Grundlagen: Rechnernetze und Verteilte Systeme

Kapitel 1:
Einführung und Motivation

Trends, Internet, Nutzer, Leitbeispiel, Literatur

Prof. Dr.-Ing. Georg Carle
Lehrstuhl für Netzarchitekturen und Netzdienste
Technische Universität München
carle@net.in.tum.de
http://www.net.in.tum.de

Georg Carle

- Studium Elektrotechnik, Universität Stuttgart
- Master of Science in Digital Systems, Brunel University, London, U.K. (Master Thesis bei General Electric Corporation, Hirst Research Centre, London)
- Projekt bei Telecom Paris - Ecole Nationale Supérieure des Télécommunications (ENST), Paris
- Promotion in Informatik an der Universität Karlsruhe, am Institut für Telematik; Stipendium im Graduiertenkolleg 'Beherrschbarkeit komplexer Systeme'
- Postdoktorand am Institut Eurecom, Sophia Antipolis, France
- Fraunhofer Institut FOKUS (GMD FOKUS), Berlin
  Leiter des Competence Center Global Networking
- Universität Tübingen, Lehrstuhl für Rechnernetze und Internet
- Seit 1. April 2008: Lehrstuhl für Netzarchitekturen und Netzdienste, TU München

Vorlesungsorganisation

- Vorlesung
  - Mittwochs 14:15-15:45 Uhr, MW 2001
  - Donnerstags 8:30-10:00 Uhr, MI HS 1
  - 3SWS Vorlesung ⇒ Genauer Plan der Vorlesung auf Webseite (voraussichtlich ab 14. Mai Donnerstags alle zwei Wochen keine Vorlesung)
- Übung
  - Anmeldung über Grundstudiumstool (ab Do 12 Uhr möglich)
  - Übungsgruppenorganisation durch Herrn Marc-Oliver Pahl <pahl@net.in.tum.de>
- Fragen / Sprechstunde
  - Prof. Dr.-Ing. Georg Carle
    - Nach der Vorlesung
    - Sprechstunde: Zunächst Donnerstag 11-12 Uhr Raum 03.05.054 nach Voranmeldung, bzw. nach Vereinbarung
  - Dipl.-Inform. Marc-Oliver Pahl; Dipl.-Ing. Gerhard Münz
  - E-mail-Liste für Fragen: rnvs@net.in.tum.de
- Aktuelles
  - Wird auf der Vorlesungs-Webseite bekanntgegeben: http://www.net.in.tum.de/de/lehre/ss09/vorlesungen/vorlesung-rechnernetze-und-verteilte-systeme/
- Handouts
  - Die Folien können von der Vorlesungswebseite heruntergeladen werden

Übungsleitung

Gerhard Münz
muenz@net.in.tum.de

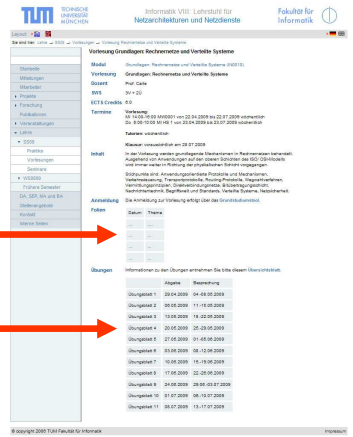
Marc-Oliver Pahl
pahl@net.in.tum.de

Übung

- **Nehmen Sie an der Übung Teil!**
  Ohne Übung werden Sie deutlich weniger von der Vorlesung mitnehmen.
- **Wöchentlich** ein Übungsblatt.
  http://www.net.in.tum.de/de/lehre/ss09/vorlesungen/vorlesung-rechnernetze-und-verteilte-systeme/
- Eine Woche Bearbeitungszeit.
- **Abgabe** jeweils am **Mittwoch vor** der **Vorlesung** in die entsprechend bereitgestellten Mappen.
- **Keine elektronischen Abgaben.**

Vorlesungswebsite

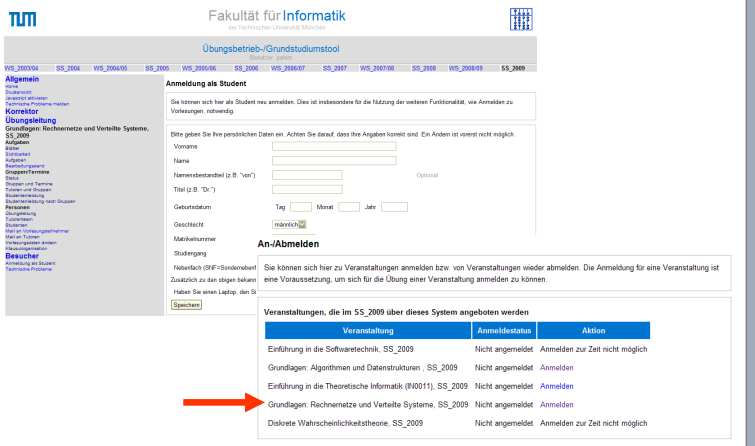
- http://www.net.in.tum.de/de/lehre/ss09/vorlesungen/vorlesung-rechnernetze-und-verteilte-systeme/



- Vorlesungsfolien
- Übungsblätter

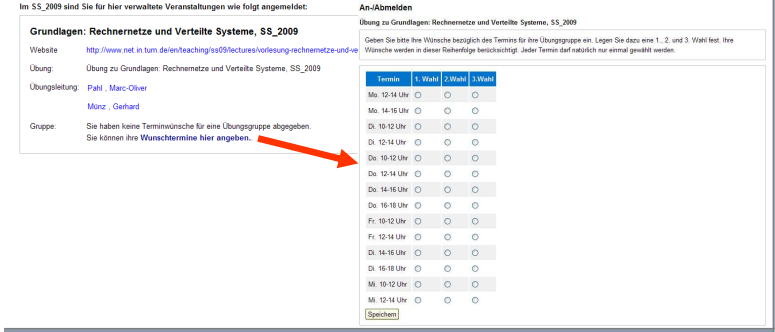
Anmeldung zur Vorlesung

- **http://grundstudium.in.tum.de**



Übungsanmeldung

- Übungsanmeldung ab Donnerstag, **22.4.2009, 12:00 Uhr**



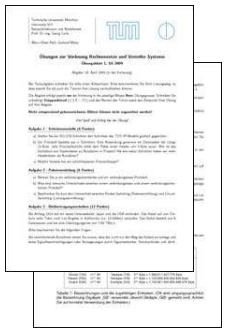
Übungsmodalitäten (Bonus)

- Bei erfolgreicher Teilnahme an den Übungen erhalten Sie bei *bestandener* Klausur einen **Notenbonus von 0,3 Notenpunkten** bei der Scheinklausur. Ihre Übungen gelten als erfolgreich bestanden, wenn Sie
  - in den Tutorien anwesend waren (**Anwesenheitsliste**).
  - mindestens eine Aufgabe richtig **an der Tafel vorgerechnet** haben
    - Sie können sich dazu freiwillig in der Übung melden. Sollte sich niemand bereit finden, vorzurechnen, so sind die Tutoren angehalten, jemanden auszuwählen. Sehen Sie das Vorrechnen als gute Übung für sich, etwas zu präsentieren!
  - mindestens **70% der möglichen Übungspunkte** erreicht haben.
  - das **letzte Blatt** abgegeben haben.

Nächste Schritte…

Teamarbeit in **Zwei**erteams ist **erwünscht und empfohlen!**

- Teampartner suchen
- Mit der Bearbeitung von Blatt 1 beginnen. Dieses…



- …befindet sich auf der Website
- …erfordert ggf. ein wenig Nachlesen in der angegebenen Literatur oder im Web.
- …ist abzugeben am 29.4.2009 vor der Vorlesung physikalisch nicht elektronisch.
- …wird besprochen in den ersten Tutorien in der Woche vom 4.5.-8.5.2009.

Abschlussklausur

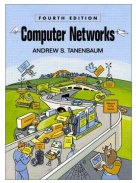
- Findet statt am **28.7.2009** (= erste Woche der vorlesungsfreien Zeit) genaueres wird bekannt gegeben, sobald wir es wissen.
- Die Tutorien in der Woche vom 20. bis zum 24.07.2009 sind speziell dafür da, eventuell beim Lernen aufgekommene Fragen noch vor der Klausur zu klären.
- Nutzen Sie die **Tutorien**, um neben der Übungsblattbesprechung eventuelle **Fragen zu Vorlesungsinhalten** mit Ihrem Tutor und Ihren Kommilitonen zu klären.
- Bei Fragen, die sich auf diese Weise nicht klären lassen, erreichen Sie die Vorlesungsverantwortlichen unter der Sammeladresse **rnvs@net.in.tum.de**

Acknowledgements

- Die vorliegenden Unterlagen sind im Laufe mehrerer Vorlesungen an den Universitäten Karlsruhe (Prof. Krüger, Prof. Juling, Prof. Zitterbart), Kiel (Prof. Schiller), Braunschweig (Prof. Zitterbart), FU Berlin (Prof. Schiller), Bern (Prof. Braun) entstanden. Zusätzliche Inhalte stammen von Vorlesungen an der Universität Paderborn (Prof. Karl), der Kansas University (Prof. Sterbenz) und der Universität Tübingen (Prof. Küchlin).
  Die Vorlesungsunterlagen beinhalten auch Material diverser Firmenveröffentlichungen, Internet-Quellen etc. Zahlreiche Autoren haben hierzu beigetragen, welche im Einzelnen gar nicht mehr alle genannt werden können. Daher ohne Namensnennung ein großer Dank an alle, die im Laufe der Jahre etwas zu diesen Folien beigetragen haben!
- Bei Fragen, Anregungen, Kommentaren zu diesen Folien bitte eine Email an carle@net.in.tum.de !

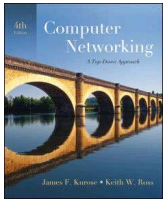
Grundlegende Bücher für diese Vorlesung

- Andrew S. Tanenbaum:
  - *Computer Networks*
    Prentice-Hall, **4th edition** 2003
    ISBN-10: 0130661023, 80 €
  - (Wurde - nicht fehlerfrei und z.T. eher schwer lesbar - auch ins Deutsche übersetzt:
    Computernetzwerke,
    Pearson Studium; 50 €, 4. Auflage 2003
    ISBN-10: 3827370469)
- Gerhard Krüger & Dietrich Reschke:
  - *Lehr- und Übungsbuch Telematik* Fachbuchverlag Leipzig im Carl-Hanser-Verlag, 3. Auflage, 2004
    ISBN 3-446-22073-9, < 30 €
  - gute Erläuterung von Teilen der Vorlesung
- Sebastian Abeck, Peter Lockemann, Jochen Seitz, Jochen Schiller
  - *Verteilte Informationssysteme*
    dpunkt.verlag, 2002
    ISBN 978-3-89864-188-3, 49 €
  - Stellt eine leicht zu lesende Erläuterung von Teilen der Vorlesung zur Verfügung

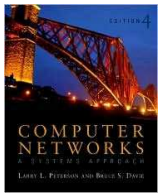



Weitere empfehlenswerte Bücher

- J. F. Kurose & K. W. Ross, *Computer Networking: A Top-Down Approach Featuring the Internet*, 2007, 4th edition, Addison Wesley
  - Innovation: Erläuterung der Protokolle Top-Down, beginnend mit der Anwendungsebene
  - Vorstellung von Schlüsselpersonen auf dem Gebiet Rechnernetze
  - **Deutsche Übersetzung: Computernetzwerke: Der Top-Down-Ansatz, Pearson Studium; 30/60 €, 4. Auflage 2008 ISBN-10: 3827373301**

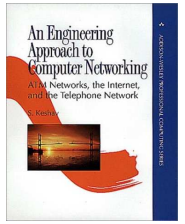


- L. L. Peterson & B. S. Davie, *Computer Networks – A Systems Approach*, 2007, 4th edition, Morgan Kaufman
  - Technisch und fundiert
  - Zahlreiche Beispiele

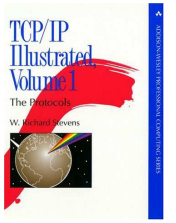


Weitere Buchempfehlungen

- S. Keshav: *An Engineering Approach to Computer Networking*. Addison-Wesley, 1999
  - Sehr gute quantitative Behandlung von Rechnernetzen
  - Erläutert zahreiche Entwurfsentscheidungen



- W.R. Stevens: *TCP/IP Illustrated, Vol. 1- 3,* 1994, Addison-Wesley
  - Erläutert sehr detailliert die Implementierung von TCP/IP



Übersicht

Entwurfsprinzipien für Telekommunikationssysteme (Schalttechnik leicht gemacht, Beispiel Beirut)

Ziel: transparente Kabelführung gemäß Struktur des Netzes

Schalttechnik leicht gemacht, Beispiel Beirut

Ziele:

- Präzise Dokumentation an jeder Leitung, um schnellen Zugriff auf jeden Anschluss zu gewährleisten.
- Bauweise des Gehäuses schütz Technik und verhindert Manipulation.

Schalttechnik leicht gemacht, Beispiel Beirut

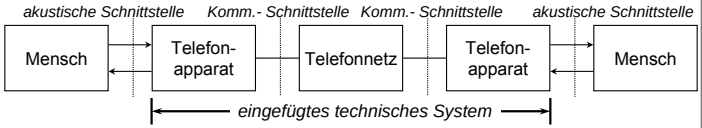
Ziel: straffe Schaltdraht-führung und Übersichtlichkeit erleichtert Reparaturen.

Historie: Kommunikationstechnologien

Jahr	*Innovation*	*Leistung*
1840	Morse-Telegraf	Elektronischer Nachrichtenaustausch über größere Distanzen
1861	Telefon (Reiss)	Sprachkommunikation (unidirektional) über über größere Distanzen
1876	Telefon (Bell)	Patentierung des Telefons (bidiektional)
1887	elektromagn. Wellen	Funktechnik
1892	Automatischer Drehwähler	Automatisierung der Telefonvermittlung (→ Ablösung des "Fräuleins vom Amt")
1923	Rundfunk	Massenkommunikation
1929	Koaxialkabel	Höhere Datenraten
1964	Nachrichtensatelliten	Grundlage für globale Kommunikation
1966	Glasfaser	extreme Steigerung der Datenraten
1969	ARPANET Knoten	Paketvermittlung
1973	Ethernet	Lokale Netze mit hohen Datenraten
1984	Deregulierung (*USA*)	Aufhebung des Fernmeldemonopols
1990	WWW	Architektur und Protokoll für Hypertext-Anwendung
1997	WDM (*Wavelength Division Multiplex*)	Steigerung der Datenraten auf Glasfaserstrecken auf bis zu 1 Terabit/s (Tera = 10^{12})

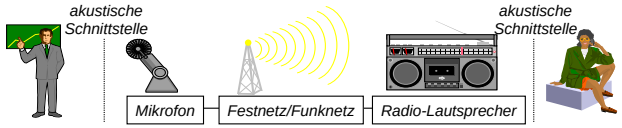
Kommunikation mit technischer Mitteln - Telekommunikation

- Die klassische Nachrichtentechnik / Telekommunikationstechnik ist von der Sprachkommunikation (Telefon) geprägt - technisch und wirtschaftlich
- Menschen als Kommunikationspartner:



Modell einer Telefonkommunikation

⇨ Das technische System wird in den - ansonsten weitgehend unveränderten - Kommunikationsablauf eingefügt.



Modell einer Rundfunkkommunikation

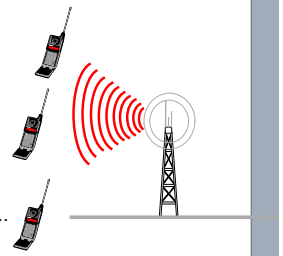
Computergestützte Telekommunikation

- Digitale Telekommunikation
  - Digitalisierung aller Kommunikationsformen (Gesprochene Sprache, Musik, Text, Grafik, Festbild, Bewegtbild (z.B. Video), Technische Daten)
  - Ausrichtung auf Multimedia (Integration mehrerer Kommunikationsformen) vorzugsweise für den Menschen als Empfänger
- Grundlage: Computer-Computer-Kommunikation
  - Digitale Telekommunikation ist auf Mikroelektronik/Computer-Basis und durch Hard-/Software-Systeme realisiert.
  - Moderne Telekommunikationsnetze (unter Einschluss der Endgeräte) sind Computernetze (Computer Networks).

Entwicklungstrend: Mobile Kommunikation

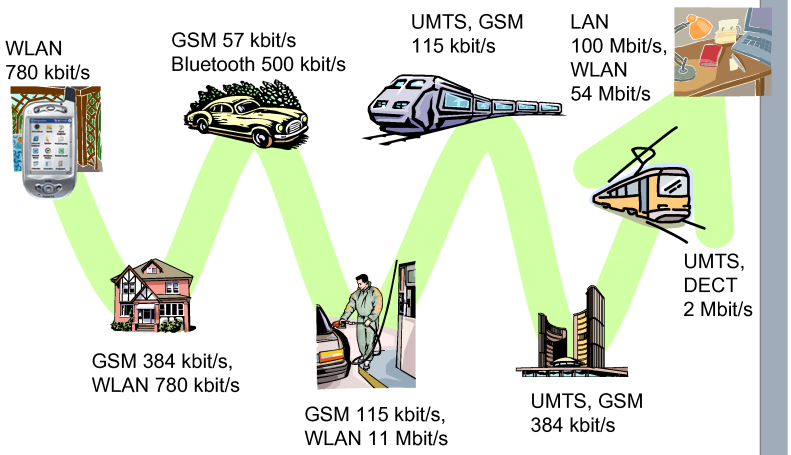
- „Jedermann, zu jeder Zeit, an jedem Ort (mit jeder Kommunikationsform)“

anybody, anytime, anywhere



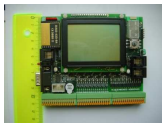
- Schrittmacherrolle: Mobiltelefonie
  - derzeit bereits über 2 Milliarden Nutzer
  - Festnetztelefonie bereits übertroffen
    - ebenso das „feste“ Internet
  - hohe Kosten einer drahtgebundenen Anschlussinfrastruktur
- Ziel:
  - Übertragung von Sprache, Daten, Audio, Video ...
- Mobilitätsaspekte
  - Gerätemobilität (Standortwechsel des Geräts möglich)
  - Benutzermobilität (Kommunikation von beliebigem Standort, z.T. über unterschiedliche Geräte)

Mobile and Wireless Web Services – Always Best Connected

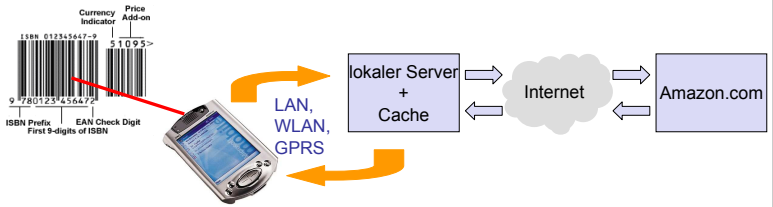


Entwicklungstrend: Kommunikation von Geräten

- **Heute**:
  - Telekommunikation zwischen Menschen im Vordergrund
- **Zukünftig**:
  - Technische Geräte / technische Systeme kommunikationsfähig
    „Internet of Things“
- Beispiele:
  - Produktionseinrichtungen
    Tele-Diagnose, Tele-Wartung, Tele-Betrieb
  - Kommunikation in/mit Fahrzeugen
    u.a. Verkehrstelematik
  - Hausnetze
    Sicherheit, Haushaltsgeräte-Kommunikation, Heizungssteuerung, usw.
  - Sensor-Netze
    häufig für Überwachungaufgaben



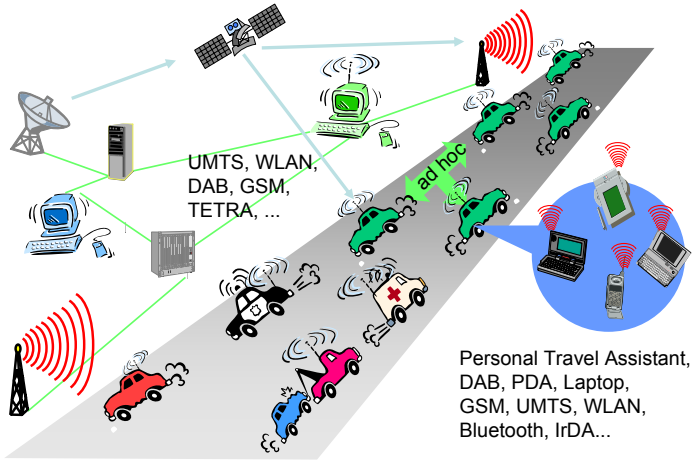
Beispielszenarien



Entwicklungstrend: Ubiquitäre Informationstechnologien

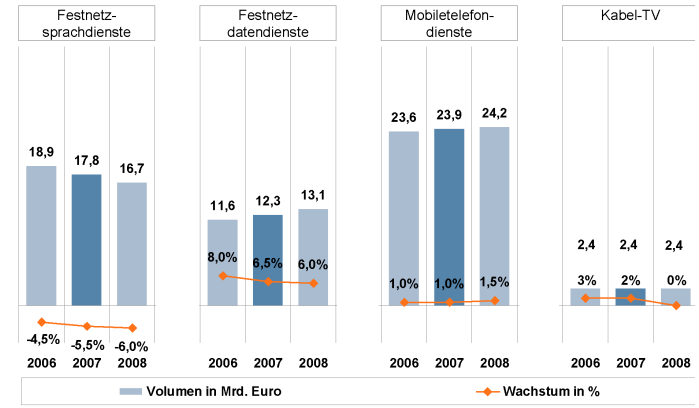
- Ubiquität („Allgegenwärtigkeit“):
  - Nichtgebundensein an einen Standort
  - Information als überall erhältliches Gut
  - ⇨ Information Technology (IT) beyond the PC
- Persönliche Technologien
  - Zugang zu IT-Diensten mit sich herumtragen
  - Beispiele: Persönliche Digitale Assistenten (PDAs), Wearable Devices
- Informationsumgebungen
  - Zugang zu IT-Diensten überall vorhanden
  - Beispiele: Intelligente, kommunikationsfähige Geräte/Systeme, Aktive Gebäude (cooperative buildings)
- Allgemeine Entwicklungstendenz
  - früher: Viele Menschen an einem Computer
  - heute: Ein Computer pro Person
  - bald: Viele Computer pro Person
- Ubiquitäre Unterstützung
  - wirkt im Hintergrund,
  - wird selbst aktiv,
  - (teil-)autonom von Menschen.

Entwicklungstrends in der Übersicht



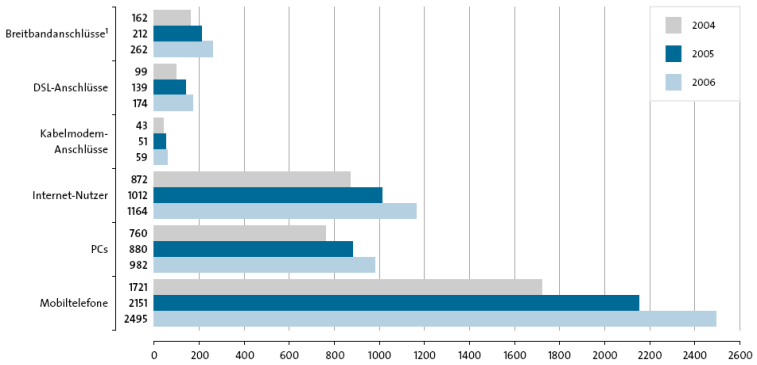
Telekommunikationsdienste

Marktsegmente TK-Dienste, Deutschland 2005-2007



Informationsinfrastruktur

Die Entwicklung weltweiter Informationsinfrastrukturen 2004 bis 2006 (in Millionen)

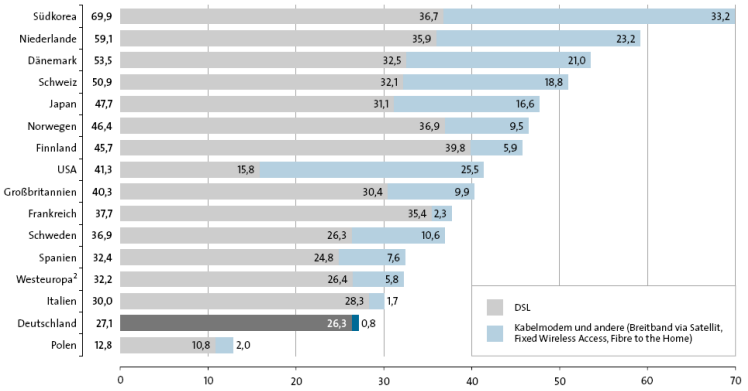


(1) DSL, Kabelmodem und andere

BITKOM; Basis: EITO

Breitbandanschlüsse

Breitbandanschlüsse je 100 Haushalte 2005[1]



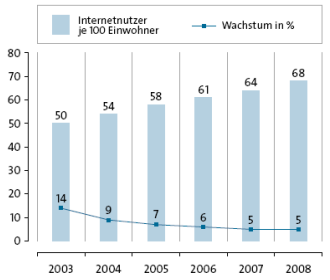
(1) Es wird die Gesamtzahl der Breitbandanschlüsse (einschließlich Unternehmensanschlüsse) auf die Anzahl der Haushalte bezogen

(2) einschließlich Türkei

BITKOM; Basis: EITO

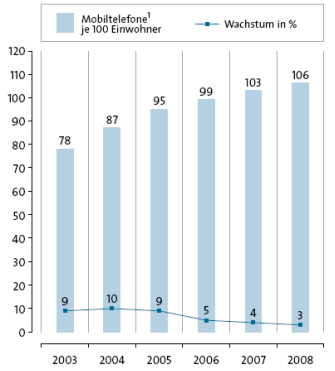
Internet und Mobilkommunikation in Deutschland

Prognose Internetnutzer Deutschland



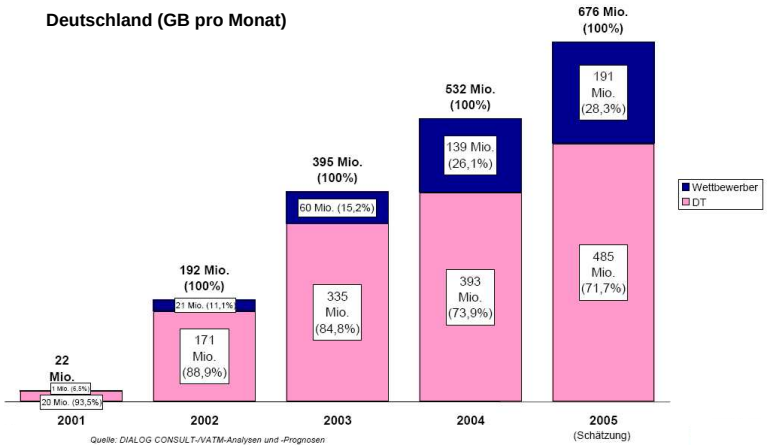
BITKOM; Basis: EITO

Prognose Mobiltelefone[1] Deutschland

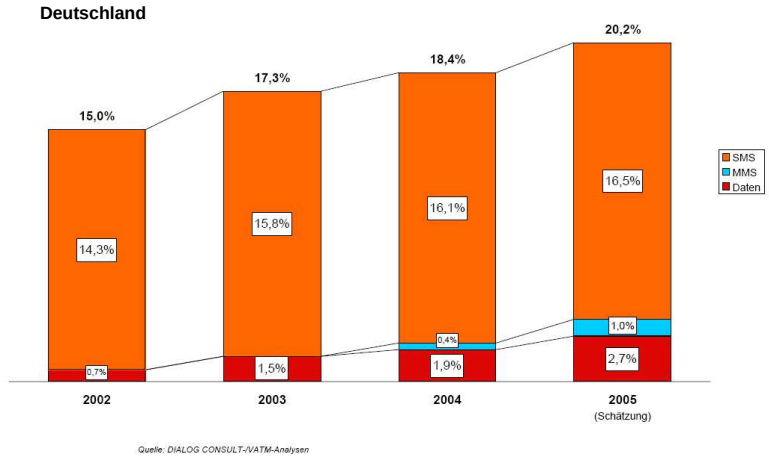


BITKOM; Basis: EITO

Volumenentwicklung Breitband-Internet-Verkehr

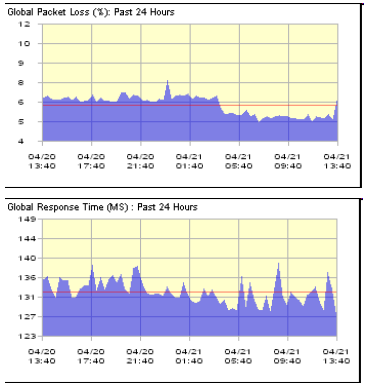


Datenanteil an den Diensteumsätzen im Mobilfunk



Qualität des Internet

- Zahlreiche Projekte führen Internet-Messungen durch, z.B. Internet Traffic Report: http://www.internettrafficreport.com/



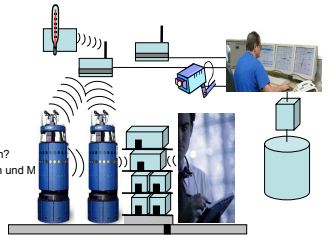
Einblick in aktuelle Forschungsaktivitäten

AmbiSense
Kooperation autonomer mobiler Systeme unter Berücksichtigung ambienter Sensoren

Kooperationsprojekt unter Beteiligung der Professoren Zell, Rosenstiel, Strasser (Univ. Tübingen) sowie Prof. Spath und Frau PD Weisbecker (Univ. Stuttgart)

Motivation - Digitale Objektwelt

- Digitale Objektwelt
  - Viele Objekte werden digital mit gekennzeichnet (Barcodes, RFIDs, …)
  - Datenbanken speichern Informationen zu den Objekten
- Entwicklungen
  - Zunehmender Einsatz autonomer mobiler Systeme (Roboter)
  - Arbeitsabläufe vermehrt in ambient-intelligenten Umgebungen
  - Mensch-Maschine-Schnittstelle mit wachsender Funktionalität und Bedeutung
- Wichtige Fragestellungen
  1. Was befindet sich in der Umgebung eines mobilen Systems?
  2. Lokalisation: Wo befinden sich Objekte, mobile Systeme und Menschen?
  3. Wie sieht eine geeignete Realisierung der Interaktion zwischen Mensch und M aus?



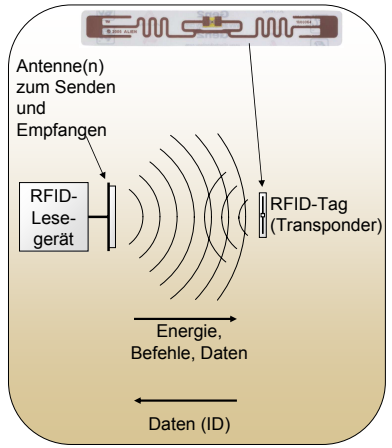
Radio-frequency Identification (RFID)

- Historie:
  - 1939: British Army benutzt RFID
  - 1973: Erstes RFID-Patent von Mario Cardullo
  - 1999: Gründung des Auto-ID Centers am MIT
  - 2003: Electronic Product Code (EPC) und Gründung EPCglobal Inc.

- Technologien:
  - Erkennung der RFID-Tags in der näheren Umgebung mi RFID-Lesegerät (keine Sichtverbindung erforderlich)
  - Jedes Objekt erhält eine eindeutige Nummer
  - Frequenzen: HF bei 13,56 MHz (ISO 14443, 15693), UHF bei 433 MHz, 868 MHz, 915 MHz und 2,45 GHz (ISO18000-7)
  - Allerdings keine global einheitliche Frequenz im UHF Band
  - Preis: ab 5 Cent

Objektkennzeichung mittels RFID

- Mikrochips mit Antenne (RFID-Tags, -Labels) identifizieren sich gegenüber einem RFID-Lesegerät
- Kommunikation: elektromagnetische Wellen
- Identifikation: Weltweit eindeutige Nummer (elektronischer Produktcode) mit ≥ 96 Bit (> 10^{15} mehr Kombinationen als EAN-13-Code)
- Einsatzgebiete im Handel
  - Heute/kurzfristig: Paletten
  - Mittel- bis langfristig: Kartons, einzelne Produkte
- Warensicherung, …



Kumulierte Verkaufszahlen 1944-2005: 2,397 Milliarden RFID-Chips

Branche	Kum. Anz. (in Mio.)
Transport/Automotive	1000
Finanzen/Sicherheit	670
Handel/Konsumgüter	230
Freizeit	100
Wäschereien	75
Bibliotheken	70
Fertigung	50
Tiere/Landwirtschaft	45
Gesundheitswesen	40
Flugverkehr	25
Logistik/Post	10
Militär	2
Sonstige	80
Total	**2397**

Objektkennzeichnung mit Sensorknoten

- Drahtlose Vernetzung von Geräten über kurze Distanz
- Geräte mit eindeutiger Adresse
- Kommunikation: Funkwellen (~2,4GHz)
- Übertragung: bis zu 2,1 MBit/s
- Ad-hoc-Netzwerkfähigkeit
- Verschlüsselung anwendbar

BTnode

Mica Node

Quelle: ETH Zürich

RFID vs. Bluetooth zur Kennzeichnung

RFID

- Identifikationszwecke
- Passive Tags benötigen keine Stromversorgung
- Als Labels nicht für zus. Intelligenz ausgelegt
- Kosten:
  - Tags: 0,08-0,30 €
  - Lesegerät: 1.000-2.500 €
- Effiziente Identifikation potenziell auf Item-Level

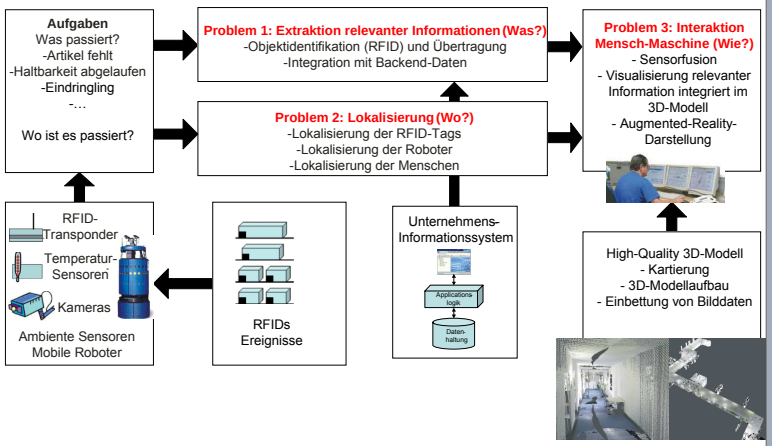
Bluetooth

- Beliebige Daten
- Sensorknoten mit Stromzufuhr
- Um zusätzliche Intelligenz erweiterbar (z.B. Wärmesensor, Mikroprozessoren)
- Kosten:
  - Bluetooth-Chip: 4 $
  - Sensorknoten: 10-170 €
- Überwachung von Containern bzw. hochwertigen Produkten

Grenzen des RFID Einsatzes

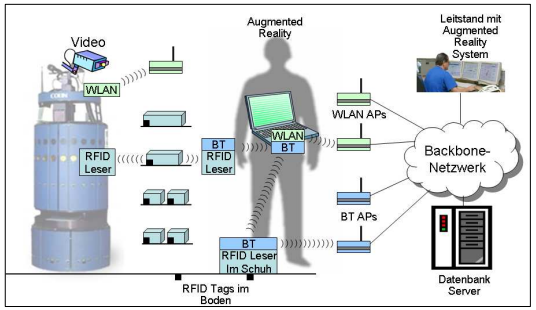
- Chaotische Lagerhaltung, z.B. im Supermarkt lässt sich noch nicht erfassen
- Noch nicht ausreichend kosteneffizient
  - Bessere Automatisierung (zum Beispiel durch Roboter)
- Erkennungsraten noch nicht hoch genug
  - Höhere Redundanz bei Erfassung erforderlich
  - Erfassung von Objekten durch ambiente Sensorik nicht nur durch Barcode oder RFID
- Keine kontinuierliche Lokalisierung von Objekten (nur wenn sie sich nahe eines Lesegeräts befinden)

Drei Schlüsselprobleme



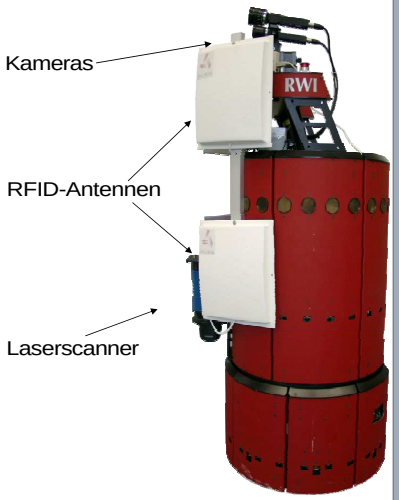
Anwendungszenario

- Lagerverwaltung
  - Zuordnung von Waren durch RFID
  - Ständige Positionsbestimmung während der Arbeit
  - Abfrage von Zusatzinformationen in einer Datenbank
  - Darstellung auf PDA / Notebook, eventuell Augmented Reality Display
  - Fortlaufende Inventur

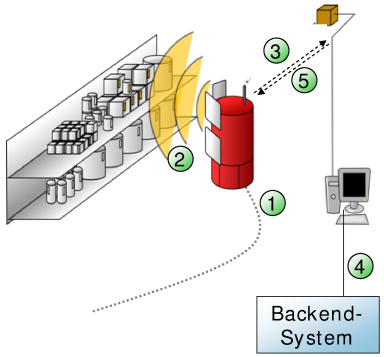


Schnittstelle: Autonome Systeme

- RWI-B21-Serviceroboter
- Verschiedene Sensoren zur multimodalen Umgebungs-modellierung/ Objekterfassung, z.B.
  - RFID-Lesegerät
  - Kameras
- WLAN-Anbindung an externe Systeme/ globales Weltmodell
- Möglichkeit der fortlaufenden Inspektion der Umgebung



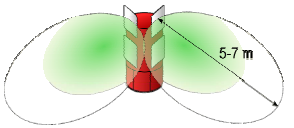
Warenerkennung mittels RFID

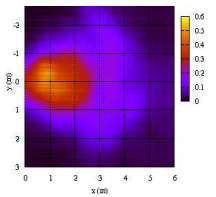


1. Roboter exploriert Umgebung
2. Objekt-ID wird gelesen
3. Weltmodell empfängt die ID
4. Zusatzinformationen vom ERP-System werden ggf. abgefragt
5. Objekt mitsamt Zusatzinformationen steht angeschlossenen Systemen bereit (auch dem Roboter selbst!)

Lokalisierung mittels RFID

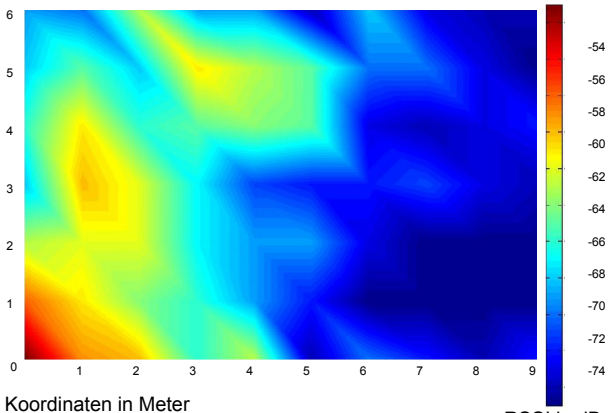
- Roboter mit handelsüblichem UHF-RFID-Lesegerät und RFID-Antennen
- Detektion von RFID-Tags ortsabhängig
  Einsatz von Partikelfilter
- Sensormodell maschinell lernbar
- Genauigkeit besser als 0,3 m





Radiosignalausbreitung Bluetooth

Feldstärke in Abhängigkeit der Entfernung

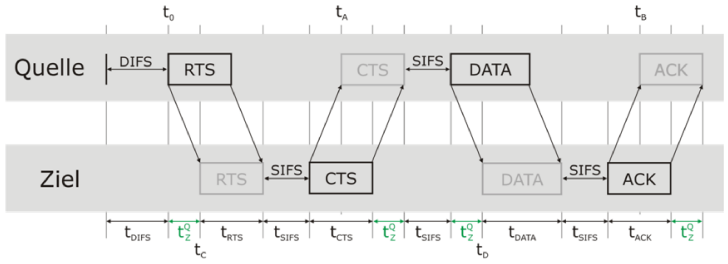


Koordinaten in Meter

RSSI in dB

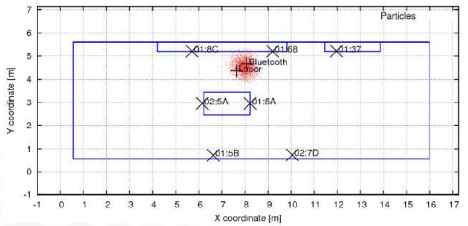
WLAN-Laufzeitmessungen

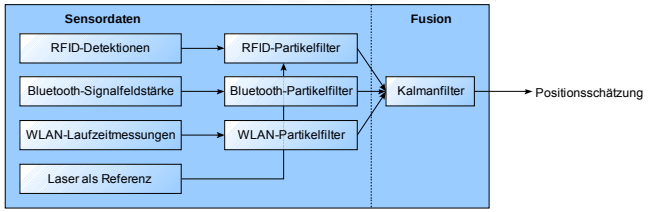
- Ausnutzung von WLAN Protokollabläufen
- Time-of-Arrival-Messungen in Standardisierung IEEE 802.11 Task Group v



Sensorfusion

- Ziel:
  - Robuste (und präzisere) Lokalisierung mit verschiedenen Typen ambienter Sensorik
- Umsetzung:
  - Statistische Fusionsverfahren (Kalman- / Partikelfilter) zur Integration der heterogenen Sensorik





Visualisierung zugeordneter Daten

- Ansatz:
  - Browser-Inhalt in VR-Grafik darstellen
  - Browser-Interaktion zur Verfügung stellen

3D-Szene

WebPage
(mit ERP-Infos, …)

Screenshot

RFIDs mit kryptographischen Algorithmen

Authentifizierung
z.B. für KFZ-Schlüssel, Bezahlsysteme

- Beispiel: Texas Instrument DST40 RFID Kryptographie-Chip (z.B. eingesetzt in KFZ-Schlüsseln, Ford 2005)
- Challenge-Response-Mechanism
- 40 Bit Schlüssel
- Proprietäre Verschlüsselungsfunktion von Texas Instruments

Schlüssel		PKW
• Send identifier	⇨	• Check ID
• Encrypt challenge	⇦	• Generate and send challenge
• Send as response	⇨	• Verify response

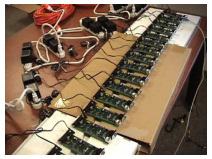
RFIDs mit kryptographischen Algorithmen

Schwächen des Texas Instruments DST40 RFID Chips

- 40 Bit Schlüssel ⇨ Brute force Angriffe möglich
- Proprietärer Algorithmus ⇨ Möglicherweise zusätzliche Schwächen

Erster Angriff

- John Hopkins University
- Reverse engineering und Veröffentlichung des Algorithmus
- 10 personal computers ⇨ 2 Wochen
- 16 FPGAs 5 keys in 2h ⇨ ~24 min



Weiterführende Arbeiten

- Informatik-Methoden zur Berechnung von Tabellen ⇨ schnelle Berechnung in SW
- Kleine Geräte zum Kopieren solcher Schlüssel

www.rfidanalysis.org

Ausblick

- Zunehmenden Einsatz der vorgestellten Technologien
  - Wirtschaftliches Potential
- Noch viele ungelöste Probleme, u.a.
  - Informationelle Selbstbestimmung
  - Sicherheitsschwächen
- Kommunikation, Mobilität, Sicherheit
  ⇨ immer neue spannende Anwendungen werden möglich
- Die vorgestellten Technologien sind exemplarisch zu sehen