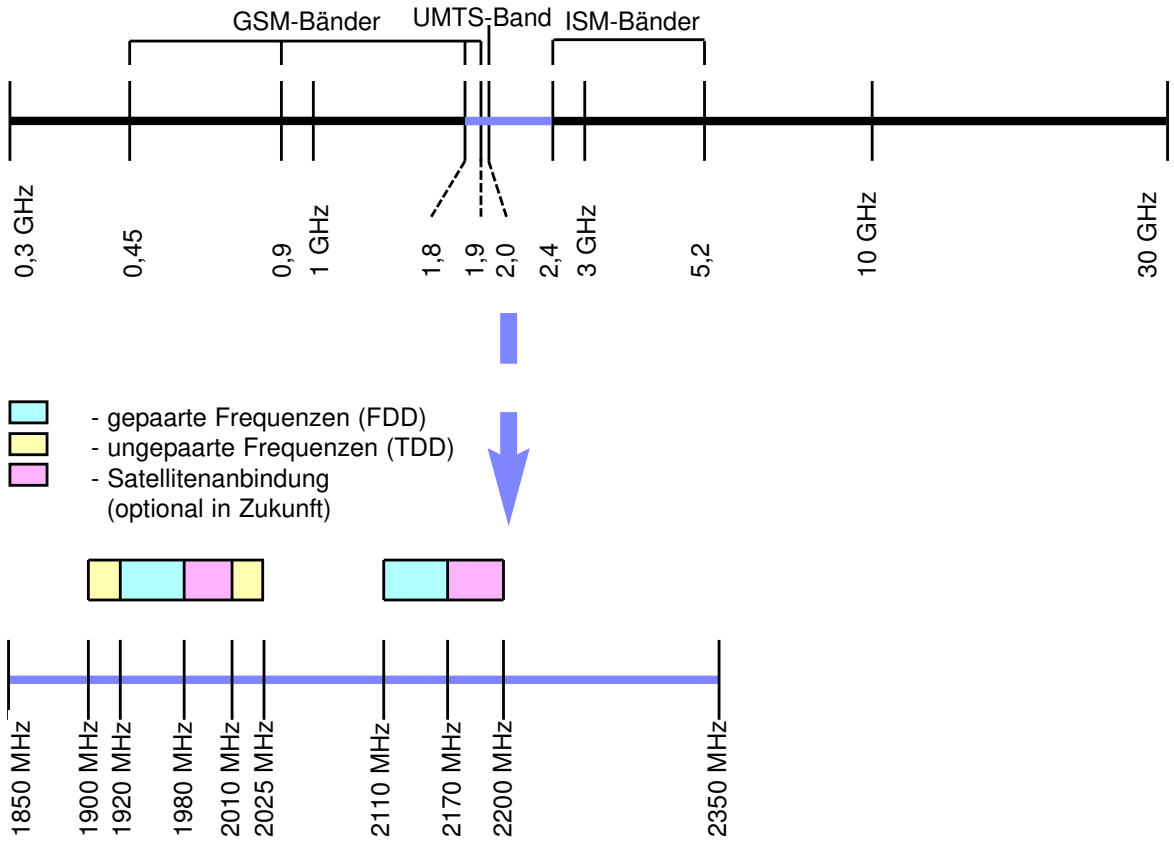


Abbildung 11: UMTS Frequenzverteilung

relevant.

Der Vielfachzugriff auf das Übertragungsmedium erfolgt über die Funkschnittstelle U_u. Der UTRA/FDD-Modus wird für symmetrische Dienste und der UTRA/TDD-Modus für symmetrische und asymmetrische Dienste eingesetzt.

Der FDD-Modus nutzt die in Abbildung 11 dargestellten gepaarten Frequenzbereiche von 1920-1980 MHz für die Aufwärtsrichtung und 2110-2170 MHz für die Abwärtsrichtung.

Für die Bildung des Übertragungskanals wird eine DSSS-basierende Breitband-CDMA-Technik W-CDMA (Wideband Code Division Multiple Access) eingesetzt. Die Übertragungskanäle werden hier sowohl durch verschiedene Spreizcodes, als auch durch unterschiedliche Frequenzen gebildet.

Der TDD-Modus sendet und empfängt auf den gleichen Frequenzen. Dazu nutzt er die ungepaarten Frequenzbereiche zwischen 1900-1920 MHz und 2010-2025 MHz. Die Übertragungskanäle werden hier durch eine Kombination von Spreizcodes und Frequenzsprungverfahren getrennt. Die Übertragungstechnik wird auch TD-CDMA (Time Division Code Division Multiple Access) bezeichnet.

Beide Modi sind darauf ausgelegt, nebeneinander zu existieren. Auch Verbindungsübergaben

max. Datenrate in Kbit/s	max. Bewegungsgeschwindigkeit in Km/s	Codierungsverfahren	max. Latenzzeit in ms
2048	≤ 10	TDD	unbeschränkt
384	≤ 120	FDD	300 ms
144	≤ 500	FDD	300 ms
14.4-16	≤ 500	FDD	20 ms

Tabelle 4: Mögliche Datenraten für UMTS relativ zur Bewegungsgeschwindigkeit und eingesetztem Übertragungsmodus

zwischen TDD, FDD und GSM sind aufgrund ähnlicher Rahmenstrukturen möglich. Ebenfalls ist mittelfristig vorgesehen, vertikales Roaming zwischen UMTS, GSM und Satellitennetzen zu unterstützen. Dies ist wichtig, da eine Vollversorgung mit UMTS aufgrund der hohen Kosten und geringer Zellgröße auszuschließen ist. So ergibt es sich, dass zukünftig alle UMTS-Endgeräte eine Auswahl von Fallback-Techniken auf andere drahtlose Kommunikationsnetze beherrschen werden.

Übertragungsraten: Das UMTS-Funknetz ist in Versorgungsebenen aufgeteilt, die mit unterschiedlichen Bandbreiten arbeiten. Diese sind abhängig von der Geschwindigkeit, mit der sich der mobile Teilnehmer bewegt. Je schneller sich eine mobile Station bewegt, desto größer müssen die Zellen sein. Somit stellt das Übertragungsmedium weniger Bandbreite pro Quadratmeter zur Verfügung.
Dies ist auch der Grund, warum die Entscheidung für zwei Übertragungsmodi getroffen wurde. Aufgrund ihrer unterschiedlichen Eigenschaften kann sowohl dem Bedürfnis, bei hohen Bewegungsgeschwindigkeiten ($\leq$ 500 Km/h) noch Daten zu empfangen, als auch dem hohen Bandbreitenbedarf ($\leq$ 2 Mbit/s) genüge getan werden.
Der FDD-Modus verfügt durch seine getrennten Frequenzenverbindungen über gute Sende- und Empfangseigenschaften in der Fläche und in größeren Funkzellen. Selbst bei hohen Geschwindigkeiten lassen sich die Signale noch gut rekonstruieren (144 Kbit/s).
Für kleinere Zellen eignet sich der TDD-Modus besser. Bei vorwiegend ruhiger Position oder langsamer Fortbewegung ($\leq$ 10 Km/h) lassen sich Übertragungsgeschwindigkeiten bis zu 2 Mbit/s erreichen. Durch die Unterstützung asymmetrischer Anwendungen seitens des TDD-Modus lässt sich die verfügbare Bandbreite auch wesentlich effizienter nutzen (siehe Tabelle 4).
Wie bei GPRS teilen sich auch hier alle Teilnehmer einer Zelle die vorhandene Bandbreite. Diese Aufteilung kann in Serviceklassen erfolgen. Teilnehmer erhalten dabei je nach Serviceklasse unterschiedliche Prioritäten.

Sicherheit: Die Sicherheitsarchitektur von UMTS basiert auf der von GSM. Auch hier wird eine SIM-Karte USIM (UMTS SIM) als Sicherheitsmodul übernommen. Verbesserungen wurden bezüglich der Authentifizierung vorgenommen, so dass sich nun auch das Netz gegenüber dem mobilen Endgerät authentifizieren muss.

Für die Authentifizierung wird wieder ein *Challenge-Response*-Verfahren eingesetzt. Hierbei wird neben der Zufallszahl auch ein sogenanntes *Authentification Token* übertragen. Dieses wird von der USIM auf Korrektheit geprüft. Verläuft die Prüfung erfolgreich, so erfolgt die Authentifizierung seitens des mobilen Endgerätes wie bei GSM.
Für die Verschlüsselung der Teilnehmerdaten werden nun 128-Bit-Übertragungsschlüssel berechnet. Zusätzlich kommt hier ein Integritätsschlüssel zum Einsatz. Dieser ist ebenfalls 128 Bit lang. Mit ihm lassen sich *Message Authentification Codes* erzeugen, die sich mit allen paketvermittelnden Nutz- und Signalisierungs-Daten verknüpfen lassen.
Die in UMTS eingesetzten Algorithmen basieren durchgehend auf offener Kryptographie. Für Verschlüsselung und Integritätsprüfung wird der *Kasumi*-Algorithmus eingesetzt. Zur Authentifizierung wurde als Beispiel der Algorithmus *Milenage* entwickelt. Es wird jedoch den Funknetzanbietern empfohlen, eigene Algorithmen einzusetzen [11].
[51] [59]

2.3 Satellitenbasierende Systeme

In vielen Gegenden ist Satellitenfunk die einzige Kommunikationsmöglichkeit. Es handelt sich dabei um eine Technik, die mittelfristig als Fallbacktechnik für Mobilfunknetze eingebunden wird. Ihre Netzabdeckung ist weitgehend unabhängig von nationalen Regelungen. Es werden drei Klassen von Satelliten unterschieden: GEO, MEO und LEO.

2.3.1 Satellitenfunk

Geostationäre Satelliten GEO (Geostationary Earth Orbit) sollen für Beobachter von der Erde eine feste Position einnehmen. Die dafür benötigte Entfernung von der Erde beträgt etwa 36.000 Kilometer. Diese feste Umlaufbahn liegt direkt über dem Äquator und wird als GEO-Umlaufbahn bezeichnet. Mithilfe von drei Satelliten lässt sich so theoretisch jeder Punkt der Erde funktechnisch versorgen. Es ist allerdings eine relativ hohe Sendeleistung notwendig, um eine (fast) globale Versorgung zu erreichen. Die Polarregionen lassen sich durch geostationäre Satelliten nicht abdecken. Auch liegen die Latenzzeiten aufgrund der hohen Umlaufbahn bei > 0.25 s pro Link.
Niedrig fliegende Satelliten LEO (Low Earth Orbit) bewegen sich in Höhen von 500 bis 1500 Kilometer. Mit ihnen lässt sich eine globale Versorgung erreichen, wofür allerdings mindestens 48 Satelliten notwendig sind. Durch ihre geringe Flughöhe benötigen sie nur etwa ein Viertel der Sendeleistung bezogen auf GEO-Satelliten. Die Latenzzeit beträgt etwa 10 ms. LEO-Satelliten besitzen eine Umlaufzeit von 90 bis 120 Minuten. Daraus ergibt sich, dass sie jeweils nur etwa 10 Minuten für ein stationäres Endgerät zur Verfügung stehen. Das macht häufige Handover-Vorgänge notwendig.
Satelliten mittlerer Umlaufbahnen MEO (Medium Earth Orbit) fliegen in Bahnen von ca. 10.000 Kilometer Höhe. Für eine globale Abdeckung reichen etwa 12 Satelliten. MEO-Satelliten besitzen Latenzzeiten von etwa 70 bis 80 ms.
Bei der Satellitenkommunikation sind hohe Datenraten bis zu einigen Megabit in Empfangsrichtung unproblematisch. Die Senderichtung ist jedoch sehr aufwendig. Das Problem besteht

	LEO	MEO	GEO
min. Anzahl der Satelliten	48	12	3
Flughöhe in Km	500 - 1500	ca. 10000	ca. 35000
Fluggeschwindigkeit in Km/h	ca. 30.000	ca. 7000	stationär
max. Sendeleistung in Watt	500	1000	2000
max. Datenrate in Kbit/s	einige 1000	600	300

Tabelle 5: Satellitenkommunikation

	Satelliten	Höhe in Km	Datenrate Kbit/s
Teledesic (2005)	288	700	128-100000 $\uparrow$, 720000 $\downarrow$
Iridium	66 (+6)	780	2.4 - 4.8
Globalstar	48 (+4)	14000	9.6
ICO	10 (+2)	10000	4.8
Inmarsat	5	geostationär	2.4

Tabelle 6: Satellitensysteme und verfügbare Datenraten

bei geostationäre Satelliten in der großen Flughöhe. Bei LEO-Satelliten ist die hohe Bewegungsgeschwindigkeit von bis zu 30.000 Km/h problematisch.

In Tabelle 5 sind die erwähnten Eigenschaften der drei Satellitentypen zusammengefasst.

Die Bewegungsgeschwindigkeit der mobilen Teilnehmer kann bei Satellitenkommunikation aufgrund der großen Zellen vernachlässigt werden.

Der angestrebte internationale Mobilfunkstandard der dritten Generation IMT-2000 sieht in zukünftigen Entwicklungsstadien eine satellitenbasierte Variante S-UMTS vor. Diese wird in dem dafür vorgesehenen Bereich von 2170 bis 2200 MHz arbeiten (siehe Abbildung 11). Es sollen dabei unter Nutzung von LEO-Satelliten Datenraten bis zu 384 Kbit/s möglich sein.

Die Funkschnittstelle SRI (Satellite Radio Interface) ist allerdings noch nicht vollständig spezifiziert. Auch ist noch nicht klar, ob nur LEO-Satelliten eingesetzt werden, oder auch MEO- und GEO-Satelliten. Erstere bieten aufgrund ihrer niedrigen Umlaufbahn eine wesentlich bessere Kapazität. Sie bedeuten allerdings auch mehr Aufwand wegen der hohen Umlaufgeschwindigkeit und der hohen Anzahl notwendiger Satelliten, um eine vollständige Netzabdeckung zu gewährleisten.

Entscheidende Unterschiede zur Funkschnittstelle des terrestrischen UMTS ergeben sich auch aus der geringeren Empfangsleistung und den längeren Signallaufzeiten. In jedem Fall werden die Mobiltelefone der ersten UMTS-Generation sich nicht für S-UMTS eignen. Erst zukünftige Geräte werden optional über die zusätzliche Technik verfügen.

In Tabelle 6 sind aktuelle Satellitensysteme und deren verfügbare Datenübertragungsraten aufgeführt.

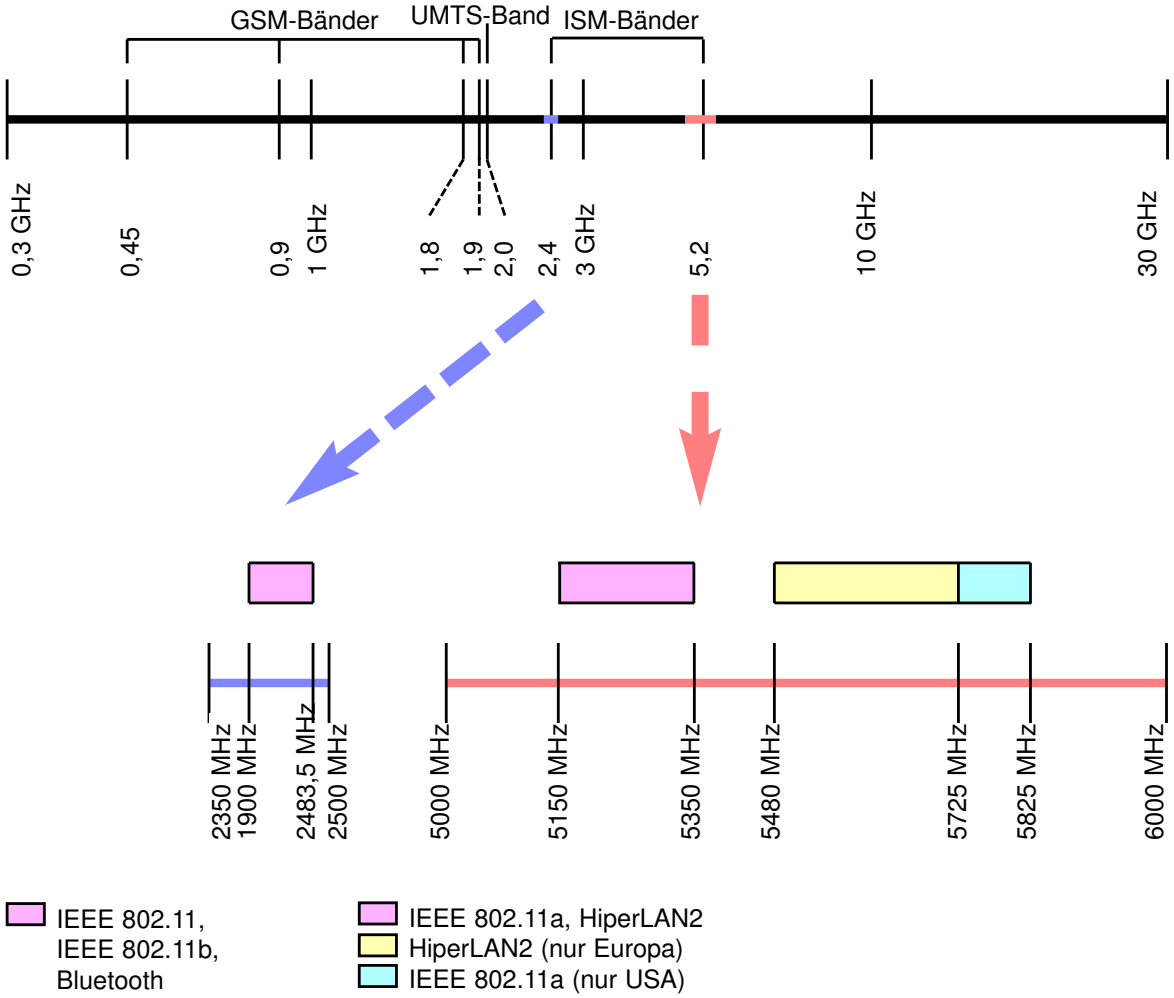


Abbildung 12: Von LANs und PANs genutzte lizenzfreie ISM-Frequenzbänder

2.4 Drahtlose LANs

Local Area Networks (LAN) sind auf einen Standort begrenzte Rechnernetzwerke. Drahtlose LANs (WLAN) ergänzen oft solch eine vorhandene LAN-Infrastruktur um spezielle Zugangspunkte, welche die drahtlose Netznutzung ermöglichen. Ein spezielles Einsatzgebiet für kurzreichweitige wireless LAN Systeme sind sogenannte *hot spots*. Darunter versteht man Ballungsgebiete mit hohem Kommunikationsbedarf wie Bahnhöfe, Flughäfen, Universitäten oder ähnliche, in denen die LAN-Technologie das Mobilfunksystem ersetzt.

Dem mobilen Endgerät werden durch WLANs wesentlich höhere Bandbreiten als durch den Mobilfunk angeboten. Dies geht auf Kosten der Gerätekomplexität und des Stromverbrauchs.

Von drahtlosen LANs und PANs (Private Area Networks) werden die in Abbildung 12 dargestellten lizenzfreien Frequenzbänder (ISM-Bänder) genutzt.

LANs und PANs werden in Netze mit und ohne feste Infrastruktur unterschieden. Infrastrukturlose Netze werden als Ad-hoc Netze bezeichnet. Sie entstehen durch die direkte Kommunikation der Endgeräte innerhalb eines Sende- und Empfangsbereichs.
Durch Endgeräte die *Routing*-Funktionen übernehmen, sind auch größere Ad-hoc Netze realisierbar. Bei Bluetooth wird dies beispielsweise durch *Bridge*-Knoten realisiert.

2.4.1 IEEE 802.11a/b

Die IEEE 802.11 Standards sind die drahtlosen Varianten der IEEE 802.x-Standard-Gruppe für lokale Netzwerke. Sie gehören zu derselben Standardgruppe wie auch Ethernet (IEEE 802.3). Die Standards IEEE 802.11a und IEEE 802.11b sind Nachfolger des inzwischen veralteten IEEE 802.11 Standards.

Infrastruktur: IEEE 802.11 WLANs unterstützen sowohl Infrastrukturgebundene- als auch Ad-hoc- Netzwerke. In Abbildung 13 ist ein infrastrukturgebundenes WLAN dargestellt. Die Zellen werden durch Dienstzugriffspunkte, den sogenannten *Access Points* (AP), gebildet. Mobile Endgeräte werden hier meist als *Stations* (STA) bezeichnet.
Die von einem Dienstzugriffspunkt verwaltete Zelle bildet gemeinsam mit dem mobilen Endgerät ein *Basic Service Set* (BSS).
Ein zellübergreifendes Netz wird durch ein Verteilsystem DS (Distribution System) gebildet. Durch dieses sind alle Dienstzugriffspunkte und somit auch die *Basic Service Sets* miteinander verbunden.
Durch das Verteilsystem wird das 802.11 Netz auch über *Gateways* mit anderen Netzwerken verkoppelt. Es enthält eine Datenbank, in der gespeichert wird, an welchen Zugangspunkt ein mobiles Endgerät gebunden ist. Ähnlich wie auch bei den Mobilfunknetzen durch das Heimatregister und das Besucherregister, wird solch eine Datenbank genutzt, um Rahmen effizient an Teilnehmer des drahtlosen Netzes auszuliefern.
Die Ad-Hoc-Kommunikation ist hier auf eine Zelle beschränkt. Weiterleitungsfunktionen, die Wegwahl oder der Austausch von Zusatzinformationen werden hier nicht unterstützt.
IEEE 802.11 nutzt das freie ISM-Band von 2.400 bis 2.483 GHz und setzt die Bandspreizverfahren DSSS und FHSS ein.
Der IEEE 802.11b-Standard arbeitet in demselben Frequenzband mit erweiterten DSSS. Durch komplexere Modulationstechniken wurden höhere Datenraten möglich. Dabei wird das 83 MHz breite ISM-Band in 14 sich überlappende Kanäle mit 22 MHz Bandbreite eingeteilt. Die Kanalzentren liegen dabei in einem Abstand von 5 MHz.
IEEE 802.11a nutzt das bei 5.2 GHz liegende ISM-Band. Dieses verfügt über eine wesentlich geringe Störbelastung als das stark frequentierte 2.4-GHz-Band. Das dafür vorgesehene Spektrum beträgt insgesamt 300 MHz. Das Frequenzband wird dabei in drei Subbänder je 100 MHz eingeteilt, für die jeweils unterschiedliche maximale Sendeleistungen festgelegt wurden.
Durch die Leistungsbeschränkungen ergeben sich unterschiedliche Anwendungsbereiche.
Die beiden von 5.150 - 5.250 GHz und von 5.250 - 5.350 GHz reichenden Frequenzbänder dürfen bis maximal 0.25 beziehungsweise 0.50 Watt betrieben werden. Sie werden von den

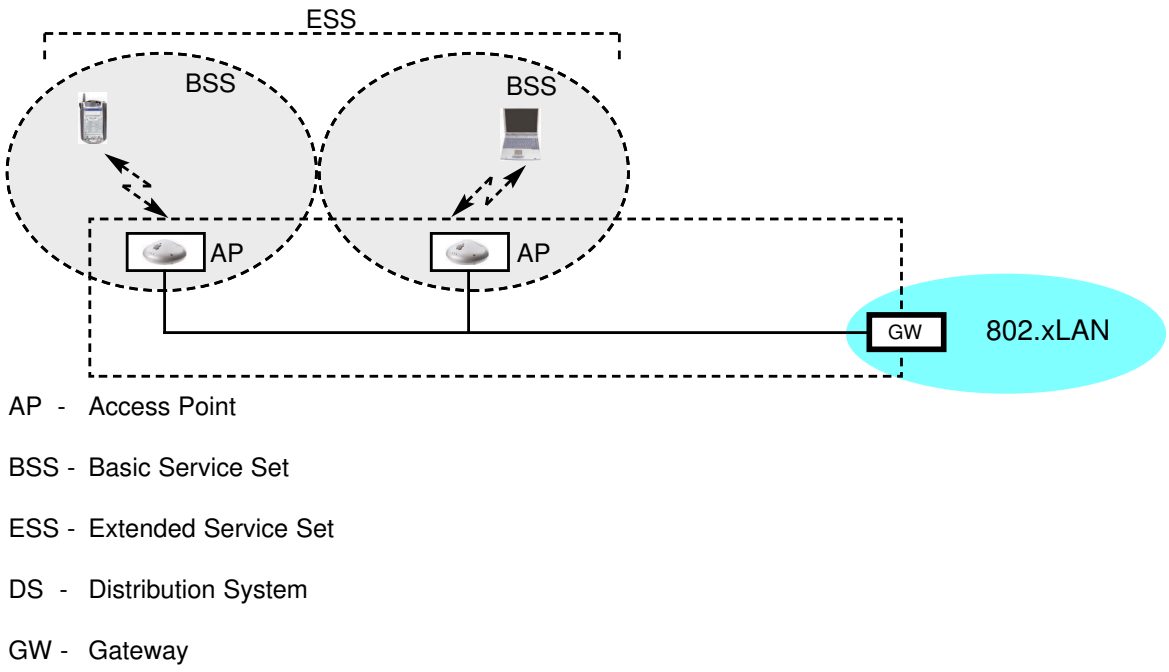


Abbildung 13: Architektur eines infrastrukturbasierten IEEE-802.11-Netzwerks

Dienstzugriffspunkten eingesetzt.
In dem oberen Band von 5.650 - 5.750 GHz darf nur mit einer maximale Sendeleistung von 1 Watt gesendet werden. Damit sollen Netze über längere Strecken drahtlos verbunden werden. In Europa sind lediglich die unteren beiden Frequenzbänder freigegeben.
Ein weiteres Problem ist, die Tatsache dass IEEE 802.11a keine Leistungskontrolle unterstützt. Dies ist allerdings innerhalb Europas eine Voraussetzung für den Betrieb im 5.2-GHz-Band.
Als Codemultiplextechnik wird hier OFDM eingesetzt, womit wesentlich höhere Datenraten übertragen werden können. Der Datenstrom wird dabei auf 52 Träger aufmoduliert. Für jeden Träger wird ein seiner Qualität entsprechendes, optimales Modulationsverfahren gewählt.
Da die Reichweite in Gebäuden durch Wände auf 15 - 50 m beschränkt sein kann, sehen IEEE 802.11 LANs Intrasystemroaming vor.
Alle Varianten nutzen CSMA/CA (Carrier Sense Multiple Access / Collision Avoidance) für den Mediumzugriff. Hierbei fordert jedes mobiles Endgerät vor der eigentlichen Übertragung eine Erlaubnis zum Senden von dem zuständigen Empfänger an. Erst wenn der Adressat empfangsbereit ist, antwortet dieser mit einer Freigabe und der Sender beginnt mit der Übertragung.

Übertragungsraten: Je nach Leistungsfähigkeit des mobilen Endgerätes und der Qualität der Übertragungsstrecke werden bei IEEE 802.11-LANs unterschiedliche Kodierungsverfahren eingesetzt. Ursprünglich wurde bei IEEE 802.11 Datenraten von 1 und 2 Mbit/s vorgesehen.

	IEEE 802.11	IEEE 802.11b	IEEE 802.11a	HiperLAN2
Modulation	FSSS / DSSS	DSSS	OFDM	OFDM
Frequenzband in GHz	2.4	2.4	5.2	5.2
Bruttodatenraten in Mbit/s	1, 2	1, 2, 5, 11	6, 12 , 24 (9, 18, 36, 48, 54)[a]	6, 9, 12, 18 27, 36, 54
max. Nettodatenrate in Mbit/s	1	5	25	32

[a] optional

Tabelle 7: Verfügbare Datenraten der IEEE 802.11-Standard Familie und HiperLAN2

Der Folgestandard IEEE 802.11b bietet zusätzlich Datenraten von 5 und 11 Mbit/s. Bei IEEE 802.11a werden Datenraten von 6, 9, 12, 18, 24, 36, 48 und 54 Mbit/s angeboten. Es sind in Endgeräten jedoch nur 6, 12 und 24 Mbit/s zwingend zu implementieren. Die angegebenen Datenraten sind Bruttowerte. Für den Teilnehmer stehen Nettowerte von etwa 50% zur Verfügung.
Die maximale Bewegungsgeschwindigkeit, bei der noch eine Übertragung möglich ist, ist hier stark von Umwelteinflüssen abhängig und liegt zwischen 50 und 100 Km/h.
In Tabelle 7 sind die verfügbaren Datenraten der IEEE 802.11-Standard Gruppe und HiperLAN2 aufgeführt.

Sicherheit: IEEE 802.11x-Netze sehen eine Authentifikation des mobilen Endgerätes anhand der MAC-Adresse (Medium Access Control) vor (Link-Level-Authentifikation). Jede Netzwerkkarte besitzt solch eine weltweit individuelle Adresse. Diese lässt sich allerdings auch beliebig neu konfigurieren. Leider lassen sich in den meisten Fällen auch nur maximal 256 MAC-Adressen in einem Dienstzugriffspunkt speichern.
Eine Teilnehmerauthentifikation ist nicht Teil des Standards. Properitäre Verfahren werden aber seitens des Standards unterstützt.
Zusätzliche Sicherheit bei der Zugangskontrolle lässt sich durch den *Service Set Identifier* (SSID) erreichen. SSIDs funktionieren wie ein Passwort und bieten eine vergleichbare Sicherheit. Sie werden eingesetzt, um das drahtlose Netzwerk in Segmente einzuteilen. Bei der Konfiguration der Dienstzugriffspunkte muss darauf geachtet werden, dass sie die SSID nicht im Broadcastverfahren verbreiten.
Um die Nutzdaten vor dem Abhören zu schützen, steht der Verschlüsselungsalgorithmus WEP (Wired Equivalent Privacy) zur Verfügung. WEP setzt einen RC4-Algorithmus mit einem 64-Bit-Schlüssel (optional auch 128-Bit) ein. 24 Bit werden davon für einen Initialisierungsvektor benötigt, so dass für die Verschlüsselung nur 40 beziehungsweise 104 Bit eingesetzt werden.
In kleinen Netzen gilt der 128-Bit-WEP in Kombination mit MAC Adressfilterung und SSID als einigermaßen sicher. Dies gilt allerdings nur solange Schlüssel, MAC-Adressen und SSID

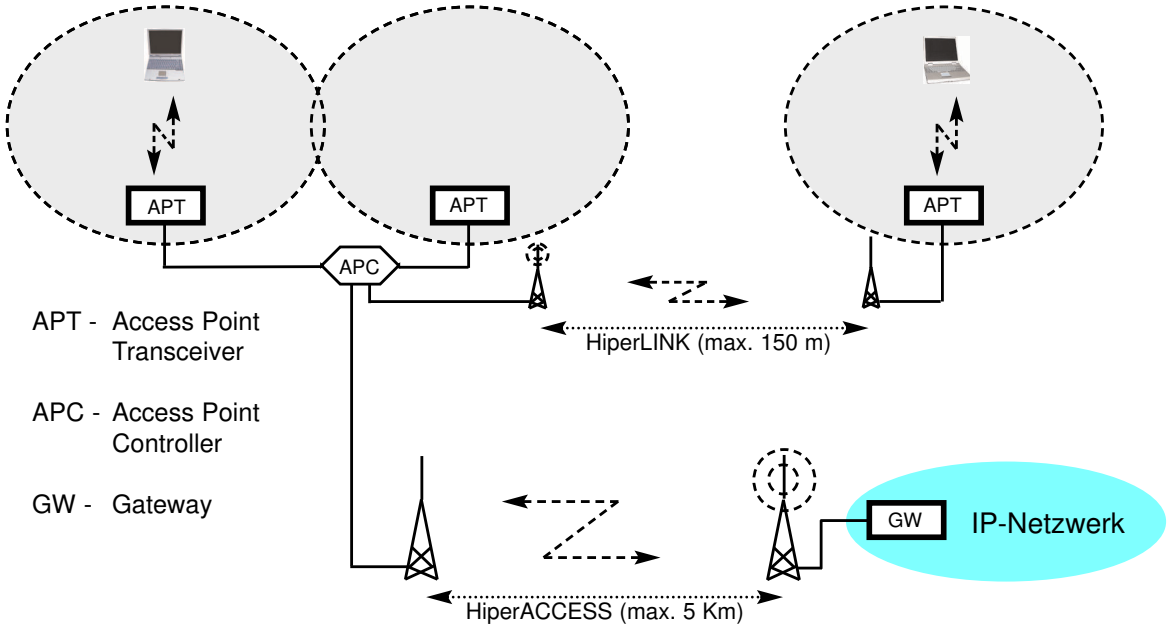


Abbildung 14: Breitbandige Funkzugangsnetze nach ETSI-BRAN

tatsächlich geheim bleiben. Der Verlust oder der Diebstahl eines einzigen Notebooks zieht die Anpassung aller mobilen Teilnehmer und Dienstzugriffspunkte nach sich [56].
[35] [50] [52] [32] [24] [25] [26] [33]

2.4.2 HiperLAN2

Die Standardisierung von HiperLAN2 (High Performance Radio Local Area Network) wird von der ETSI (European Telecommunications Standards Institute) vorangetrieben. HiperLAN2 ist dabei Teil des Projektes BRAN (Broadband Radio Access Network).
Ziel von BRAN ist die Entwicklung von breitbandigen, drahtlosen Zugangsnetzen, die bis zu 155 Mbit/s über die Luftschnittstelle transportieren können. Diese Zugangsnetze sind unabhängig von vorhandenen Infrastrukturen, können diese aber ergänzen.

Infrastruktur: BRAN setzt sich aus drei Teilstandards zusammen: HiperLAN2, HiperACCESS und HiperLINK. HiperLAN2 ist die Variante für kurze Entfernungen (200 m), über die der Zugang für das mobile Endgerät erfolgt und auf den hier noch genauer eingegangen werden soll.
HiperACCESS deckt in Form von Punkt-zu-Mehrpunkt-Verbindungen Entfernungen bis zu 5 Kilometer, mit Datenraten von durchschnittlich 27 MBit/s, ab. Die Variante HiperLINK dient der Punkt-zu-Punkt Verbindung von HiperLAN- und HiperACCESS-Stationen über kurze Strecken ($\sim$ 150 m), allerdings zu sehr hohen Datenraten ($\leq$ 155 Mbit/s).
In der Abbildung 14 ist dies skizziert.

HiperLAN2 unterstützt, wie auch die Standards der IEEE 802.11 Gruppe, einen zentralisierten Modus CM (Centralized Mode) und eine Ad-hoc Modus DM (Direkt Mode). Analog zu den bereits besprochenen Kommunikationsnetzen wird beim CM-Modus jede Funkzelle durch einen Netzzugangspunkt AP (Access Point) versorgt. Dabei ist jeder Zugangspunkt mit dem Kernnetzwerk verbunden. Es spielt hierbei keine Rolle, ob auf ein drahtgebundenes Kernnetz zurückgegriffen oder eine HiperACCESS und HiperLINK basierende Infrastruktur genutzt wird.
Mobile Endgeräte können sich innerhalb der Zellen frei bewegen und werden automatisch von dem günstigsten Zugangspunkt aus versorgt. Ein Zugangspunkt setzt sich aus einem *Access Point Controller* APC und einem oder mehreren *Access Point Transceivers* APT zusammen.
HiperLAN2 nutzt, gemeinsam mit IEEE 802.11a, das 5.2 GHz IMT-Band und setzt für die Modulation ebenfalls OFDM ein. Die wesentlichen Unterschiede zu IEEE 802.11a liegen im Mediumzugriff. HiperLAN2 unterstützt *Quality of Service*, dynamische Frequenzzuweisung und verschiedene Sicherheitsmechanismen.
Vor der Übertragung von Nutzdaten richtet HiperLAN2 logische Verbindungen ein. Durch die Verbindungsorientierung wird *Quality of Service* möglich. Für einzelne Verbindungen können dienstgütespezifische Parameter vereinbart werden. Dies betrifft in erster Linie die Datenrate, maximale Latenzzeiten und deren Varianz, sowie die Verlustrate.
Bei dynamischer Frequenzzuweisung DFS (Dynamic Frequency Selektion) führen die Zugangspunkte und die mobilen Endgeräte Interferenzmessungen durch. So bestimmen sie die geeignetsten Frequenzen für eine Übertragung innerhalb des zur Verfügung stehenden Frequenzspektrums. Ein HiperLAN2-Netz kann auf diesem Wege störende Einflüsse bis zu einem gewissen Grad kompensieren.
Es wird an einer Schnittstelle zwischen UMTS und HiperLAN2 gearbeitet. HiperLAN2-Netzwerke sollen so ohne großen Aufwand in öffentliche UMTS-Strukturen integriert werden können.

Übertragungsraten: Von HiperLAN2 werden Datenraten von 6, 9, 12, 27, 36 und 54 Mbit/s unterstützt. Die Nettodatenraten sollen deutlich über 50% sein.
Die maximale Bewegungsgeschwindigkeit, bei der noch eine Übertragung möglich ist, liegt bei 36 Km/h.

Sicherheit: HiperLAN2 unterstützt eine zweiseitige Authentifizierungprozedur mittels public-key / private-key. So ist sowohl eine Authentifizierung des mobilen Endgerätes gegenüber dem Netz, als auch des Netzes gegenüber dem Endgerät möglich.
Als Verschlüsselungsalgorithmen werden DES (Data Encryption Standard) und Triple-DES angeboten. DES gehört zu den am ausführlichsten untersuchten Verschlüsselungsverfahren mit einer festen Schlüssellänge von 56 Bit. Triple-DES wendet die DES-Methode auf den zu verschlüsselnden Text dreimal mit unterschiedlichen Schlüsseln an, um das Verfahren sicherer zu machen.
[20] [45] [5] [30] [12]

2.5 Drahtlose PANs

Private Area Networks (PANs) sind weniger auf hohe Bandbreiten, sondern mehr auf geringe Kosten und Stromverbrauch spezialisiert. Sie sollen mittelfristig Verkabelungen mit niedrigen Bandbreiten zu Peripheriegeräten, wie Drucker, mp3-Player oder Digitalkamera, überflüssig machen. Mit PANs lassen sich auch Ad-hoc Netzwerke zwischen mobilen Endgeräten realisieren. PANs können jedoch auch über Handys, welche dieselbe Übertragungstechnologie beherrschen, drahtlosen Zugriff auf das Mobilfunknetz bieten.

In jedem Fall befinden sich die beteiligten Geräte bei PANs immer in unmittelbarer Nachbarschaft. Es dürfen sich keine dämpfungsintensiven Hindernisse zwischen den vernetzten Geräten befinden.

2.5.1 IrDA

IrDA (Infrared Data Assoziation) nutzt infrarotes Licht im 300-THz–Bereich (900 nm) zur Übertragung. Es wird entweder diffuses oder gerichtetes Licht eingesetzt. Bei gerichtetem Licht muss eine Sichtverbindung bestehen.

Es werden LEDs (Light Emitting Diode) oder Laserdioden als Sender und Photodioden als Empfänger eingesetzt.

Die ursprüngliche Version 1.0 sah 115 Kbit/s Übertragungsrate vor. Die aktuelle Version 1.1 lässt etwa 1 und 4 Mbit/s zu. Der geplante FIR-Standard (Fast Infrared) soll bis zu 16 Mbit/s ermöglichen. Hohe Datenraten sind allerdings nur bei kurzen Distanzen ($\sim$50 cm) und bei direkter Sichtverbindung möglich. Wesentlicher Vorteil von Infrarotübertragung ist die Unempfindlichkeit gegenüber elektrischen Störungen.

IrDA ist eine sehr kostengünstige Übertragungstechnologie und es sind auf dem infraroten Frequenzband keine Lizenzen notwendig. IrDA wird warscheinlich durch die Bluetoothtechnologie verdrängt werden.

Sicherheitsmechanismen unterstützt IrDA lediglich auf der Applikationsebene.

[23]

2.5.2 Bluetooth

1998 haben sich 5 Firmen zusammengeschlossen, um unter der Federführung von Ericson die Entwicklung einer lizenzfreien drahtlosen Kommunikationstechnologie für den Handheld-Markt voranzutreiben. Resultat dieser Bemühungen ist Bluetooth.

Der Name Bluetooth kommt von dem dänischen König Harald Bluetooth, der vor mehr als tausend Jahren maßgeblich zur Vereinigung der nordischen Völker beigetragen hat.

Im Februar 2001 wurde die Kommunikationstechnologie Bluetooth in der Version 1.1 verabschiedet.

Da Bluetooth in erster Linie für mobile Endgeräte entworfen wurde, besitzt es verschiedene Verfahren, um den Stromverbrauch zu reduzieren.

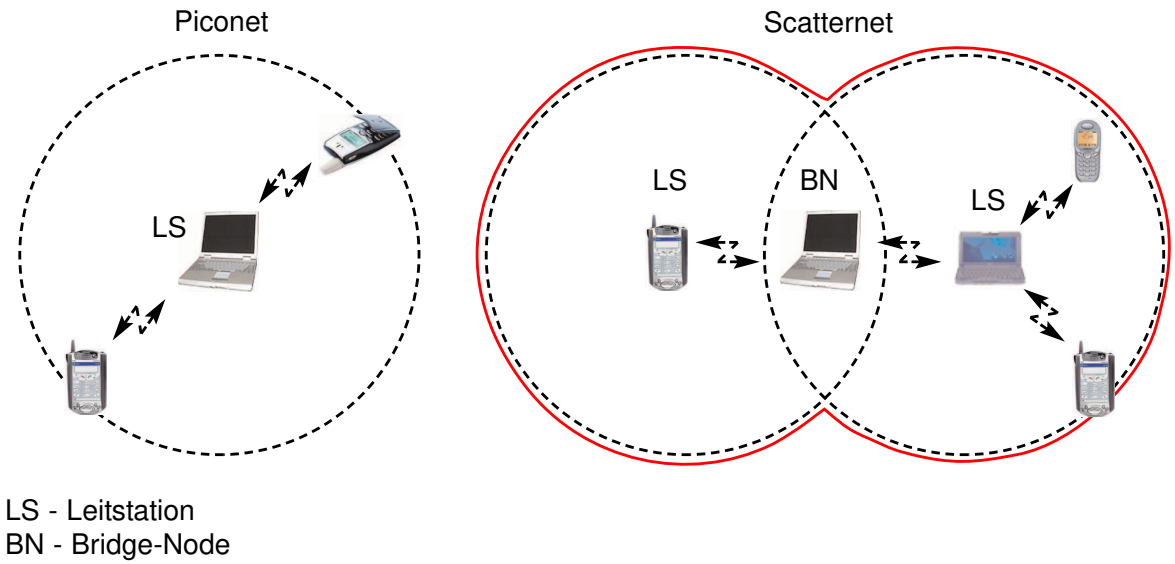


Abbildung 15: Piconetz und Scatternetz

Infrastruktur: Bluetooth ist auf keine feste Infrastruktur angewiesen. Es kann sowohl für Punkt-zu-Punkt Verbindungen, als auch für Verbindungen zu mehreren Kommunikationsteilnehmern eingesetzt werden.

Zwei oder mehr Teilnehmer, die sich einen Kommunikationskanal teilen, bilden ein Piconetz. Ein Kommunikationspartner übernimmt immer die Funktion der Leitstation. Alle weiteren Stationen ordnen sich der Leitstation unter und werden automatisch zu Folgestationen. Jede Station besitzt die Fähigkeit, Leitstation zu sein und ein Bluetooth-Netz zu bilden. Es ist pro Kommunikationszelle jedoch nur eine Leitstation möglich.

Bluetooth bildet Piconetze mit einer Zellausdehnung von 10 Metern. Es sind allerdings unter günstigen Bedingungen auch Zellen mit einer Größe von bis zu 100 Metern denkbar.

Die Vernetzung von Piconetzen erfolgt durch die Bildung von Umbrellazellen. Diese werden in Bluetooth als Scatternet bezeichnet. Ein Scatternet wird, wie in Abbildung 15 dargestellt, durch Bildung von Gruppen von Piconetzen möglich.

Innerhalb von Scatternetzen gibt es Endgeräte, die weiterleitende Funktionen einnehmen. Diese werden als *Bridge*-Knoten bezeichnet. Dabei gehören *Bridge*-Knoten zwei oder mehr Piconetzen an. Solch ein Knoten partizipiert aktiv an einer Pikozelle für einen begrenzten Zeitraum und wechselt dann die Zelle. Pakete anderer Endgeräte können so von *Bridge*-Knoten in andere Zellen weitergereicht werden.

In den von Bluetooth gebildeten Pikonetzen existieren bis zu 7 aktive Folgestationen. Die Beschränkung auf max. 8 aktive Geräte folgt aus den von Bluetooth genutzten internen 3-Bit-Adressen. Es können jedoch bis zu 256 passive Teilnehmer an einem Pikonetz partizipieren. Passive Teilnehmer besitzen 8-Bit-Adressen. Geräte mit passiven Adressen sind zwar nicht aktiv am Netz beteiligt, bleiben jedoch mit dem Takt und der Sprungsequenz der Leitstation synchron.

Von Bluetooth wird das weltweit lizenzfreie ISM-Frequenzband von 2.400 bis 2.483 GHz genutzt. Bei einer verfügbaren Bandbreite von 80 MHz nutzt Bluetooth 79 Trägerfrequenzen im Abstand von 1 MHz.
Zur Bildung des Übertragungskanals setzt Bluetooth ein Frequenzsprungverfahren mit 1600 Sprüngen pro Sekunde ein, was es relativ robust gegen Störungen macht. Der Wechsel durch die 79 Träger wird von einer Pseudo-Zufalls-Sprungfolge bestimmt.
Die Sprungfolge wird von der Leitstation mit Hilfe ihrer Geräteadresse und einer internen Uhr gebildet. Geräte, die sich mit der Leitstation synchronisieren und die gleiche Sprungfolge einsetzen, können an dem von ihr gebildeten Pikonetz teilhaben. Die Leitstation steuert den Mediumzugriff innerhalb des von ihr gebildeten Piconetzes.
Die Datenübertragung erfolgt paketorientiert. Jedes Paket erstreckt sich normalerweise über einen Zeitschlitz. Es sind jedoch auch Pakete mit einer Größe von maximal fünf Zeitschlitzen zulässig.
Die Pakete setzen sich aus einem Zugriffscode, dem Paketkopf und der Nutzlast zusammen.
Die Zeitschlitze sind zyklisch von 0 bis 2^{27} durchnummeriert. Die Leitstation beginnt ausschließlich in geraden nummerierten Zeitschlitzen mit der Sendung von Paketen. Folgestationen übermitteln ihre Pakete nur in ungeraden Zeitschlitzen.
Bluetooth bietet einige Mechanismen, um Paketverlusten in Umgebungen mit höheren Bitfehlerraten entgegenzuwirken. Mithilfe von Vorwärtsfehlerkorrekturmechanismen (Forward Error Correction, FEC) wird eine erhöhte Redundanz erreicht. Durch schnelle Übertragungwiederholungsverfahren (Automatic Repeat Request, ARQ) werden Pakete solange neu übertragen, bis eine erfolgreiche Übertragung im folgenden Zeitschlitz bestätigt wird.
Um fehlerhafte Nutzdaten schnell zu erkennen, setzt Bluetooth einen CRC-16 (16 Bit Cyclic Redundancy Check) ein.

Übertragungsraten: Das von Bluetooth genutzte Übertragungsprotokoll unterstützt sowohl synchrone, verbindungsorientierte Übertragung SCO (Synchronous Connection Oriented), als auch asynchrone, verbindungslose Übertragung ACL (Asynchronous Connection Less).
Die verbindungsorientierte SCO-Übertragung dient Punkt-zu-Punkt-Verbindungen zwischen einer Leitstation und einer Folgestation. Zeitschlitze lassen sich hier fest reservieren. SCO ist geeignet für die Übertragung von Sprachdaten. Jeder SCO-Kanal besitzt 64 Kbit/s synchrone Übertragungskapazität in jede Übertragungsrichtung.
Der verbindungslose ACL-Kanal kann bis maximal 723.2 Kbit/s asymmetrisch übertragen. Für den Rückkanal stehen dann allerdings lediglich 57.6 Kbit/s zur Verfügung. Ein symmetrischer ACL-Kanal kann bis zu 433.9 Kbit/s gleichzeitig in beiden Richtungen übertragen.
Leitstationen können entweder einen ACL-Kanal, 3-SCO-Kanäle oder einen ACL und einen SCO-Kanal gleichzeitig betreiben. Dabei ist es unabhängig davon, ob es sich um einen oder verschiedene Kommunikationspartner handelt.
In Tabelle 8 sind alle möglichen Übertragungsraten tabellarisch aufgeführt.

Sicherheit: Auch Bluetooth kann ein *Challenge-Response*-Verfahren für die Authentifizierung verwenden. Dabei kann die Authentifizierung sowohl einseitig, als auch in beiden Rich-

Datenrate in Kbit/s (symmetrisch)	Datenrate in Kbit/s (asymmetrisch)		FEC	CRC	Pakettyp
64.0	-	-	√	-	SCO
64.0	-	-	√	-	“
64.0	-	-	-	-	“
108.8	108.8	108.8	√	√	ACL
172.8	172.8	172.8	-	√	“
258.1	387.2	54.4	√	√	“
390.4	585.6	86.4	-	√	“
286.7	477.8	36.3	√	√	“
433.9	723.2	57.6	-	√	“

Tabelle 8: Verfügbare Datenraten unter Bluetooth

tungen erfolgen. Eingesetzt wird ein modifizierter SAFER+-Algorithmus mit einer Schlüssellänge von 128 Bit.

Die eingesetzten Sicherheitsalgorithmen zur Verschlüsselung der Nutzdaten verwenden die öffentliche Kennung des Gerätes, einen geheimen privaten Schlüssel und eine intern erzeugte Zufallszahl für die Verschlüsselung der Daten. Dabei kommt ein Bluetooth-eigenes Verfahren mit variabler Schlüssellänge zwischen 8 und 128 Bit zum Einsatz. Für jede einzelne Transaktion wird eine eigene Zufallszahl generiert.

Der Anspruch an die bei Bluetooth eingesetzten Sicherheitsmechanismen ist nicht sehr hoch. Ihre Aufgabe ist lediglich einen gewissen lokalen Bereich des Vertrauens zu schaffen. Komplexere Verfahren bleiben den Applikationen überlassen.

[4] [6] [7] [61]

2.6 Zusammenfassung und Auswertung

Dieses Kapitel bot eine Einführung in die drahtlose Kommunikationstechnik. Es wurden die digitalen Mobilfunknetze GSM und UMTS, sowie die GSM Trägerdienste HSCSD, GPRS und EDGE vorgestellt. Es wurde auf die verbreiteten WLAN-Standards IEEE 802.11 und IEEE 802.11b eingegangen, wie auch auf deren breitbandigere, potentielle Nachfolgetechnologien IEEE 802.11a und HiperLAN2. Schließlich wurden die PAN-Technologien IrDA und Bluetooth beschrieben.

Alle drahtlosen Übertragungstechnologien wurden hinsichtlich ihrer Infrastruktur, unterstützten Datenraten und den implementierten Sicherheitsmechanismen untersucht.

Zusammenfassend konnte folgendes festgestellt werden:

2.6.1 Mobilfunknetze

Infrastruktur und Akzeptanz: Zum gegenwärtigen Zeitpunkt haben wir in Deutschland eine fast vollständige Netzabdeckung mit GSM. Die durch die Trägerdienste HSCSD und GPRS möglichen höheren Datenraten werden auch von aktuelleren Endgeräten unterstützt und von den Mobilfunkbetreibern angeboten. Bei der Nutzung sind allerdings nur langsam ansteigende Zuwachsraten zu beobachten. Zumindest für GPRS wird es mit dem fortschreitenden Ausbau von UMTS zukünftig auch eine noch höhere Verfügbarkeit geben.
Der GSM-Trägerdienst EDGE wird im Moment noch nicht angeboten. Auch existieren noch keine Endgeräte, welche die neuen Modulationstechniken beherrschen. Die Einführung von EDGE ist aufgrund der hohen Investitionskosten auch noch ungewiss.
UMTS wird bis zum Jahre 2005 in den Ballungsräumen flächendeckend zur Verfügung stehen. Es werden bereits im Handel Endgeräte angeboten, die neben GSM und den Trägerdiensten auch die neue Übertragungstechnik beherrschen. Unklar ist hier, ob die neue Technik tatsächlich von den mobilen Teilnehmern akzeptiert wird. Die Kosten für den Ausbau der Infrastruktur und die Lizenzen sind in Deutschland so hoch, dass mit hohen Nutzungskosten zu rechnen ist.
Satellitenfunksysteme sind bereits seit längerer Zeit im Einsatz. Technisch ist die Anbindung an die digitalen Mobilfunknetze ebenfalls schon möglich, allerdings ist die Nutzung aufgrund sehr hoher Kosten für Endgeräte und Betrieb zur Zeit nur Minderheiten vorbehalten. Mittelfristig wird Satellitenfunk als Standard-*Fallback*-Technologie für den Mobilfunk genutzt werden und damit eine größere Verbreitung finden. Dies lässt sich insbesondere auch am Einzug von S-UMTS in UMTS ablesen, womit der Satellitenfunk als fester Bestandteil einer zukünftigen globalen Infrastruktur eingeplant ist.
Für einen Teilnehmer, der ausschließlich auf Mobilfunk sowie Satellitentechnologien zugreift, lässt sich damit eine optimale Mobilität erreichen. Insbesondere das in der Motivation dieser Arbeit aufgeworfene Problem der ortsunabhängigen und kontinuierlichen Netzanbindung ist damit erfüllt.
Zu einer flächendeckenden Infrastruktur für Mobilfunknetze und insbesondere für die Satellitentechnik ist zu bemerken, dass deren Aufbau mit hohen Kosten verbunden ist. Nicht unerheblich ist hierbei die stets zu wahrende Abwärtskompatibilität bei neu einzuführender Technik. Zusätzlich treten Kosten durch die Nutzung von lizenzpflichtigen Frequenzbändern auf. Da alle Kosten auf den Endnutzer umgelegt werden müssen, stellen diese einen bremsenden Faktor in der Verbreitung dieser Technologien dar.

Datenraten und Bewegungsgeschwindigkeit: Hinsichtlich der Datenraten wurde festgestellt, dass GSM den heutigen Anforderungen nicht mehr gewachsen ist. HSCSD und GPRS bringen diesbezüglich Verbesserungen. EDGE könnte eine Datenübertragungsrate weit über den beiden bereits im Einsatz befindlichen Trägerdiensten bieten. Erst mit UMTS wird ein Standard zur Verfügung stehen, der zumindest mittelfristig die derzeitigen Anforderungen der Datenübertragung erfüllen kann.
Ein großer Nachteil des GSM-Netzes liegt in der verbindungsorientierten Weiterleitung von Daten, wodurch die theoretisch mögliche Datenrate innerhalb einer Zelle nicht ausgenutzt

werden kann. Wie gezeigt wurde, verschärft sich dieses Problem bei HSCSD. Mit GPRS wird paketorientierter Betrieb möglich, was zu einer effizienteren Zellnutzung führt. Dazu müssen hierfür die GPRS-Datenkanäle dauerhaft reserviert werden. Erst mit UMTS entfällt auch diese Beschränkung.
Die Übergabe von Verbindungen ist ein wichtiger Aspekt bei der mobilen Kommunikation. Dieses Roaming sowohl innerhalb der einzelnen Mobilfunksysteme als auch zwischen Systemen unterschiedlicher Generationen ist problemlos möglich. Durch die geplante Einbindung von Satellitennetzen mit S-UMTS wird es sogar globales Roaming geben. Roamingvorgänge sind in Mobilfunktnetzen auf eine hohe Mobilität hin ausgelegt. Bei allen vorgestellten Systemen ist auch bei hohen Bewegungsgeschwindigkeiten eine Kommunikation möglich.

2.6.2 Wireless LANs und PANs

Infrastruktur und Akzeptanz: Für drahtlose LAN und PAN Architekturen stellt sich das Problem der großflächigen Netzabdeckung nicht, da für deren Einsatz eine andere Zielsetzung besteht. Es werden mittelfristig in Ballungsräumen *hot spots* mit kurzreichweitigen Wireless LAN-Systemen zur Verfügung stehen.
Der WLAN-Standard IEEE 802.11b ist momentan die meist eingesetzte drahtlose Kommunikationstechnik für Rechnernetzwerke. Entsprechende Hardware steht seit etwa zwei Jahren zur Verfügung. Stetig sinkende Kosten für Infrastruktur und Endgeräte, sowie mit drahtgebundenen LANs vergleichbaren Übertragungsraten, sorgen für eine weitere Verbreitung.
Für die konkurrierenden Folgestandards IEEE 802.11a und HiperLAN2 sind momentan nur wenige beziehungsweise keine Geräte verfügbar. Die weitere Entwicklung ist hier schwer abschätzbar und von den Kosten, sowie den tatsächlich angebotenen Nettobandbreiten beider Technologien, abhängig. Sie werden mittelfristig den IEEE 802.11b-Standard ergänzen und ersetzen und auf absehbare Zeit in bestimmten Bereichen drahtgebundene LAN-Strukturen verdrängen.
IrDA ist ein sehr verbreiteter PAN-Standard. Obwohl die Übertragungstechnik in vielen Geräten eingebaut wurde, konnte sie sich beim Endnutzer nicht recht durchsetzen. Die Nachfolgetechnolgie Bluetooth ist noch relativ neu, wird aber bereits in diverse Endgeräte eingebaut. Hier ist zu erwarten, dass sich diese Technologie in naher Zukunft beim Endnutzer durchsetzen wird.
Die Kosten für den Aufbau eines WLANs sind zum gegenwärtigen Zeitpunkt noch relativ hoch. Da für die Nutzung der Frequenzbänder keine Lizenzkosten anfallen werden, beschränken sich die Kosten auf die Hardware, so dass hier mittelfristig mit relativ geringen Kosten für den Betrieb zu rechnen ist. Die Kosten für die recht einfache PAN-Technik sind mittlerweile so sehr gesunken, dass schon jetzt eine hohe Verbreitung festzustellen ist.

Datenraten und Bewegungsgeschwindigkeit: Die unterstützten Bandbreiten für die Datenübertragung mittels WLAN-Technologie sind teilweise wesentlich höher als bei Mobilfunknetzen. Allerdings sind auf Grund der geringen Zellgröße hier Einschränkungen bezüglich der Mobilität festzustellen.

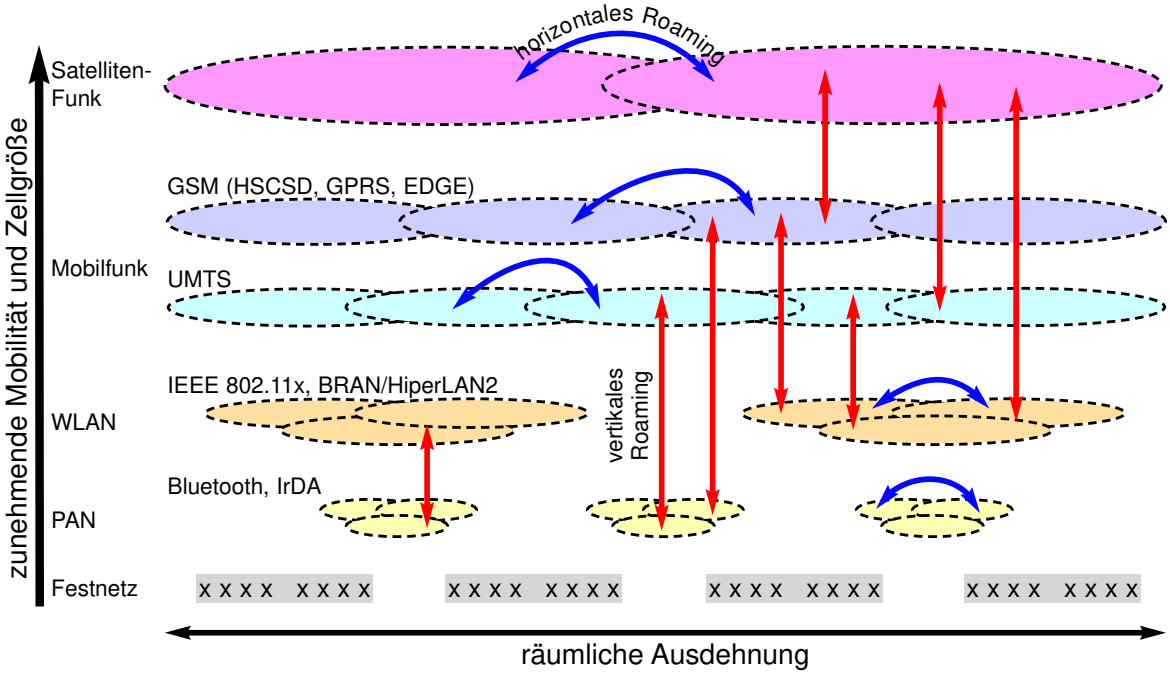


Abbildung 16: Anforderungen an eine drahtlosen Infrastruktur

Die angebotenen Datenraten bei den PANs liegen zwischen denen des digitalen Mobilfunks und von WLANs. Wegen der geringen Zellgröße werde hier faktisch keine hohen Bewegungsgeschwindigkeiten unterstützt. Auch sehen die vorgestellten Standards kein systemübergreifendes Roaming vor. Dieses liegt auch nicht im Fokus der Technologie, vielmehr ersetzen drahtlose PANs das Datenkabel im Nahbereich.

2.6.3 Sicherheit

Ein großes Problem stellen Authentifikation, Datenintegrität und Verschlüsselung bei der drahtlosen Übertragung dar. Es ist festzustellen, dass keine der vorgestellten Kommunikationstechnologien als sicher betrachtet werden kann. Dies macht den Einsatz von Sicherheitsmechanismen auf höheren Ebenen zwingend notwendig.

2.6.4 Fazit

Um sowohl die Vorteile der Mobilkommunikation hinsichtlich der hohen Netzabdeckung und Mobilität als auch der drahtlosen LAN und PAN-Technologien bezogen auf die hohen Datenübertragungsraten und der geringen Nutzungskosten optimal anwenden zu können, ist ein erschöpfendes, systemüberbreifendes Intra- und insbesondere Inter-System-Roaming (Abbildung 16) wünschenswert.

Ein netzseitiges Roaming von Mobilfunknetzen in drahtlose LANs und PANs erscheint zur Zeit noch nicht möglich.
In den Tabellen 2.6.4 und 2.6.4 sind die beschriebenen Eigenschaften der vorgestellten Technologien noch einmal zusammenfassend aufgeführt.

Technologie	Frequenzband	Datenraten	Zellradius	Mobilität	Verfügbarkeit
GSM	890 - 960 MHz 1710 - 1880 MHz 1850 - 1990 MHz 460.4 - 496 MHz	2.4-9.6 Kbit/s 14.4 Kbit/s (optional) “ ?	0.5-35 Km 0.5-8 Km “ ?	250 Km/h	1992
HSCSD	GSM	4.8-57.6 Kbit/s	GSM	250 Km/h[a]	1999
GPRS	GSM	9.05-171.2 Kbit/s	GSM	250 Km/h	2001
EDGE	GSM	max. 384 Kbit/s	GSM	250 Km/h	2002
UMTS	1885-2025 MHz, 2110-2200 MHz	144 kbit/s 384 kbit/s 2 Mbit	30 m - 20 Km	500 Km/h 120 Km/h 6-10 Km/h	2003
Satellitenfunk (SUMTS)	1980 - 2010 MHz 2170 - 2200 MHz div. Frequenzbereiche	1.2-64 Kbit/s 384 Kbit/s (geplant) (später einige Megabit)[b]	$>$ 200 Km	praktisch unbeschränkt	frühstens 2003
IEEE 802.11b	2.400-2.483 GHz	1-11 Mbit/s (brutto) 0.5 - 5 Mbit/s (netto)	50 - 250 m 15 - 50 m (indoor)	50-100 Km/h	2000
IEEE 802.11a	5.1-5.3 GHz	6-24 Mbit/s (brutto) bis 54 Mbit/s (optional) max. 25 Mbit/s (netto)	50 - 200 m 15 - 20 m (indoor)	36 Km/h	2002
HiperLAN2	5.1-5.3GHz	6-54 Mbit/s (brutto) max. 32 Mbit/s (netto)	50 - 200 m 15 - 20 m (indoor)	36 Km/h	2002
IrDA	300 THz (900 nm)	115 Kbit/s (V1.0) 1.152-16 Mbit/s (V.1.1)	0.5 - 10 m	kaum	1998
Bluetooth	2.400-2.483 GHz	64-192 kbit (SCO) 723.2/57.6 Kbit/s (ACL) 433.9 Kbit/s (ACL)	10 - 100 m	kaum	2001

Tabelle 9: Überblick der vorgestellten drahtlosen Kommunikationsnetze

[a] Roaming selten erfolgreich
[b] wenige tausend Nutzer pro Zelle

Technologie	Infrastruktur (Netzabdeckung)	Kosten Anschaffung[b]	Kosten Nutzung	Sicherheit Authentifikation	Sicherheit Verschlüsselung	Akzeptanz[a]
GSM	sehr hoch	gering	hoch	A3 [c]	A5, A8	sehr hoch
HSCSD	Ballungsgebiete	gering	hoch	“	“	gut
GPRS	Ballungsgebiete	gering	hoch	“	“	gut
EDGE	Ballungsgebiete [d]	?	?	“	“	-
UMTS	hot spot (geplant 2003)	?	?	(Milenage) proprietäre	Kasumi	-
Satellitenfunk	global	gering	sehr hoch	?	?	gering
IEEE 802.11b	lokal / hot spot	hoch	keine	MAC-Adresse SSID proprietär	WEP (RC4) [e]	hoch
IEEE 802.11a	lokal / hot spot (geplant 2002)	hoch	keine	optional proprietär	WEP	? [f]
Hiperlan2	lokal / hot spot (geplant 2002)	hoch	keine	public-key/ private-key	DES, Triple-DES	-[g]
IrDA	Nahbereich	gering	keine	keine	keine	sehr hoch
Bluetooth	Nahbereich / hot spot	gering	keine	SAFER+ (8-128 Bit)	eigenes Verfahren (128 Bit)	sehr hoch

Tabelle 10: Vergleich von Infrastruktur, Kosten, Sicherheit und Akzeptanz der vorgestellten Kommunikationsnetze

[a] innerhalb Europas
[b] bei Mobilfunk nur Endgeräte, da Infrastruktur vorhanden
[c] nur Endgerät gegenüber Basisstation
[d] (geplant 2002, Umsetzung zweifelhaft)
[e] 40 bzw. 104-Bit-Schlüssel
[f] Geräte erst seit kurzer Zeit verfügbar
[g] noch keine Endgeräte verfügbar

3 TCP/IP in drahtlosen Umgebungen

TCP/IP (Transport Control Protocol/Internet Protocol) ist ein Protokollsatz, der 1974 von der ARPA (Department of Defense Advanced Research Projects Agency) entwickelt wurde. Anfangs war er lediglich im Dienst des ARPANET und des US-Verteidigungsministeriums. Es handelte sich beim ARPANET um den Vorläufer des Internets, dessen Basis auch heute noch TCP/IP ist.
Im Jahre 1982 wurde TCP/IP als zentraler Bestandteil in eine der bedeutenderen UNIX-Versionen (UNIX 4.2 BSD) integriert. Heute gilt TCP/IP als Standard-Protokollsatz für die paketorientierte Datenübertragung.
Das Internetprotokoll IP dient der Adressierung und Weiterleitung von Nachrichten. Nachrichten werden hier in kleine Pakete aufgeteilt und über verbundene Netzwerke hinweg zu einem Zielrechner transportiert. Durch IP werden auch empfangene Pakete wieder zusammengefügt.
Der Transportprotokoll TCP sorgt für die korrekte Reihenfolge der Nachrichten und für das erneute Senden bei fehlerhaften Übertragungen.
Beide Protokolle wurden hinsichtlich der Eigenschaften stationärer Endgeräte und drahtgebundener Kommunikationswege entwickelt. Dem Einsatz des IP-Protokolls mit mobilen Endgeräten sind enge Grenzen gesetzt. Der TCP-Protokoll erfüllt seine Aufgabe auf drahtlosen Verbindungen nur noch unzureichend.
Im Folgenden wird gezeigt, wo die Probleme im Einzelnen auftreten und welche Lösungsmöglichkeiten zur Verfügung stehen.
[53]

3.1 Paketweiterleitung mit IP

Eine Postanschrift setzt sich aus einem Namen, einer Straße, einer Hausnummer, einer Stadt, einer Postleitzahl und einem Land zusammen. Unabhängig davon, in welchem Land man einen Brief abgibt, ist eine Auslieferung möglich, ohne eine Liste aller möglichen Empfänger zu besitzen. Die Adressierung bildet eine hierarchische Struktur, die es jeder Poststelle ermöglicht, eine Weiterleitung zu veranlassen.
Das Internetprotokoll IP veranlasst entsprechend dem hierarchischen Prinzip die Weiterleitung von Paketen eines Quellrechners zu einem Zielrechner.
Durch Router sind einzelne Netzwerke miteinander verbunden. Sie leiten die Pakete innerhalb des Gesamtnetzverbundes weiter. Jedes Paket besitzt einen Paketkopf, in dem eine Quell- und eine Zieladresse steht. Diese Netzadressen werden als IP-Adressen bezeichnet. Jeder Host und jeder Router besitzt eine eigene, eindeutige IP-Adresse. Die Weiterleitung erfolgt auch hier in Abhängigkeit von der IP-Adresse des Zielrechners. Die Router besitzen Tabellen, anhand derer sie den Weg zum nächsten Router für eine bestimmte IP-Adresse feststellen können.
Die IP-Adresse lässt sich in einen Präfix und einen Suffix einteilen. Der Präfix identifiziert das Netz, an dem das Endgerät angeschlossen ist, und der Suffix identifiziert das bestimmte Netzelement. Alle Geräte in einem Netz müssen den gleichen Adresspräfix besitzen. Netze können

zu Netzen höherer Klasse zusammengefasst werden. Somit bildet sich hier eine hierarchische Netzstruktur, die es den Routern ermöglicht, ihre Tabellen so klein wie möglich zu halten.
So ergibt sich, dass eine IP-Adresse einem festen Netzzugangsbereich zugewiesen ist. Bei einem Netzwechsel eines mobilen Endgerätes können an den neuen Netzzugangspunkt keine Daten mehr ausgeliefert werden, sofern die alte Adresse beibehalten wird. Im Beispiel entspricht dies dem Umstand, dass eine Auslieferung eines Briefes nach einem Umzug des Empfängers nicht möglich ist, da die Adresse keine Gültigkeit mehr besitzt. Eine Beibehaltung der vollständigen Adresse ist nicht möglich, da es das hierarchische Schema zerstören würde.
Für das IP-Protokoll gibt es zwei naheliegende Lösungsansätze, um dieses Problem zu lösen:

- dynamische Anpassung und Veröffentlichung der IP-Adresse
- Wegewahl durch eine adaptive Konfiguration der Routertabellen

[31]

3.1.1 Anpassung der Adresse

Ein Knoten kann seine alte IP-Adresse verwerfen und über einen Verteilmechanismus eine neue, gültige Adresse anfordern. Das *Dynamic Host Configuration Protocol* (DHCP) [10] ist solch ein Verteilmechanismus. DHCP kann einen Rechner mit allen notwendigen Daten versorgen, die für eine Netzintegration notwendig sind. Ein mobiles Endgerät kann jedesmal, wenn es seinen Dienstzugangsbereich wechselt, vom Gastnetz neue Konfigurationsparameter zugewiesen bekommen. Dazu gehören eine topologisch korrekte IP-Adresse, ein DNS-Server (Domain Name System), die geforderte MTU-Größe (Maximal Transfer Unit) und der zuständige Router.
Bei einem Wechsel der IP-Adresse müssen Verbindungen höherer Schichten neu aufgebaut werden. Häufige Adresswechsel führen zwangsläufig zu ernsthaften Problemen mit einigen Protokollen. Auch ist ein betroffenes Endgerät, sobald es das Netz wechselt, nicht mehr erreichbar, da seine neue IP-Adresse den Kommunikationsteilnehmern nun nicht mehr bekannt ist. Die Aktualisierung im *Domain Name System* benötigt im günstigen Fall einige Minuten, um die neue Adresse weltweit korrekt abzubilden. Für schnelle Änderungen der IP-Adressen vieler mobiler Endgeräte ist DNS aus diesem Grund ungeeignet.

3.1.2 Anpassung der Routen

Die zweite Möglichkeit ist, dass speziell für die IP-Adresse eines mobilen Endgerätes in allen betroffenen Netzelementen spezielle Routen konfiguriert werden, die Pakete im Netz entsprechend weiterleiten.
Die Einrichtung spezifischer Routen ist allerdings mit hohem Konfigurationsaufwand verbunden. Die Wegewahltabellen weltweit aller am Internet beteiligten Router müssten ständig geändert werden, um mobile Rechner zu berücksichtigen.
Dieser Ansatz ist nur für eine sehr geringe Anzahl von Knoten praktikabel.

3.2 Mobile IP

Mobile IP [42] löst das beschriebene Problem, indem es dem mobilen Teilnehmer erlaubt, zwei unterschiedliche IP-Adressen zu besitzen: eine Heimatadresse und eine temporäre Adresse.
Die Heimatadresse dient zur eindeutigen Identifizierung des mobilen Endgerätes. Unter ihr ist das mobile Endgerät für Kommunikationspartner erreichbar, und durch sie lassen sich dauerhafte Verbindungen durch höhere Protokolle aufbauen. Sie verändert sich nicht und ist unabhängig vom Standort des mobilen Endgerätes.
Für die Lokalisierung außerhalb des Heimatnetzes wird die zusätzliche temporäre Adresse herangezogen. Diese wird als *Care-Of-Adress* (COA) bezeichnet.
Mobile IP geht davon aus, dass jedes mobile Endgerät einen über seine Heimatadresse ständig erreichbaren, stationären Heimatagenten besitzt. Der Heimatagent kann sich in dem Router befinden, der für das Heimatnetz verantwortlich ist, oder auf einem beliebigen stationären Rechner innerhalb des Heimat-Subnetzes.
Aufgabe des Heimatagenten ist, die Standorte des mobilen Teilnehmers zu verfolgen und ankommende Pakete an diesen weiterzuleiten.
Netzbereiche, in denen ein Mobilitätsservice angeboten wird, besitzen ebenfalls einen Agenten. Dieser bietet einen Weiterleitungsservice für mobile Endgeräte, die sich außerhalb ihres Heimatnetzes befinden und wird als Fremdagent (FA) bezeichnet. Er übernimmt die Versorgung von mobilen Endgeräten, die sich innerhalb ihres Subnetzes befinden, allerdings nicht Teilnehmer des selben sind. Von ihm wird das mobile Gerät mit einer COA-Adresse versorgt.
Agenten können sowohl Heimatagent als auch Fremdagent sein. Es ist auch möglich, Mobile IP in Netzen zu nutzen, die keinen Fremdagenten, jedoch einen Adressverteilungsservice, z.B. DHCP, anbieten.
In Abbildung 17 sind alle Elemente dargestellt.

3.2.1 Entdeckung von Agenten

In einem Netzbereich, in dem Mobile IP angeboten wird, werden in regelmäßigen Abständen durch die Agenten spezielle Broadcast-Nachrichten gesendet. Diese *Agent Advertisements* informieren mobile Endgeräte über verfügbare COA-Adressen. Sie besitzen eine begrenzte Lebenszeit. Die Lebenszeit entspricht der Zeitspanne von drei aufeinander folgenden *Agent Advertisements*.
Endgeräte können auch von sich aus eine sogenannte *Agent Solitation* initiieren. Diese veranlasst einen Agenten zu einem sofortigen *Agent Advertisement*.
Beide Nachrichtentypen sind ICMP-*Router Discovery Messages* (Internet Control Message Protokoll) [22]. Für die Verwendung in Mobile IP wurden spezielle Erweiterungen der ICMP-Optionen eingeführt [42].
Anhand der regelmäßigen *Agent Advertisements* und des Präfix der darin enthaltenen COA-Adressen, kann das mobile Endgerät feststellen, ob es sich immer noch in demselben Netz befindet, oder ob ein Netzwechsel stattgefunden hat.
Wenn die Lebenszeit des letzten empfangenen *Agent Advertisement* abgelaufen ist, wird angenommen, dass der alte Fremdagent nicht mehr erreichbar ist und ein neuer gesucht werden

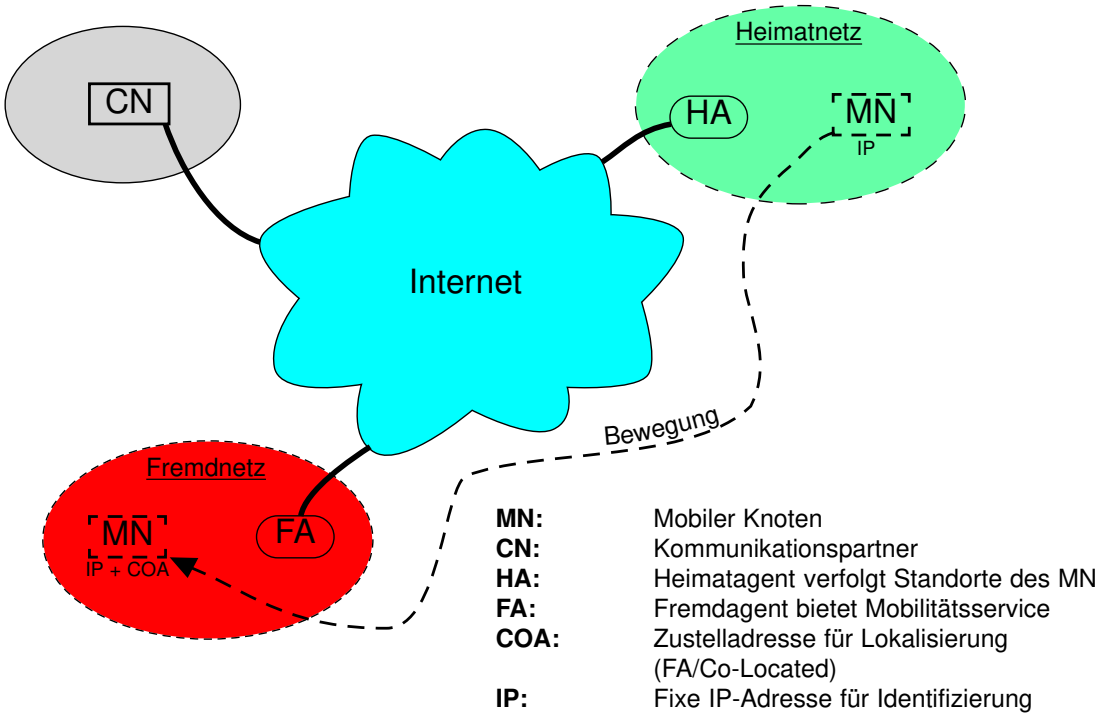


Abbildung 17: Elemente von Mobile IP

muss.
Erhält das mobile Endgerät ein *Agent Advertisement* mit COA-Adressen, deren Präfix sich von der genutzten COA-Adresse unterscheidet, so hat mit hoher Wahrscheinlichkeit ein Netzwechsel stattgefunden und ein neuer Agent ist zuständig. Dieser Vorgang der Netzüberwachung wird als *Move Detection* bezeichnet.
Innerhalb seines Heimatnetzes nutzt das mobile Endgerät keinerlei Mobilitätsservice. Wenn das Gerät aus einem Fremdnetz zurückkehrt, meldet es sich sofort bei seinem Heimatagenten ab, da es seine Unterstützung nicht mehr benötigt. Für die Kommunikation mit dem Heimatagenten aus Fremdnetzen wird eine An- und Abmeldungsprozedur eingesetzt.
Stellt das mobile Endgerät nun fest, dass es sich in einem Fremdnetz befindet, für welches es noch keine COA-Adresse besitzt, so bezieht es eine Adresse aus dem letzten erhaltenen *Agent Advertisement*. Es erhält so eine Fremdagenten-COA (FA-COA).
Sollte kein Fremdagent verfügbar sein, besteht die Möglichkeit, sich an einen externen Verteilerdienst zu wenden. Diese Adresse wird dann als *Co-Located*-COA bezeichnet.
In jedem Fall wird die neue temporäre IP-Adresse dem Heimatagenten durch eine Registrierung mitgeteilt. Pakete, die an das mobilen Endgerätes adressiert sind, werden nun vom Heimatagenten weitergeleitet.

3.2.2 Registrierung bei Agenten

Jedesmal, wenn ein mobiles Endgerät das Netz wechselt und sich eine neue COA nimmt, muss es die Agenten durch eine Registrierung darüber informieren.
Eine Mobile IP Registrierung beginnt damit, dass durch das mobile Endgerät eine *Registration Request* an den Fremdagenten geschickt wird. Dieser leitet die Nachricht an den Heimatagenten weiter. Der Heimatagent prüft die Nachricht auf Authentizität.
Für die Authentifizierung wird ein auf privaten Schlüsseln basierender MD5-Algorithmus eingesetzt [36]. Verläuft die Prüfung erfolgreich, wird durch eine *Registration Reply* über den Fremdagenten geantwortet.
Es ist auch möglich, dass die Registrierung direkt zwischen mobilem Endgerät und Heimatagenten durchgeführt wird.
Für Mobile IP Registrierungsnachrichten werden *User Datagram Pakete* (UDP) mit der festgelegten Portadresse 434 eingesetzt.
Die *Registration Request* enthält die feste IP-Adresse, die IP-Adresse des Heimatagenten, die temporäre COA-Adresse und ein 64-Bit-Feld. Das 64-Bit-Feld wird für die Authentifizierung herangezogen.
Neben weiteren Werten zur aktuellen Konfiguration und dem gewünschten Verbindungstyp ist auch eine Lebenszeit angegeben, in der eine Aktualisierung erfolgen muss.
Der Heimatagent richtet bei erfolgreicher Authentifizierung eine zeitlich begrenzte Verknüpfung zwischen der festen IP-Adresse des mobilen Knotens und seiner temporären COA-Adresse ein. Diese Verknüpfungen werden als *Mobility Bindings* bezeichnet.
Wenn die folgende *Registration Reply* über einen Fremdagent geht, so richtet dieser ebenfalls ein *Mobility Binding* ein. Das *Mobility Binding* enthält neben den bereits erwähnten Werten

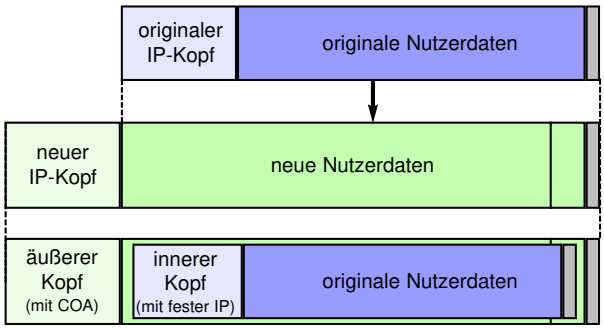


Abbildung 18: Kapselung von IP-Paketen

ein Codefeld, aus dem das mobile Endgerät entnehmen kann, ob die Registrierung erfolgreich verlaufen ist oder die begründete Ablehnung.
Auch die Lebenszeit ist hier wieder angeben. Es ist möglich, dass die Anfrage positiv beantwortet wird, aber eine andere Lebenszeit angeben ist. Dann gilt die vom Heimatagent angebotene. Wenn die Lebenszeit der Registrierung abgelaufen ist, werden die *Mobility Bindings* automatisch gelöscht.

3.2.3 IP-in-IP Kapselung

Eine Weiterleitung von Paketen vom Heimatagenten zum mobilen Endgerät, dass sich in einem Fremdnetz aufhält, erfolgt durch IP-in-IP Kapselung [27]. Dazu werden alle Pakete, die mit der Heimatadresse versehen sind, vom Heimatagenten abgefangen und in ein weiteres IP-Paket eingekapselt. Das äußere Paket enthält die COA-Adresse als Zieladresse. Dies ist in Abbildung 18 skizziert.
Diese gekapselten Pakete werden anschließend mit den Standardroutingmechanismen an die COA-Adresse weitergeleitet. Die Entkapselung kann entweder vom Fremdagenten oder bei Verwendung einer Co-Located COA-Adresse vom mobilen Endgerät selbst vorgenommen werden.
Die vom Endgerät ausgehenden Pakete werden mit der festen IP-Adresse als Absender direkt versendet.

3.2.4 Paketweiterleitung

Eine mögliche Kommunikationsprozedur ist in Abbildung 19 dargestellt, in der jedes Paket die folgenden fünf Schritte durchläuft:

1. Ein Paket wird an die Heimatadresse des Benutzers des mobilen Gerätes gesendet.
2. Die Heimatstation kapselt das Paket und sendet es an die Adresse des verantwortlichen Fremdagenten.
3. Dieser entpackt das gekapselte Paket und übergibt es direkt an das mobile Gerät.

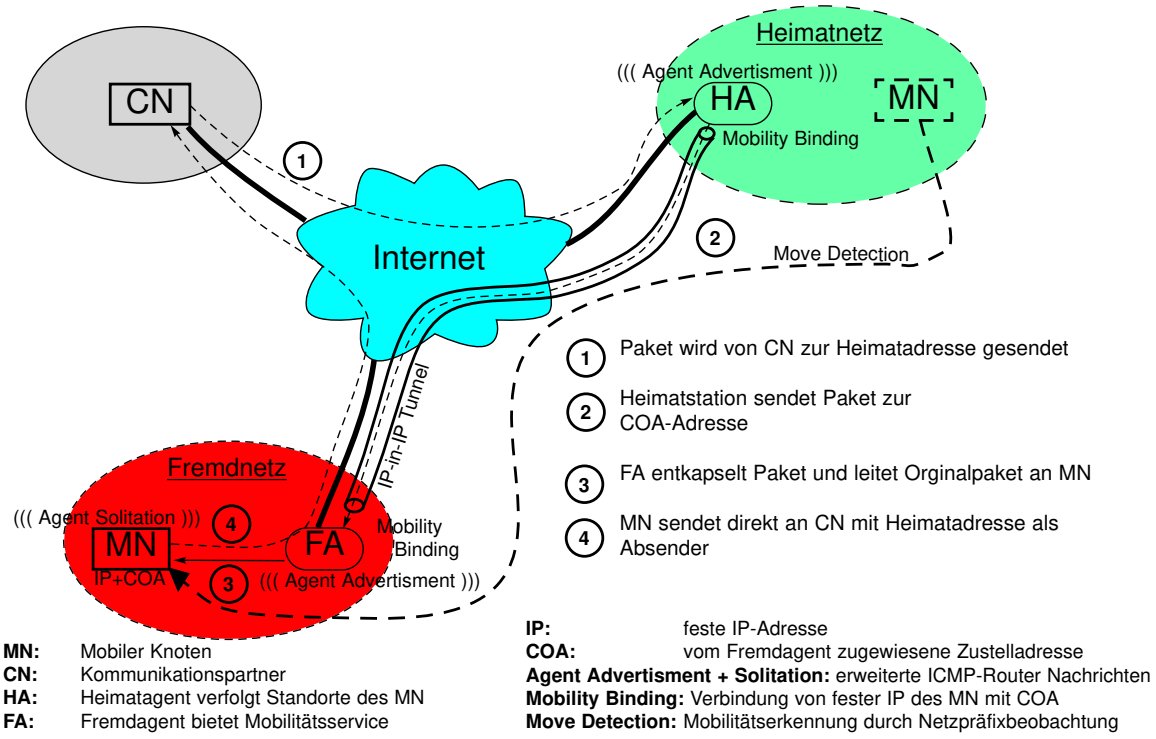


Abbildung 19: Paketweiterleitung mit Mobile IP

4. Das mobile Gerät sendet Pakete direkt an den Kommunkationspartner mit der festen IP-Adresse als Absender.

5. Die vom mobilen Host ausgehende Pakete werden mit Standardroutingmechanismen weitergeleitet.

3.2.5 Erweiterungen und Optimierungen

Reverse Tunneling: Die von Mobile IP vorgesehene direkte Versendung von Paketen vom mobilen Endgerät mit der festen IP-Adresse als Absender führt zu Problemen. *Firewalls* und viele Router nehmen sogenanntes *Ingress Filtering* vor. Dabei werden aus Sicherheitsgründen Pakete verworfen, deren Absenderadresse nicht mit dem Interface, aus dem sie kommen, konsistent ist.
Dieses Problem lässt sich durch *Reverse Tunneling* [47] lösen. Dazu werden die generierten Pakete erneut gekapselt und zum Heimatagenten zurückgeschickt. Dort werden die IP-Pakete wieder entkapselt und weiter versendet. So besitzen alle Pakete wieder topologisch korrekte Absenderadressen.

Momentan ist dies die einzig mögliche Variante, Mobile IP in größeren Netzen einzusetzen. *Reverse Tunneling* kann von einem mobilen Knoten durch ein reserviertes Feld in der *Registration Request* den Agenten ankündigt werden.

Optimierung der Routen: Das von Mobile IP genutzte *Triangular Routing*, in dem alle Pakete vom Kommunikationspartner vom Heimatagent weitergeleitet werden, ist nicht effizient. Durch die Nutzung von *Reverse Tunneling* verschärft sich diese Problematik. Deshalb wurden für Mobile IP Erweiterungen zur Routenoptimierung [41] definiert.
Diese basieren darauf, den Kommunikationspartner über die COA zu informieren, so dass dieser sie in seiner lokalen Wegewahltabelle, dem *Binding Cache*, zwischenspeichern kann. Nun kann direkt mit dem Kommunikationsparter ein bidirektionaler IP-Tunnel aufgebaut werden. Problematisch ist hierbei, dass von diesen Erweiterungen der Kommunikationspartner direkt betroffen ist. Der Standard IPv4-Stack unterstützt kein IP-Tunneling. Auch ist fraglich, ob Mobile IP Teilnehmer bereit sind, ihre Aufenthaltsinformationen jedem potentiellen Kommunikationspartner preiszugeben.

Minimale IP-in-IP-Kapselung und GRE: Durch minimale IP-in-IP-Kapselung [28] lassen sich die redundanten Informationen aus den Paketköpfen des IP-Tunnels entfernen. Beide Seiten müssen minimale Kapselung als eigenen IP-Protokolltyp unterstützen.
Ein weiteres Protokoll, welches ein Verfahren zur Kapselung eines Protokolls als Nutzdaten eines anderen bietet, ist *Generic Routing Encapsulation* (GRE) [17]. Merkmale von GRE sind die Kapselung beliebiger Protokolle, die Möglichkeit, feste Routen einzurichten und ein Schlüsselfeld, welches zur Authentifizierung genutzt werden kann.

Mikromobilität: Mobile IP wurde für Makromobilität entwickelt, d.h. für gelegentliche Netzwechsel. Bei häufigen Handovervorgängen werden durch den zusätzlichen Overhead bei der Registrierung die Latenzzeiten zwischen dem Heimatnetz und den Fremdnetzen sehr hoch. Die hohen Latenzen könnten zu Unterbrechungen der Verbindungen auf der TCP-Protokollebene führen.
Lösen lässt sich dieses Problem durch den Aufbau einer hierarchischen Struktur, in der eine Anzahl von Fremdagenten von einem sogenannten *Gateway Foreign Agent* (GFA) verwaltet wird [43]. Bei der ersten Registrierung in dem Fremdnetz wird der *Gateway Foreign Agent* mit einbezogen. Alle weiteren Registrierungen, die in den Verwaltungsbereich des *Gateway Foreign Agent* fallen, werden zwischen dem Fremdagenten und ihm abgewickelt.

Mobile IP und IPv6: IPv6 erleichtert den Einsatz von Mobile IP erheblich [40]. Es sind keine neuen Services notwendig, und einiges fällt sogar weg.
So ermöglicht IPv6 *Neighbor Discovery*, wodurch ein Endgerät Services von Netznachbarn erfragen und anbieten kann. Dies macht den Einsatz von Agenten überflüssig. Innerhalb von IPv6 werden nur noch *Co-Located* COAs eingesetzt.
Routerseitig sieht IPv6 *Smooth Handover* vor. Ein Router, der *Smooth Handover* unterstützt, kann Pakete eines mobilen Teilnehmers eine gewisse Zeit zwischenspeichern und an eine

neue Adresse weiterleiten. Dies funktioniert allerdings nur, wenn der Handover erfolgt, bevor der Zwischenspeicher gefüllt ist.
Auch lässt es IPv6 zu, dass ein Endgerät mehrere *Co-Located* COAs besitzt und auf diese reagiert.

3.2.6 Sicherheit

Das von Mobile IP eingesetzte Authentifizierungsverfahren (MD5) garantiert lediglich, dass die Registrationsinformationen auf ihrem Weg nicht verändert werden können. Neben den IP-Adressen der Kommunikationspartner stehen auch die Inhalte der Registrierung potenziellen Angreifern zur Verfügung.
Desweiteren bestehen keine Möglichkeiten, die Vertraulichkeit der Kommunikationsinhalte und deren Integrität zu gewährleisten.
Mit VPN (Virtual Private Network) und IPSec stehen Verfahren zur Verfügung, mit denen sich alle drei Forderungen der Sicherheit erfüllen lassen.

VPN und IPSec: VPN-Mechanismen (Virtual Private Network) erlauben die Abbildung von sicheren LAN-Strukturen über nicht sichere Netze, wie beispielsweise das Internet. Virtuell deshalb, weil es sich dabei um eine übergeordnete, logische Struktur handelt, die auf das unsichere Netz aufsetzt.
Zwischen dem Heimatnetz und dem mobilen Endgerät wird ein Tunnel aufgebaut, durch den die Daten versendet werden. Die so vernetzten Systeme und die darauf laufenden Applikationen verhalten sich als ob es sich um eine physikalische Struktur handelt.
Die von VPN angebotenen LAN-Strukturen lassen sich auch auf drahtlose Netze anwenden.
Von VPN werden verschiedene Einsatzszenarien unterstützt: Die Koppelung von Netzwerk-zu-Netzwerk, von Client-zu-Netzwerk und von Endgerät-zu-Endgerät. Bei der Client-zu-Netzwerk Kommunikation greift der Client auf das Netzwerk zu, indem er mit einem VPN-*Gateway* eine temporäre, gesicherte Verbindung aufbaut. Von dem *Gateway* werden die Pakete an die Zielsysteme weitergeleitet. Auf das mobile Endgerät muss dazu eine entsprechende VPN-Software installiert werden.
Für gesicherte Verbindungen können verschiedene Tunneling-Protokolle zum Einsatz kommen. Hauptsächlich wird PPTP (Point-to-Point Tunneling Protocoll) und IPSec angewendet.
PPTP basiert auf dem *Point-to-Point* Protokoll (PPP). Dabei erstreckt sich die verschlüsselte Verbindung über das ganze Netz bis zu einem PPTP-Server. Durch PPTP lassen sich alle Vermittlungsprotokolle (Layer-3-Protokolle) transportieren. Die Sicherheitsmechanismen von PPTP gelten jedoch als mangelhaft.
IPSec [29] erweitert TCP/IP um zusätzliche Sicherheitsfunktionen. Dem Teilnehmer wird starke Authentifikation angeboten, indem sich jedes Paket mit einer Signatur versehen lässt. Diese ermöglicht es, die Identität des Senders und die Integrität der Nutzdaten zu gewährleisten. Es kommt dabei eine HMAC/MD5 Verschlüsselung zum Einsatz.
Die Nutzdaten lassen sich durch verschiedene Verschlüsselungsalgorithmen (DES, Triple-DES, Idea, Blowfish, Cast, RC5) sichern.

Für die Verhandlung der eingesetzten Authentifizierungs- und Verschlüsselungsmethoden, sowie für den Schlüsselaustausch steht ein eigenes Protokoll zur Verfügung.
Es lassen sich in IPSec zwei Transportmodi nutzen. Der Unterschied resultiert aus dem jeweiligen Einsatzszenario. Der Erste bietet eine Verschlüsselung und Authentifizierung der Nutzdaten und von Teilen des IP-Paketkopfes an. Mit dem Zweiten wird jedes Paket vollständig verschlüsselt und mit einem neuen IP-Header versehen. Die Versendung der Pakete erfolgt dann über spezielle IPSec-*Gateways*.
VPN unterstützt von sich aus kein Roaming. Bei einem Netzwechsel geht die Verbindung verloren und die Anwender werden zum erneuten Einloggen aufgefordert. Die Kombination von VPN mit Mobile IP bietet sich an, um Netzwechsel zu verbergen.
[62] [56] [1]

3.3 TCP/UDP in drahtlosen Umgebungen

Die Aufgabe der beiden Transportprotokolle TCP (Transport Control Protocol) und UDP (User Datagram Protocol) ist das Multiplexen und Demultiplexen von Datenströmen von und zu Anwendungen. Erst ab der Transportschicht können über Portadressen die Anwendungen direkt angesprochen werden.
Zusätzlich berechnen beide Protokolle eine Prüfsumme, um die Integrität der Daten zu überprüfen.
Der Unterschied zwischen TCP und UDP besteht darin, dass UDP einen verbindungslosen und TCP einen verbindungsorientierten Transportdienst anbietet. UDP bietet keinerlei Garantien für die Auslieferung der Daten, im Gegensatz zu TCP, das für einen zuverlässigen, garantierten Transport sorgt.
Beide Transportprotokolle sind grundsätzlich mediumunabhängig. Dennoch scheinen TCP und UDP bei drahtlosen Netzen sehr ineffizient. Beide Protokolle wurden nicht für die Anforderungen in mobilen, drahtlosen Netzen entworfen.
Das Problem bei UDP hängt mit den Programmen zusammen, die dieses Protokoll nutzen. Meistens erwarten die Applikationen, dass die genutzte Leitung sehr zuverlässig ist. UDP bietet keine Garantien für die Übertragung und ist deshalb auch wesentlich schneller als TCP. Für Programme, die sich verlorene Pakete auf der Applikationsebene wiederbesorgen müssen, ist dies mit beträchtlichem Aufwand verbunden. UDP ist hier nur dann sinnvoll, wenn Applikationen eingesetzt werden, die tatsächlich nicht auf den Empfang aller Pakete angewiesen sind.
Im Folgenden werden die problematischen Mechanismen innerhalb TCP und mögliche Lösungsansätze kurz vorgestellt.
TCP führt den Verlust einzelner Pakete auf temporäre Überlast des genutzten Transportweges zurück. Diese Annahme ist in drahtgebundenen Netzwerken im allgemeinen auch richtig. So reduziert TCP die Senderate der Übertragung, damit sich die Überlast abbauen kann.
Eine Überlast wird bei TCP durch die fehlende Bestätigung eines Paketes ausgelöst. Der *TCP-Timeout* wird bei Standard-TCP aus der *Round Trip Time* RTT_{Est} berechnet. Diese wird für jede Verbindung erneut festgestellt und dynamisch angepasst.

$$\textit{TCP-Timeout} = RTT_{Est} + 4 * Standardabweichung(RTT)$$

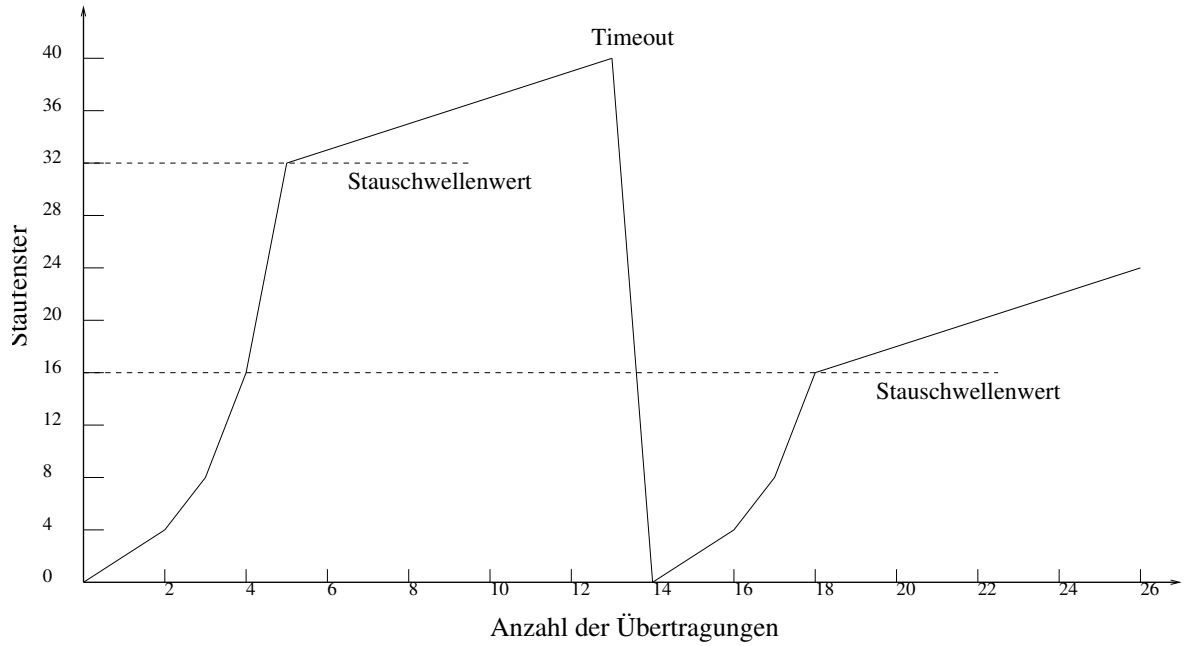


Abbildung 20: Beispiel des TCP-Slow-Start Algorithmus

Die Reduzierung der Übertragungsgeschwindigkeit wird durch einen *TCP-Slow-Start* herbeigeführt.
Bei einem *TCP-Slow-Start* versendet der Sender anfänglich ein Paket und wartet auf eine Bestätigung des Empfängers. Sobald diese Bestätigung eintrifft, inkrementiert der Sender sein Staufenster um eins und sendet dann zwei Pakete. Sobald beide Pakete bestätigt sind, wird das Staufenster für jede Bestätigung weiter um eins erhöht. Somit verdoppelt sich bei jeder fortlaufend erfolgreichen Übertragung das Staufenster bis zu einem vom System dynamisch angepassten Stauschwellenwert. Nach jedem Übertragungsfehler wird dieser auf die Hälfte des aktuellen Fenster gesetzt. Bei Erreichen des Stauschwellenwertes geht das exponentielle Wachstum des Staufensters in ein lineares über und erhöht den Wert in jeder Runde nur noch um eins. Dies geht solange weiter, bis aufgrund eines Übertragungsfehlers ein erneuter *TCP-Slow-Start* ausgelöst wird.
Abbildung 20 stellt dar, wie der Überlastalgorithmus funktioniert.
Die schnelle Übertragungswiederholung ist ein TCP-Mechanismus, um mit dem Verlust einzelner Pakete umzugehen. Es kann passieren, dass ein Sender nur noch Duplikatbestätigungen für dasselbe Paket erhält. Daraus schließt er, dass der Empfänger alle Pakete bis zum wiederholt bestätigten erfolgreich erhalten hat und immer noch Daten erhält. Der Sender nimmt nun einen kurzfristigen Stau an und überträgt die fehlenden Pakete ohne in den *TCP-Slow-Start*-Mode überzugehen.
Dieses Verfahren wird als *Fast Retransmit/Fast Recovery* bezeichnet.
Bei drahtlosen Netzwerken mit mobilen Sendern und Empfängern können hohe Paketverlustraten normal sein. TCP schließt immer wieder auf eine Stausituation und führt einen

TCP-Slow-Start durch. Dies führt hier jedoch zu einer weiteren Verschlechterung der Situation.
Auch können beispielsweise durch den Einsatz von Mobile IP erhöhte Latenzzeiten einzelner Pakete auftreten, die nicht schnell genug umgeleitet werden können. Durch *Fast Retransmit/Fast Recovery* werden dann diese Pakete verfrüht erneut übertragen und die meist schlechten drahtlosen Verbindungen werden zusätzlich durch überflüssige Kommunikation belastet.
TCP kann nicht zwischen unterschiedlichen Situationen in drahtgebundenen und drahtlosen Übertragungsmedien unterscheiden. Bei inhomogenen Übertragungswegen kann TCP überhaupt keine richtige Entscheidung treffen.
Ein weiteres Problem von Standard-TCP ist der Umgang mit längeren Verbindungsunterbrechungen, die durch Netzwechsel oder in Gebieten mangelhafter Netzabdeckung auftreten können. Der TCP-Sender versucht, die Daten wiederholt zu übertragen. Dabei verdoppelt er die Zeitspanne nach jedem erfolglosen Versuch bis zu maximal einer Minute. Nach zwölf Versuchen gibt TCP auf und beendet die Verbindung [54] [53].

Für TCP gibt es folgende Lösungsmöglichkeiten [49] [21]:

3.3.1 Indirektes TCP

Indirektes TCP (I-TCP) [2] sieht eine Aufteilung der Verbindung in einen drahtgebundenen und einen drahtlosen Anteil vor. Innerhalb des drahtgebundenen Anteils wird normales, unverändertes TCP eingesetzt. Zwischen dem mobilen Endgerät und der Empfangsstation kommt ein modifiziertes TCP zum Einsatz, in der eine hohe Paketverlustrate nicht als Überlast interpretiert wird.
Die Empfangsstation kopiert Pakete in beide Richtungen, so dass Verbindungen beidseitig homogen sind. Dies ist in Abbildung 21 skizziert.
Timeouts können nun im drahtgebundenen Anteil zu Verlangsamung der Übertragung führen, wie es in TCP vorgesehen ist. Im drahtlosen Teil der Verbindung führen *Timeouts* zu einer Beschleunigung der Übertragungsgeschwindigkeit. Durch dieses Verfahren wird allerdings die TCP-Semantik verletzt, so dass Empfangsbestätigungen nicht mehr bedeuten, dass der Empfänger das Paket erhalten hat.
Damit TCP den Wechsel einer Empfangsstation beziehungsweise eines Netzes verkraften kann, müssen vom alten Zugangspunkt bereits bestätigte Pakete zum neuen Zugangspunkt umgeleitet werden. Dies kann beispielsweise durch den Einsatz von Mobile IP mit angepassten Fremdagenten erfolgen. Außer dem Pufferinhalt müsste dann auch der aktuelle Status der TCP-Verbindung zu den neuen Fremdagenten übertragen werden.

3.3.2 Snooping TCP

Snooping TCP [3] (siehe Abbildung 22) besteht aus kleineren Anpassungen seitens der Vermittlungsschicht in den Empfangsstationen.

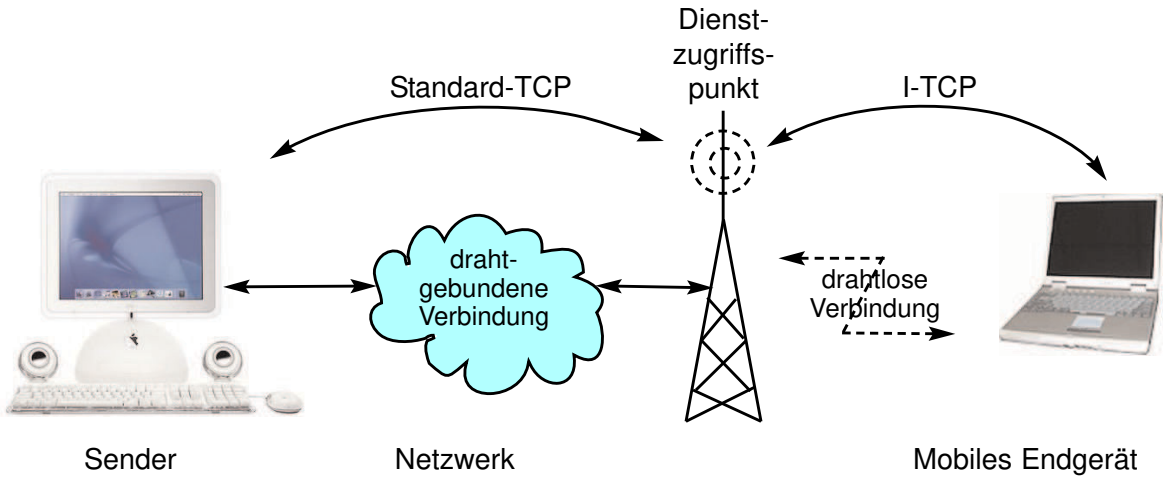


Abbildung 21: Indirektes TCP teilt eine TCP-Verbindung in zwei Teile auf

Ein Schnüffelagent (Snooping Agent) beobachtet den Paketfluß in beiden Richtungen, um Bestätigungsmeldungen zu erkennen. Duplikatbestätigungen des mobilen Endgerätes werden vom Agenten verworfen. Pakete mit dem Ziel des mobilen Endgerätes werden solange zwischengespeichert, bis diese bestätigt wurden.
Wird ein Paket innerhalb einer relativ kurzen Zeitspanne vom mobilen Endgerät nicht bestätigt oder treten Duplikatbestätigungen auf, überträgt der Agent das fehlende Paket direkt aus seinem Zwischenspeicher noch einmal.
Bei Paketen vom mobilen Endgerät in Richtung des Kommunikationspartners werden vom Agenten die Sequenznummern mitgelesen. Der Agent veranlasst bei fehlenden Paketen eine umgehende Neuübertragung.
Durch dieses Verfahren verkürzt sich die Zeit für eine erneute Übertragung um den drahtgebundenen Abschnitt. Dies senkt die Wahrscheinlichkeit, dass durch einen *TCP-Timeout* ein *TCP-Slow-Start* beim Sender ausgelöst wird.
Der Vorteil dieses Verfahrens im Vergleich zu I-TCP liegt in der Beibehaltung der Ende-zu-Ende-TCP-Verbindung. Bei sehr hohen Verlustraten auf dem drahtlosen Übertragungsweg lässt sich allerdings der *TCP-Timeout* des Senders nicht verhindern.
Auch hier kann die Funktion des Schnüffelagenten von einem modifizierten Mobile IP Fremdagenten übernommen werden.
Weitere Änderungen betreffen die Lösung für das Problem verlorener Segmente. Eine TCP-Option ermöglicht beispielsweise die Anfrage für eine selektive Wiederholung fehlender Bytes.

3.3.3 Mobile TCP

M-TCP [8] segmentiert eine TCP-Verbindung in ähnlicher Weise wie I-TCP, verzichtet jedoch auf die Zwischenspeicherung und Bestätigung von Paketen seitens des Agenten. Dadurch bleibt die Ende-zu-Ende Semantik von TCP erhalten.

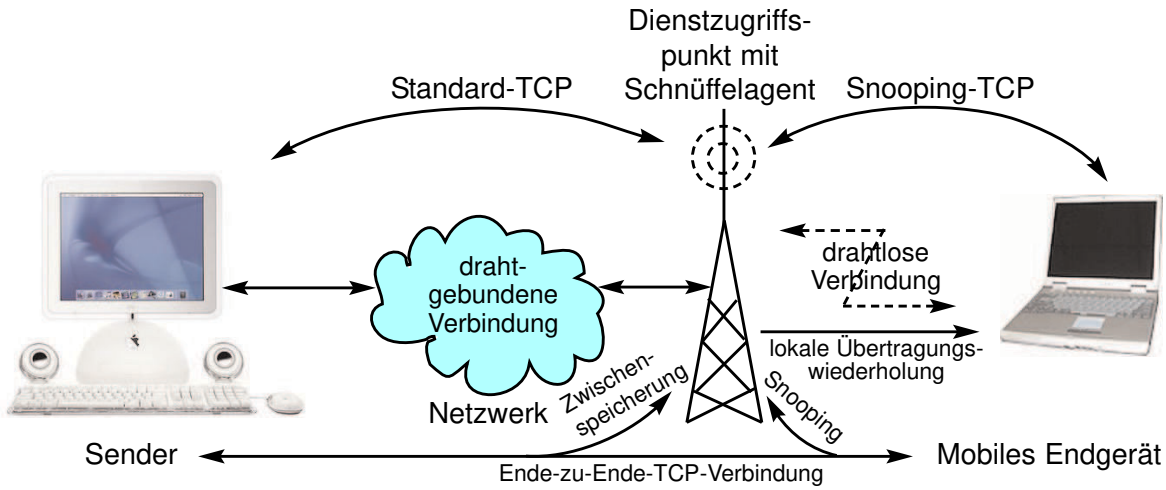


Abbildung 22: Snooping TCP teilt eine TCP-Verbindung bei Beibehaltung der TCP-Semantik in zwei Teile auf

Der Agent beobachtet alle Pakete, die zum mobilen Endgerät übertragen werden. Bleiben die Bestätigungsmeldungen aus, so geht der Agent davon aus, dass eine Verbindungsunterbrechnung zum mobilen Endgerät vorliegt. Der Agent setzt dann die *TCP-Windowsize* des Senders auf Null.
Die *TCP-Windowsize* bestimmt die Anzahl der Bytes, die ein Sender abschicken darf, bevor eine Bestätigung vom Empfänger erwartet wird. Durch sie erfolgt die Flußsteuerung. Wird sie künstlich auf Null gesetzt, wechselt der betroffene Sender in den sogenannten *persistenten Modus*. In diesem verändert sich der Zustand der TCP-Verbindung nicht.
Sobald der Agent realisiert, dass die Verbindung wiederhergestellt ist, setzt er die *TCP-Windowsize* wieder auf den alten Wert. Da seitens des Agenten auf eine Zwischenspeicherung verzichtet wird, kann es sich bei einem Verbindungswechsel durchaus um einen neuen Agenten handeln.
Das über die drahtlose Verbindung eingesetzte angepasste TCP kann sich wesentlich schneller von Paketverlusten erholen, da es keinen *TCP-Slow-Start* einsetzt.

3.3.4 Optimierungen

Fast Retransmit/Fast Recovery: Eine anderes Verfahren [9] sieht vor, dass das mobile Endgerät bei einem Verbindungswechsel sofort in den schnellen Übertragungsmodus *Fast Retransmit/Fast Recovery* wechselt.
Dazu schickt das mobile Endgerät drei Duplikatbestätigungen an den Kommunikationspartner und sendet umgehend alle noch unbestätigten Pakete. Dies veranlasst den Sender, ebenfalls in diesen Modus zu wechseln.
Das vermeidet beidseitig den *TCP-Slow-Start* und die Übertragung wird mit der zum Zeitpunkt der Verbindungsunterbrechung genutzten Übertragungsrate fortgesetzt.

Selektive Übertragungswiederholung: Bei Standard-TCP müssen bei Verlust eines einzelnen Paketes alle Folgepakete erneut übertragen werden. Durch die TCP-Erweiterung der selektiven Übertragungswiederholung [55] lassen sich einzelne Pakete gezielt erneut anfordern. Viele aktuelle TCP-Implementierungen unterstützen die selektive Übertragungswiederholung.
[21]

3.4 Zusammenfassung und Auswertung

Das IP-Protokoll wurde kurz vorgestellt und bezogen auf seine Mobilitätsunterstützung hin untersucht. Auch die naheliegenden Lösungsmöglichkeiten DHCP und die manuelle Anpassung der IP-Routen wurden gestreift. Schließlich wurde die mobilitätsunterstützende Protokollerweiterung Mobile IP vorgestellt.
Durch Mobile IP steht dem IP-Protokoll eine Erweiterung zur Verfügung, die Endgerätemobilität erlaubt, ohne dass Veränderungen an existierenden Systemen notwendig sind. Mobile IP lässt jedoch viele Probleme offen. Es bestehen Sicherheitsprobleme, die Paketweiterleitung ist ineffizient und die fehlenden Möglichkeiten der Dienstgüteunterstützung.
Es wurden Lösungsmöglichkeiten vorgestellt, die sich der Sicherheitsproblematik annehmen. Durch VPN mit IPSec lässt sich dies auf Applikationsebene lösen.
Anschließend wurde auf das Verhalten der Transportprotokolle TCP und UDP in drahtlosen Umgebungen eingegangen.
Das Transportprotokoll TCP besitzt schwerwiegende Effizienzprobleme in drahtloser Umgebung. Es geht, sobald Empfangsbestätigungen ausbleiben, von einer Stausituation aus. Diese Annahme ist bei drahtlosen Verbindungen meist falsch, da hier schwankende Bandbreiten und Latenzen, sowie fehleranfällige, asymmetrische Verbindungen und Verbindungsabbrüche üblich sind.
Es wurden anschließend die Lösungsansätze I-TCP, S-TCP, M-TCP und die Optimierungsmöglichkeiten *Fast Retransmit/Fast Recovery* und selektive Übertragungswiederholung vorgestellt. Hierbei lassen sich die Lösungsansätzen mit den Optimierungsmöglichkeiten kombinieren.
In Tabelle 11 sind die vorgestellten TCP-Modifikationen für drahtlose Verbindungen zusammenfassend mit ihren Vor- und Nachteilen dargestellt.

Verfahren	Mechanismus	Vorteile	Nachteile
Indirect-TCP	Auftrennen in zwei TCP-Verbindungen	Isolation der Teilstrecke, einfach	Verlust der TCP-Semantik
Snooping TCP	Mithören von Daten und Quittungen	Beibehaltung der TCP-Semantik	erfordert gute Verbindungsqualität
Mobile-TCP	Einfrieren der TCP-Verbindung	Beibehaltung der TCP-Semantik	erfordert gute Verbindungsqualität
Fast Retransmit/ Fast Recovery	Vermeidung des *TCP-Slow-Start*	einfach und effizient	erhöht die Netzlast
Selektive Übertragungs-wiederholung	gezielte Wiederholung verlorengegangener Pakete	sehr effizient, bereits vielfach Implementiert	erhöhter TCP-Speicherbedarf

Tabelle 11: Vergleich verschiedener TCP-Modifikationen für drahtlose Verbindungen

4 Folgerungen für das Nomadic Computing

Die Mobilfunknetze und die drahtlosen Rechnernetze unterscheiden sich zum Teil evolutionsbedingt erheblich. Für den Einsatz beim Nomadic Computing erweisen sich das unterschiedliche Mobilitätsmanagment und die Sicherheitsmängel als wesentliche Probleme. Mit einer netzseitigen Annäherung ist frühestens im Anschluss an die dritte Mobilfunkgeneration zu rechnen.
Durch Mobile IP ist es möglich, Roaming zwischen beliebigen Kommunikationsnetzen zu realisieren. Es ist dabei unerheblich, ob die zu nutzenden Netze über eine Mobilitätsunterstützung verfügen oder nicht. Einzige Voraussetzung ist der Zugang zu einem IP-Netzwerk, welches die Funktion eines *Backbones* erfüllen kann. Dabei kann es sich beispielsweise um das Internet handeln. Über dieses IP-Netzwerk müssen alle potentiellen Kommunikationsteilnehmer erreichbar sein. Es bestehen auch hier erhebliche Sicherheitsmängel, die sich nur auf Applikationsebene vollständig beseitigen lassen.
Es entstehen zusätzliche Probleme seitens der Transportebene und des dort eingesetzten TCP-Protokolls. Wie gezeigt wurde, gibt es verschiedene Lösungsmöglichkeiten.

Was ist heute möglich? Mobile Endgeräte lassen sich zur Zeit in Laptops, Subnotebooks, Handhelds und Mobiltelefone einteilen. Die Integration drahtloser Kommunikationstechnik ist noch nicht Standard, setzt sich allerdings langsam in Geräten der oberen Preissegmente durch. Zur Zeit ist es möglich, durch die Verbindung eines mobilen Rechners mit einem Mobiltelefon durch eine PAN-Brücke die Mobilfunknetze zu nutzen.
Es sind für fast alle Mobilfunknetze mobile Endgeräte vorhanden, die die unterschiedlichen Kommunikationstechnologien unterstützen. Auch die Nutzung von Satellitentechnologie ist bereits möglich, jedoch noch mit erheblichen Nutzungskosten verbunden.
Drahtlose LANs und PANs sind für die meisten in Nutzung befindlichen mobilen Endgeräte bestenfalls eine Option. Auch werden meist nicht mehr als maximal zwei unterschiedliche drahtlose Übertragungstechnologien unterstützt. Lösungen, die einen großen Teil vorhandener Übertragungsstandards nutzen können, sind leider nicht vorhanden. Es gibt allerdings erste Geräte, die sowohl drahtlose LAN (IEEE 802.11b) als auch PAN Technologie (Bluetooth) fest integriert haben.
Bei Mobile IP handelt es sich noch nicht um Standardtechnologie. Es stehen allerdings properitäre Lösungen zur Verfügung. Für die TCP-Problematik gibt es momentan lediglich die vorgestellten Lösungsansätze. Hier ist kein einheitlicher Standard vorhanden. Das bei Mobiltelefonen eingesetzte WAP (Wireless Applikation Protocol) löst dieses Problem beispielsweise durch den Einsatz eines eigenen Transportprotokolls (Wireless Transport Protocol, WTP).
VPN mit IPSec ist eine verbreitete Lösung, die in einigen Systemen sogar teilweise bereits fest im System integriert wurde. Auch systemübergreifende Lösungen sind verfügbar.

Was ist mittel/langfristig möglich? Laptops und Subnotebooks werden mit hoher Wahrscheinlichkeit zu einer neuen Geräteklasse zusammenfließen. Diese Geräte werden kleiner und leichter als heutige Laptops sein allerdings im Gegesatz zu heutigen Subnotebooks die

Leistungfähigkeit eines vollwertigen Arbeitsplatzes besitzen. Diese Geräte werden standardmäßig unterschiedliche WLAN- und WPAN-Standards unterstützen.
Handheld Computer und Mobiltelefone werden zu sehr kleinen und sehr leichten Endgeräten verschmelzen. Mit ihnen lässt sich „unterwegs“ arbeiten. Diese Geräte werden viele Mobilfunkstandards sowie WPAN und WLAN-Technologie unterstützen. Die Verbindung der unterschiedlichen Gerätetypen erfolgt über WPAN-Technologie. Sie werden zusammen mit anderen tragbaren Endgeräten die nomadische Umgebung bilden.
Die drahtlose Kommunikationstechnik wird als Standardtechnologie in diverse Geräte einfließen. Durch Software-Radio und durch adaptive Antennen können sich Geräte im gewissen Rahmen auch neuen Übertragungstechnologien anpassen. Dabei handelt es sich um durch Software konfigurierbare Hardware und umschaltbare Filter. Adaptive Antennen ermöglichen durch gezielte Ausrichtung zwischen Kommunikationspartnern eine wesentlich effizientere Nutzung der Zellen als bisher.
Die protokollseitige Unterstützung von Mobilität und drahtlosen Kommunikationswegen, beziehungsweise Teilstrecken, wird zwingend sein. Dabei ist damit zu rechnen, dass sich Mobile IP spätestens mit der Einführung von IPv6 durchsetzen wird. Bei TCP wird eine, beziehungsweise eine Kombination, der vorgestellten Lösungen eingesetzt werden. Meines Erachtens besitzen Snooping TCP und Mobile TCP hierfür die besten Voraussetzungen, da die Ende-zu-Ende TCP Semantik erhalten bleibt.
Es ist damit zu rechnen, dass sich VPN-Lösungen mit IPSec als Standardtechnologie für sichere Verbindungen über unsichere Netze durchsetzen werden. Durch IPv6 werden auch neue Authentifizierungs und Verschlüsselungsverfahren zur Verfügung stehen.

A Erklärungen

A.1 Selbstständigkeitserklärung

Hiermit erkläre ich, dass ich die vorliegende Arbeit selbstständig und nur unter Nutzung der angegebenen Literatur und Hilfsmittel angefertigt habe.

Berlin, den 02. Mai 2002 Ralf Staudemeyer

A.2 Einverständniserklärung

Ich erkläre mich damit einverstanden, dass diese Arbeit öffentlich in der Universitätsbibliothek ausgestellt wird.

Berlin, den 02. Mai 2002 Ralf Staudemeyer

B Literatur

Literatur

[1] Daniel Bachfeld. *Sicheres Netz im Netz*, Heise Verlag, c't 17/2001, S.164

[2] A. Bakre, B.R. Badrinath. *I-TCP: Indirect TCP for Mobile Hosts*, Department of Computer Science, Rutgers University, Piscataway, NJ 08855, Oktober 1994

[3] H. Balakrishnan, S. Seshan, R. Katz. *Improving Reliable Transport and Handoff Performance in Cellular Wireless Networks*, ACM Mobile Computing and Networking Conference (Mobicom95), ACM, pp. 2-11, Dezember 1995

[4] Pravin Bhagwat. *Bluetooth: Technologie for Short-Range Wireless Apps*, IEEE Internet Computing, Mai/June 2001, S.96

[5] Keith Biesecker. *The Promise of Broadband Wireless*, IEEE IT Pro, November/December 2000, S.31

[6] Bluetooth SIG. *Specification of the Bluetooth System - Core*

[7] Bluetooth SIG. *Specification of the Bluetooth System - Profiles*

[8] Kevin Brown, Suresh Singh. *M-TCP: TCP for Mobile Cellular Networks* Department of Computer Science, Univercity of South Carolina, Columbia, SC 29205, July 1997

[9] Ramon Caceres, Liviu Iftode. *Improving Performance of Reliable Transport Protocols in Mobile Computing Environments* IEEE Journal on Selected Areas in Communications (JSAC), Special Issue on Mobile Networks, 1994

[10] R. Droms. *Dynamic Host Configuration Protocol*, Request for Comments, 2131, Internet Engineering Task Force, März 1997

[11] Hannes Federrath. *Sicherheit mobiler Kommunikation, Schutz in GSM-Netzen, Mobilitätsmanagment und mehrseitige Sicherheit*, Vieweg, Braunschweig/Wiesbaden, 1999

[12] Frank Fitzek, James Gross, Andreas Köpsel. *Kurzstrecken-Sprinter - Einblicke in die Technik neuer WLANs*, heise Verlag, c't 26/2001, S.214

[13] Federal office for communications. *Faktenblatt GSM*, Federal office for communications, Mai 2001

[14] Stefan Gneiting. *Mehr Datenrate im Funknetz*, Funkschau, 19/2001, S.40-42

[15] Stefan Gneiting. *HiperLAN2 für drahtlose Zugangsnetze*, Funkschau, 23/2001, S.35-37

[16] Alexandra Götz. *UMTS-Systemtechnik im Detail*, Funkschau, 10/2001, S.50

[17] S. Hanks, T. Li, P. Traina. *Generic Routing Encapsulation (GRE)* Request for Comments, 1701, Internet Engineering Task Force, Oktober 1994

[18] Jaap Haartsen. *Die Bluetooth-übertragung*, Funkschau, 15/1999, S.76

[19] Uwe Hansmann, Lothar Merk, Martin S.Nicklous, Thomas Stober. *Pervasive Computing Handbook*, Springer, Germany, 2000

[20] Martin Johnsson. *HiperLAN2 - The Broadband Radio Transmission Technology Operating in the 5 GHz Frequency Band*

[21] G. Huston. *TCP in a Wireless World*, IEEE Internet Computing, March/April 2001, S.82

[22] S. Deering. *ICMP Router Discovery Messages*, Request for Comments, 1256, Internet Engineering Task Force, September 1991

[23] IrDA-Specifications. *IrDA Serial Infrared Data Link Standard Specifications*

[24] IEEE Std 802.11, 1999 Edition. *IEEE Standard for Information Technology - Telecommunications and Information Exchange between Systems - Local and Metropolitan Area Network - Specific Requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*,

[25] IEEE 802.11a-1999, *Information technology Telecommunications and information exchange between systems Local and metropolitan area networks Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications Amendment 1: High-speed Physical Layer in the 5 GHz band*

[26] IEEE 802.11b-1999, *Supplement to 802.11-1999,Wireless LAN MAC and PHY specifications: Higher speed Physical Layer (PHY) extension in the 2.4 GHz band*

[27] C. Perkins. *IP Encapsulation within IP* Request for Comments, 2003, Internet Engineering Task Force, Oktober 1996

[28] C. Perkins. *Minimal IP Encapsulation within IP* Request for Comments, 2004, Internet Engineering Task Force, Oktober 1996

[29] S. Kent, R. Atkinson. *Security Architecture for the Internet Protocol* Request for Comments, 2401, Internet Engineering Task Force, November 1998

[30] Gerhard Kafka. *Neue Standards für das WLAN*, funkschau, November 2001, S.43

[31] Olaf Kirch, Terry Dawson. *Linux Network Administrators Guide*, O´Reilly, 2nd Eddition, 2000

[32] Rene Kriedemann. *Standards für kabellose Netzwerke der Zukunft*, LANline, 08/2001, S.114ff

[33] David G. Leeper. *A Long Time View of Short-Range Wireless*, IEEE Computer, June 2001, S.39

[34] Rudolf Mäusl. *Digitale Modulationsverfahren*, Hüthig, Heidelberg/Germany, 1988

[35] Roger B. Marks, Ian C. Gifford, Bob O'Hara. *Standards in IEEE802 - Unleash the Wireless Internet*, microwave, June 2001, S.47

[36] H. Krawczyk, M. Bellare, R. Canetti. *HMAC: Keyed-Hashing for Message Authentication* Request for Comments, 2104, Internet Engineering Task Force, Februar 1997

[37] H. Meinke, F.W. Grundlach. *Taschenbuch der Hochfrequenztechnik*, Springer Verlag, Berlin/Heidelberg/New York, 1968

[38] Sandra Kay Miller. *Facing the Challange of Wireless Security*, IEEE Computer, July 2001

[39] C. Perkins. *IP Mobility Support for IPv4 (revised)* Internet Draft, IP Mobility Support for IPv4 (revised), Internet Engineering Task Force, September 2001

[40] David B. Johnson, C. Perkins. *Mobility Support for IPv6* Internet Draft, IP Mobility Support in IPv6, Internet Engineering Task Force, July 2001

[41] C. Perkins. *Route Optimization in Mobile IP* Internet Draft, Route Optimization in Mobile IP, Internet Engineering Task Force, September 2001

[42] C. Perkins. *IP Mobility Support* Request for Comments, 2002, Internet Engineering Task Force, Oktober 1996

[43] Eva Gustafsson, Annika Jonsson, Charles E. Perkins. *Mobile IPv4 Regional Registration* Internet Draft, Mobile IPv4 Regional Registration, Internet Engineering Task Force, September 2001

[44] Dr. Dirk Nikolai, Klaus Daniel, Dr. Edgar Kühn. *Turbolader für Funk-Bits*, Heise Verlag, c't 19/2000, S.190

[45] Linda Dailey Paulson. *Exploring the Wireless LANscape*, IEEE Computer, Oktober 2000, S.12

[46] Christian Rauch. *Zukunft von 3G*, Funkschau, 12/2001, S.18-20

[47] G. Montenegro. *Reverse Tunneling for Mobile IP, revised* Request for Comments, 3024, Internet Engineering Task Force, Januar 2001

[48] Tristan Richardson, Quentin Stafford-Fraser, Kenneth R. Wood, Andy Hopper. *Virtual Network Computing*, IEEE Computer, Jan/Feb 1998

[49] Jochen Schiller. *Mobilkommunikation, Techniken für das allgegenwärtige Internet*, Addison Wesley, München/Germany, 2000

[50] Charles Severance. *IEEE802.11: Wireless Is Coming Home*, IEEE Computer, November 1999, S.126

[51] Richard Sietmann. *Quo Vadis, Mobilfunk?*, Heise Verlag, c't 05/2001, S.94

[52] William Stallings. *IEEE 802.11: Moving Closer to Practical Wireless LANs*, IEEE IT Pro, May/June 2001, S.17

[53] Andrew. S. Tanenbaum. *Computernetzwerke*, Prentice Hall, München/Germany, 1998

[54] W. Stevens. *TCP Slow Start, Congestion Avoidance, Fast Retransmit and Fast Recovery Algorithms, TCP Selective Acknowledgment Options* Request for Comments, 2001, Internet Engineering Task Force, January 1997

[55] M. Mathis, J. Mahdavi, S. Floyd, A. Romanow. *TCP Selective Acknowledgment Options* Request for Comments, 2018, Internet Engineering Task Force, October 1996

[56] Mark Thorne. *Sicherheit in drahtlosen Netzen*, Funkschau, 18/2002, S.36

[57] Upkar Varshney. *Recent Advances in Wireless Networking*, Computer, June 2000, S.100-103

[58] Upkar Varshney, Ronald J. Vetter, Ravi Kalakota. *Mobile Commerce: A New Frontier*, Computer, Oktober 2000, S.32-38

[59] Bernhard Walke. *Mobilfunknetze und ihre Protokolle 1*, B.G.Teubner, Stuttgart/Leipzig/Wiesbaden, 09/2001

[60] Bernhard Walke. *Mobilfunknetze und ihre Protokolle 2*, B.G.Teubner, Stuttgart/Leipzig/Wiesbaden, 11/2001

[61] Oliver Weissmann, Christoph Ruland. *Sicherheit bei Bluetooth*, Funkschau, 10/2001, S.43

[62] Roger Younglove. *Virtual Private Networks - Secure Access for E-Business*, IEEE Computer, July/August 200, S.96

[63] Dusan Zivadinovic. *Drahtlos anknüpfen, GPRS: schneller mobil surfen*, Heise Verlag, c't 7/1999, S.186

[64] Dusan Zivadinovic. *Wellensalat satt, Daten-Mobilfunk holt Modems ein*, Heise Verlag, c't 2/2000, S.166

[65] Dusan Zivadinovic. *Surf-Tempo mit HSCSD, Handys mit schneller Datenübertragung*, Heise Verlag, c't 13/2000, S.42

[66] Dusan Zivadinovic. *Pakete per Funk, Mobilfunk und Internet verheiratet*, Heise Verlag, c't 21/2000, S.152