Reliability – from Distributed Systems to Ubicomp

RESEARCH GROUP FOR

Distributed Systems

Ubiquitous Information Doktorandenseminar

23. Januar 2002

Jürgen Bohn

BOHN@INF.ETHZ.CH

ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

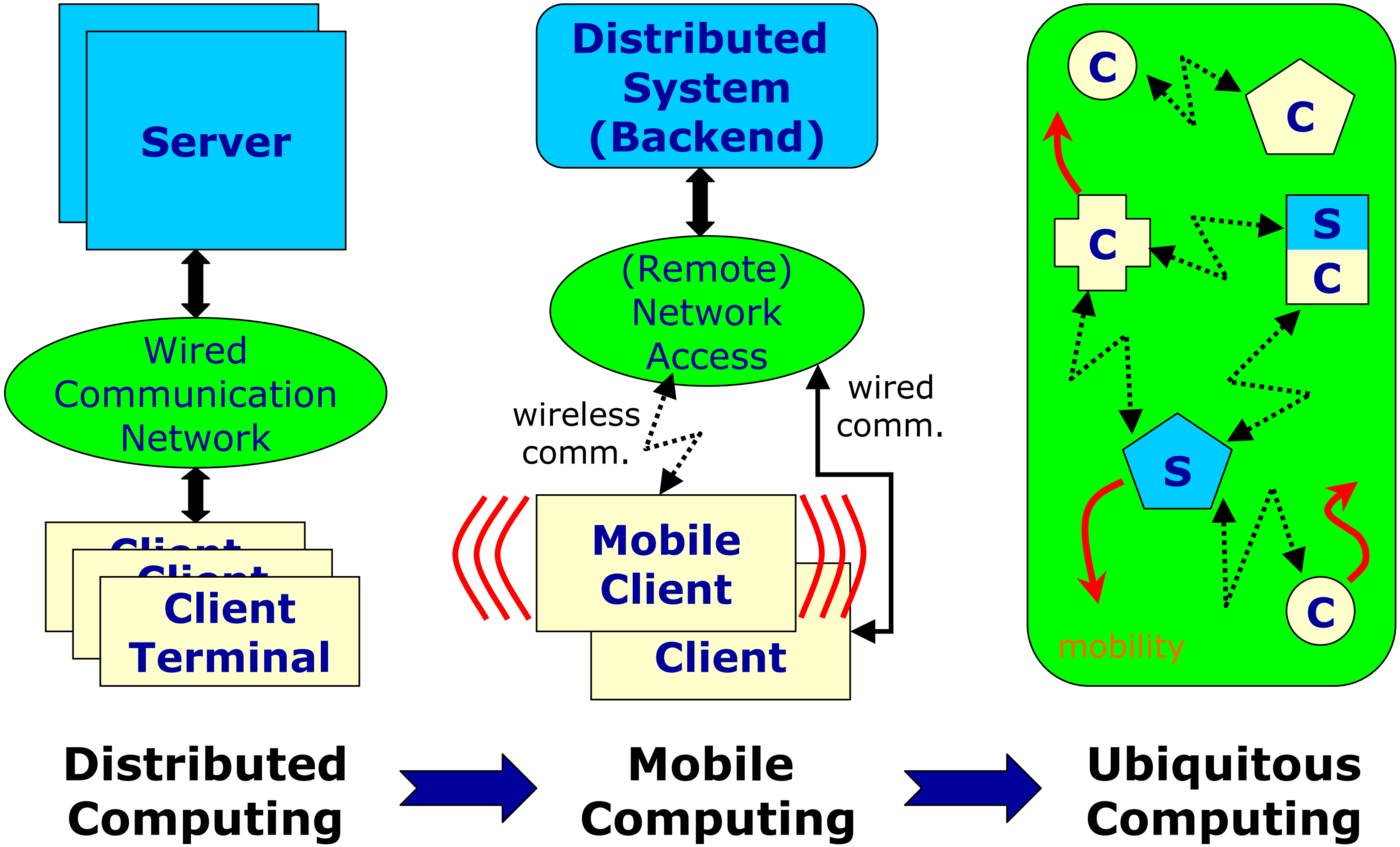
Outline

- Development of Distributed Systems
  - Distributed Computing (DC)
  - Mobile Computing (MC)
  - Ubiquitous Computing (UC/Ubicomp)
- Evolution of Reliability Problems
- Reliability Challenges in Ubicomp

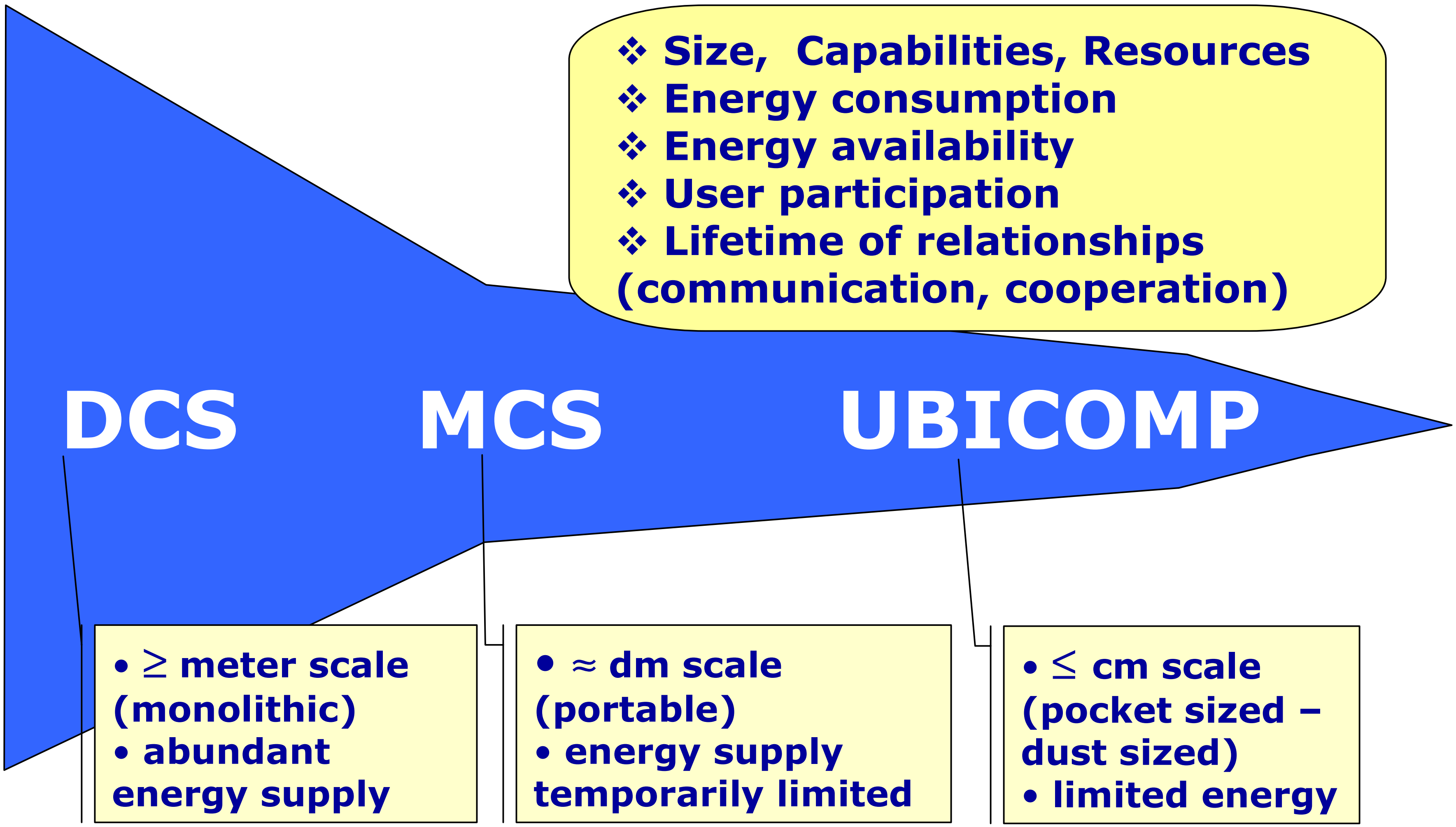
Distributed Systems

- Definition:
  "All computer applications where several autonomous computers, processors or processes cooperate in some way" [Tel 2000]
- Coordination requires communication
- Reasons for Distributed Systems:
  - information exchange
  - resource sharing
  - increased reliablility through replication
  - increased performance through parallelization
  - simplification of design through specialization

Development of Distr. Systems



Evolution of Characteristics I



Evolution of Characteristics II

- ❖ Diversification, heterogeneity
- ❖ Specialization, simplicity
- ❖ Number of interacting units
- ❖ Decentralization
- ❖ Spontaneity
- ❖ Mobility

DCS

- authorized networks
- static network topology
- absolute position (fixed)

MCS

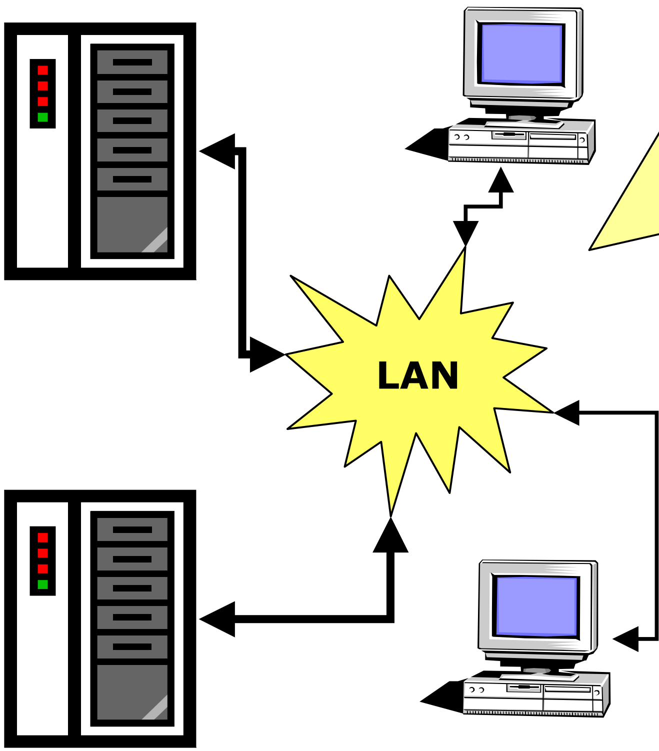
- infrastructure-based networks
- static backbone topology
- absolute position (variable)

UBICOMP

- ad-hoc networks
- highly dynamic topology
- relative position (dynamic, physical proximity)

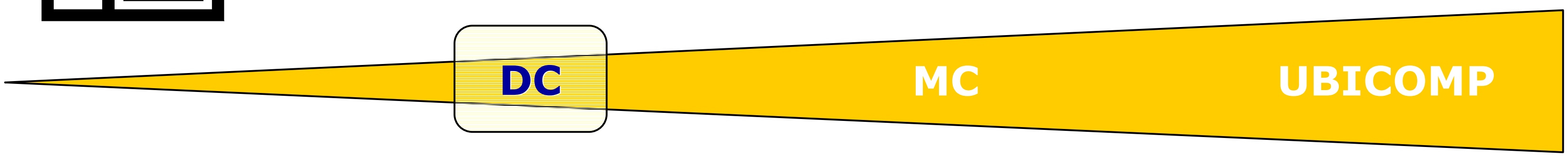
Distributed Computing Syst.

Distribute Hardware, Applications and Services



Technical Characteristics

- immobility
- authorized networks, static topology
- homogeneous entities
- terminal (client) vs. server
- static topology
- permanent connectivity
- constant power supply
- one client for many users
- size ≥ meter scale



Reliable Distributed Systems

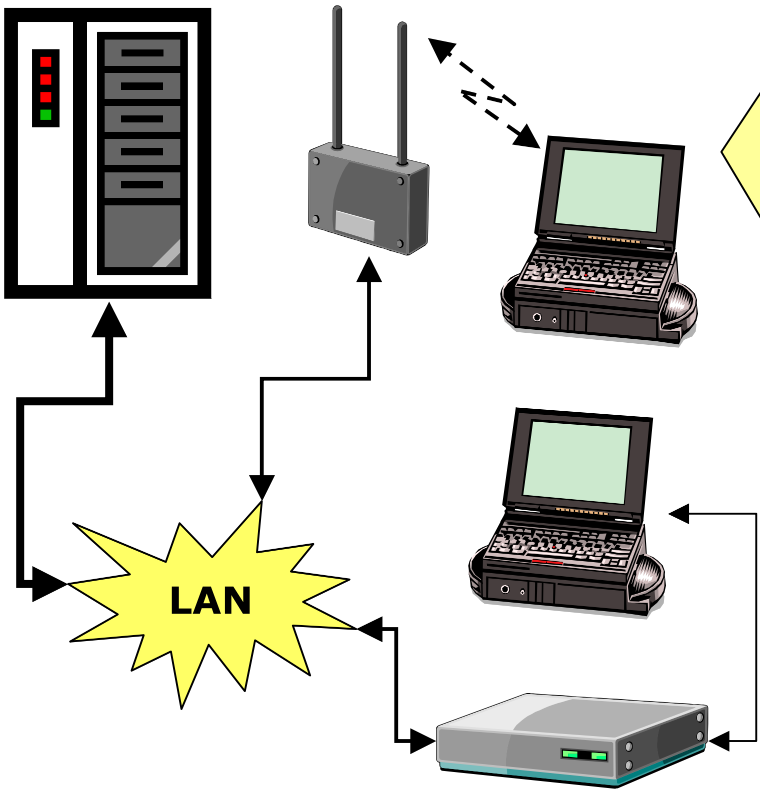
- Reliable system =
  reliable soft- and hardware
  - appearance of faults is treated as anomaly
- Achieved by introducing fault tolerance
  = ability of a system to behave in a well-defined manner once faults occur
- Allot redundancy to troublespots
- Technology dominated approach
  - user expectations reduced to quality of technical system properties

Building Reliable Distr. Systems

- Fault Tolerant Services
  - fault tolerant software (cont. service under *design faults*)
  - process resiliency (continued service under *node failures*)
  - data resiliency (continued service under *node failures*)
  - atomic actions (consistency under *node failures*)
  - consistent state recovery (consist. under *node failures*)
- Basic Building Blocks
  - reliable and atomic broadcast
  - fail stop processors, stable storage, reliable communication
- Distributed System

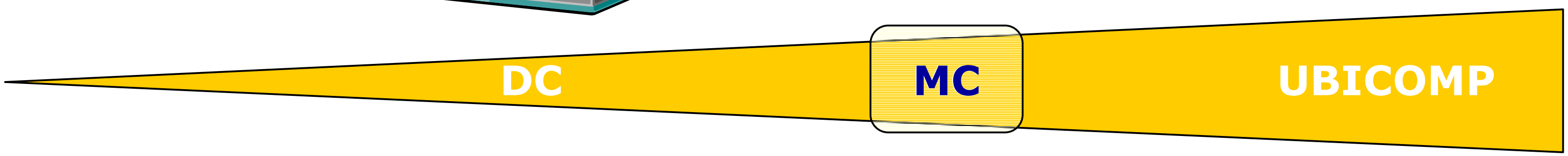
Mobile Computing Systems

Support client mobility



Technical Characteristics

- nomadic client vs. server
- variable network topology
- infrastructure-based client comunication
- new wireless communication technologies
- intermittent disconnections
- intermittent power shortage
- one client per user
- size ≈ decimeter scale

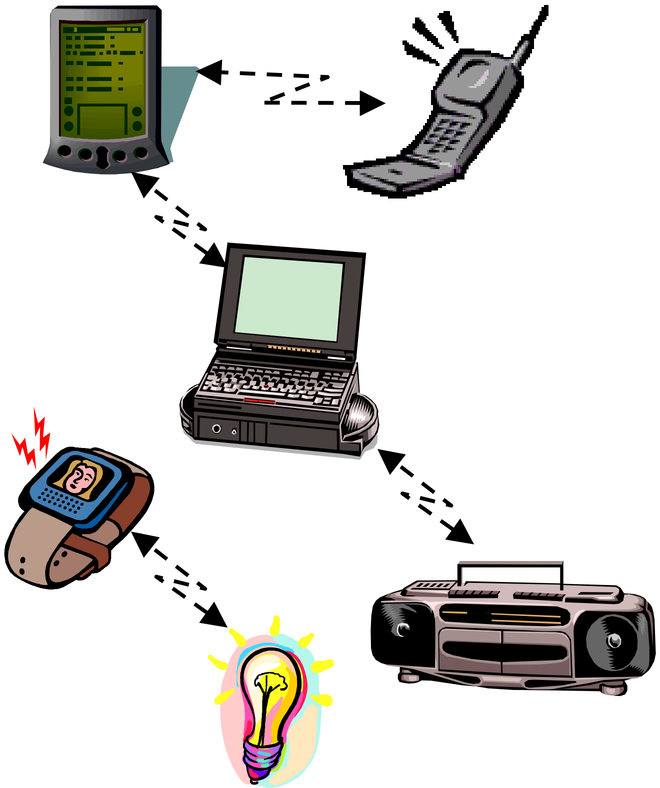


Reliable in spite of Mobility

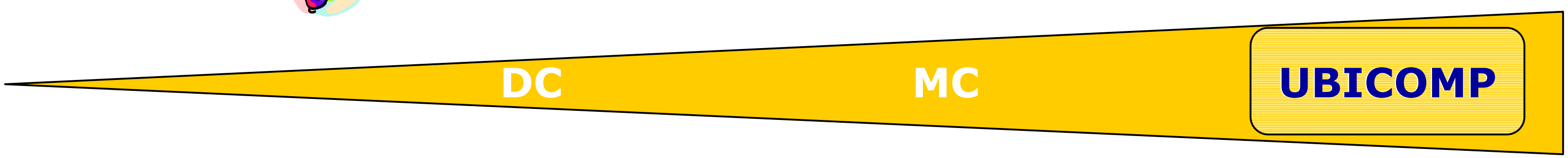
- Mobile information access
  - disconnected operation
  - bandwidth adaptive file access
- Support for nomadicity
  - mobile networking, e.g., Mobile IP
- Reliable communication
  - enhanced wireless mobility support, e.g. cellular systems such as 3G systems and IMT 2000 standard
  - choice of access standards, e.g., CDMA, TDMA, GSM
  - reliable routing and communication protocols
- Adaptive applications and resource management

Ubiquitous Computing Syst.

Sense and control environment



Technical Characteristics
- high mobility / dynamics
- frequent topology changes
- device ≈ client ≈ server
- ad-hoc short-range wireless communication
- intermittent connectivity
- limited power supply
- many devices per task
- size ≤ centimeter scale
- vulnerable to failures



Technical Challenges

- High diversity and large numbers of devices
  - device density varying, unevenly distributed
  - increased probability that device faults occur
- Transient short-lived relationships
  - high degree of fluctuation regarding communication, interaction, cooperation, position
- Spontaneity of relations and interactions
  - initative devices, proactive behaviour
  - spontaneous establishment/cancelling of interconnection/interaction/cooperation

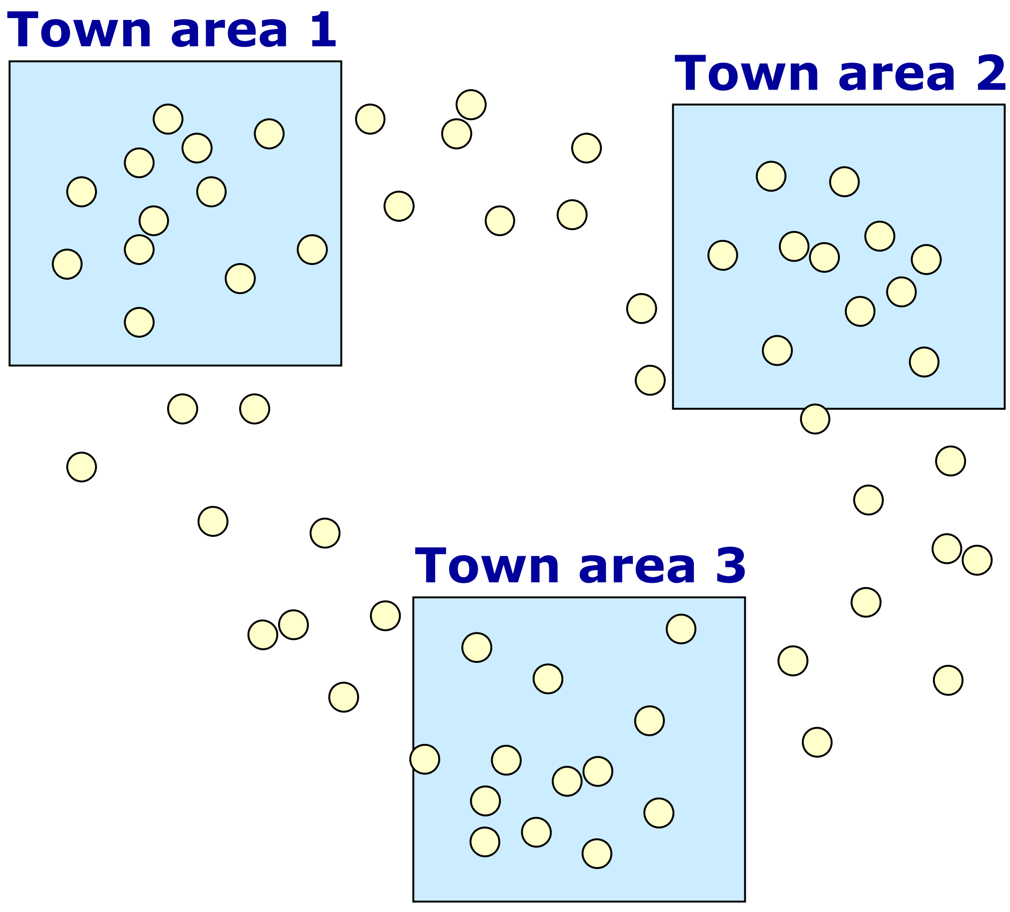
Coordination Problem

- Decentralized coordination of autonomous devices
  - number of active units increases tremedously
  - ever smaller, more heterogeneous and more specialized devices → uneven conditions
  - device capabilities (resources and energy) diminish
  - inherent system dynamics seem to prevent
    - centralized management
    - global system snapshot
- Scalability
  - number of sensors vs. communication costs
  - today‘s wireless sensor protocols do not scale well

Example: Terminodes Project

- Terminodes = terminal + node (EPFL NCCR)
- Self-organized wide area mobile ad-hoc network
  - public environment, run by users, non-authority based
  - potentially very large, unevenly distributed
  - highly co-operative (task solving)
- Terminode (local & remote) routing
  - Key issues: mobility, scalability, geographic coverage
  - local vs. remote routing (relative vs. geographic pos.)
  - maintain multiple paths, keep track of friendly devices
- Not covered
  - practical scalability experiments, e.g. considering radio interference (250m range per node), energy efficiency

Terminode Routing Simulation



Setting:
- town & highway mobility model
- (no random waypoints)
- peer-to-peer communications
- 600 terminodes
- 30 traffic flows

Results:
Packet delivery rate up to 80% vs. 10% in trad. MANETs.

Persistent/Intrinsic Problems

- Robustness and Availability
- Security related
  - lack of confidentiality due to limited cryptographic device capabilities
  - vulnerable "on the air" communication
- Privacy related
  - talkative proactive devices
  - lack of awareness and control over information and data flow, e.g. in smart spaces
  - user tracking/surveillance

Where Fault Tolerance Comes In

- Fault Tolerance as well-known means to increase overall robustness
- BUT: Do classic FT models and terminologies still hold in ubiquitous environments?
  - what is a transaction/checkpointing in UC?
  - what is consistency of state/data? ...

Boundary Conditions for FT

In Traditional DCS	In Ubicomp Systems
– reliable communication – infrastructure networks	– unreliable communication – ad-hoc wireless networks
– topology rather static – long-lived relationships – global snapshot viable	– topology very dynamic – short-lived relationships – local snapshots only
– faults occur rarely	– faults are common
– resourcefulness – capable devices	– scarcity of resources – simple specialized devices

There's a big discrepancy!

Classic FT fit for Ubicomp?

- Enormous shift in boundary conditions challenges classic FT solutions:

(a) Basic FT building blocks become inapplicable?

- e.g., stable storage, reliable communication, reliable atomic broadcast, ...

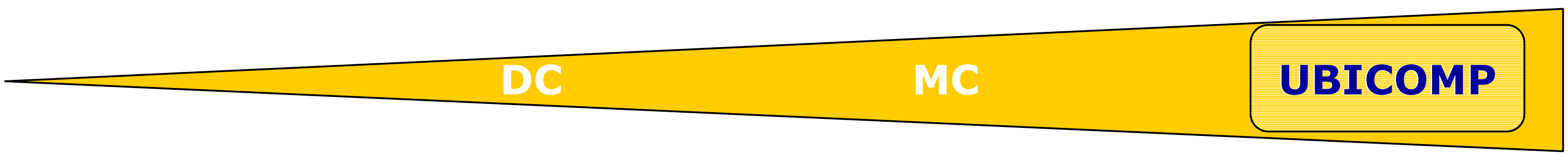
(b) Do today's fault tolerant mechanisms and distributed algorithms still work in Ubicomp?

- e.g., consistent state recovery, checkpointing, leader election, ...

➔ Many open questions – promising field for future work

Research Challenges

- Intensified coordination problem
  - prediction/assessment of global predicates?
    snapshot of global system state impossible?
  - role of device specialization?
- Self-stabilizing systems and algorithms
  - local optimization and organization?
- Formalization of and adequate models for fault tolerance in Ubicomp
- High redundancy as an advantage



Further Problematic Characteristics

- Faults are part of the game (normality)
  - increased fault probability with growing number of small and simple devices
- Pervasion of everyday life
  - pervades objects and environment
  - no way to escape
  - potentially high reliance of users
- Invisibility and concealment
  - hidden contact and interaction
  - unobtrusive, not perceptible to user

Further Research Challenges

- A trustworthy Ubicomp system that justifies reliance should meet the user‘s expectations
- Evidence that reliability in Ubicomp is interwoven with other disciplines
  - e.g., security, privacy, trust
- Is there a more holistic reliability model that respects the new circumstances?
  - fault tolerance and redundancy helps to achieve robustness (technology-based view point)
  - what about other properties such as pervasiveness, invisibility, concealment of actions etc.?

Research in Progress

- Ad-hoc networks
  - reliable communication (technical wireless aspects)
  - scalable ad-hoc routing
  - self-organization
  - security
- Masking Uneven Conditioning
  - harmonize huge differences in smartness in different environments
- Localized Scalability
  - physical distance vs. relative physical proximity
- Invisibility in Ubicomp
  - minimize user distraction, meet user‘s expectations

Conclusion & Discussion

- Characteristics of Ubicomp systems differ significantly from traditional distributed systems
- It seems very likely that classic solutions for reliable distributed systems do no longer hold in ubiquitous environments
- What are the ramifications? Is there even a more holistic reliability model conceivable?
- What means exist to assess and quantify reliability in this new context?
- Discussion!