Final Meeting
(before the exams)

- Meeting Point: Waldkirch, main station
- Date: Tuesday 27.02.2006 14:01
  (Train departs Freiburg main station at 13:40)

- Plan
  - Hike the Kastelburg
  - Picknick

- BYOF
  - Order drinks on-line

- Don’t forget
  - Food
  - Umbrella
  - Matches
Data-centric and content-based networking

- Interaction patterns and programming model
- Data-centric routing
- Data aggregation
- Data storage
Data-centric storage

- Problem: Sometimes, data has to be stored for later retrieval – difficult in absence of gateway nodes/servers

- Question: Where/on which node to put a certain datum?
  - Avoid a complex directory service

- Idea: Let name of data describe which node is in charge
  - Data name is hashed to a geographic position
  - Node closest to this position is in charge of holding data
  - Akin to peer-to-peer networking/distributed hash tables
  - Hence name of one approach: **Geographic Hash Tables (GHT)**
  - Use geographic routing to store/retrieve data at this “location” (in fact, the node)
Geographic hash tables – Some details

- Good hash function design
- Nodes not available at the hashed location – use “nearest” node as determined by a geographic routing protocol
  - E.g., the node where an initial packet started circulating the “hole”
  - Other nodes around hole are informed about node taking charge
- Handling failing and new nodes
  - Failure detected by timeout, apply similar procedure as for initially storing data
- Limited storage per node
  - Distribute data to other nodes on same face
Conclusion

- Using data names or predicates over data to describe the destination of packets/data opens new options for networking.

- Networking based on such “data-centric addresses” nicely supports an intuitive programming model – publish/subscribe.

- Aggregation a key enabler for efficient networking.

- Other options – data storage, broadcasting aggregates – also well supportable.
Naming and Indexing

➢ Non-standard options for denoting the senders/receivers of messages
  - Traditional (fixed, wireless, ad hoc): Denote individual nodes by their identity
  - WSN: Content-based addresses can be a good complement

➢ When addresses are not given a priori, they have to be determined “in the field”
  - Some algorithms are discussed
Names vs. addresses

- **Name**: Denote/refer to “things”
  - Nodes, networks, data, transactions, ...
  - Often, but not always, unique (globally, network-wide, locally)
  - Ad hoc: nodes – WSN: Data!

- **Addresses**: Information needed to find these things
  - Street address, IP address, MAC address
  - Often, but not always, unique (globally, network-wide, locally)
  - Addresses often hierarchical, because of their intended use in, e.g., routing protocols

- **Services to map between names and addresses**
  - E.g., DNS

- **Sometimes, same data serves as name and address**
  - IP addresses are prominent examples
Issues in address management

- **Address allocation**: Assign an entity an address from a given pool of possible addresses
  - Distributed address assignment (centralized like DHCP [Dynamic Host Configuration Protocol] does not scale)

- **Address deallocation**: Once address no longer used, put it back into the address pool
  - Because of limited pool size
  - Graceful or abrupt, depending on node actions

- **Address representation**

- **Conflict detection & resolution** (*Duplicate Address Detection*)
  - What to do when the same address is assigned multiple times?
  - Can happen e.g. when two networks merge

- **Binding**
  - Map between addresses used by different protocol layers
  - E.g., IP addresses are bound to MAC address by ARP (Address Resolution Protocol)
Distributed address assignment

- **Option 1**: Let every node randomly pick an address
  - For given size of address space
  - Risk of duplicate addresses

- **Option 2**: Avoid addresses used in local neighborhood

- **Option 3**: Repair any observed conflicts
  - Temporarily pick a random address from a dedicated pool and a proposed fixed address
  - Send an *address request* to the proposed address, using temporary address
  - If *address reply* arrives, proposed address already exists
  - Collisions in temporary address unlikely, as only used briefly

- **Option 4**: Similar to 3, but use a neighbor that already has a fixed address to perform requests
Content-based addresses

- Recall: Paradigm change from id-centric to data-centric networking in WSN
- Supported by content-based names/addresses
  - Do not described involved nodes (not known anyway), but the content itself the interaction is about
- Classical option: Put a naming scheme on top of IP addresses
  - Done by some middleware systems
Geographic addressing

- Express addresses by denoting physical position of nodes
  - Can be regarded as a special case of content-based addresses
  - Attributes for x and y coordinates (and maybe z)

- Options
  - Single point
  - Circle or sphere centered around given point
  - Rectangle by two corner points
  - Polygon/polytope by list of points
  - …
ISO/OSI 7-layer reference model (complete network)

- Layer 7: Application
  - Application protocol
  - Application
    - APDU

- Layer 6: Presentation
  - Presentation protocol
  - Presentation
    - PPDU

- Layer 5: Session
  - Session protocol
  - Session
    - SPDU

- Layer 4: Transport
  - Transport protocol
  - Transport
    - TPDU
  - Communication subnet boundary
    - Internal subnet protocol

- Layer 3: Network
  - Network
  - Network
    - Packet
  - Data link
    - Data link
      - Frame
  - Physical
    - Physical
      - Bit

- Host A
  - Network layer host-router protocol
  - Data link layer host-router protocol
  - Physical layer host-router protocol

- Host B

Name of unit exchanged
Protocols for dependable data transport

- Dependability requirements
- Delivering single packets
- Delivering blocks of packets
- Delivering streams of packets
**Dependability aspects**

- **Coverage & deployment**
  - Is there a sufficient number of nodes such that an event can be detected at all? Such that data can accurately measured?
  - How do they have to be deployed?

- **Information accuracy**
  - Which of the measured data have to be transported where such that a desired accuracy is achieved?
  - How to deal with inaccurate measurements in the first place?

- **Dependable data transport**
  - Once it is clear which data should arrive where, how to make sure that it actually arrives?
  - How to deal with transmission errors and omission errors/congestion?
“Dependable” is an umbrella term

Main numerical metrics

- **Steady state availability** – probability that a system is operational at any given point in time
  - Assumption: System can fail and will repair itself
- **Reliability at time t** – Probability that system works correctly during the entire interval \([0,t)\)
  - Assumption: It worked correctly at system start \(t=0\)
- **Responsiveness** – Probability of meeting a deadline
  - Even in presence of some – to be defined – faults
- **Packet success probability** – Probability that a packet (correctly) reaches its destination
  - Related: packet error rate, packet loss rate
- **Bit error rate** – Probability of an incorrect bit
  - Channel model determines precise error patterns
Wireless sensor networks (WSN) have unique constraints for dependable data delivery
- Transmission errors over a wireless channel
- Limited computational resources in a WSN node
- Limited memory
- Limited time (deadlines)
- Limited dependability of individual nodes

**Standard mechanisms: Redundancy**
- Redundancy in nodes, transmission
- Forward and backward error recovery
- Combinations are necessary!
Dependable data transport – context

- **Items to be delivered**
  - Single packet
  - Block of packets
  - Stream of packets

- **Level of guarantee**
  - Guaranteed delivery
  - Stochastic delivery

- **Involved entities**
  - Sensor(s) to sink
  - Sink to sensors
  - Sensors to sensors

50% delivered
Constraints

- **Energy**
  - Send as few packets as possible
  - Send with low power → high error rates
  - Avoid retransmissions
  - Short packets → weak FEC
  - Balance energy consumption in network

- **Processing power**
  - Only simple FEC schemes
  - No complicated algorithms (coding)

- **Memory**
  - Store as little data as briefly as possible
Overview

- Dependability requirements
  - Delivering single packets
    - Single path
    - Multiple paths
    - Gossiping-based approaches
    - Multiple receivers
  - Delivering blocks of packets
  - Delivering streams of packets
Delivering single packets – main options

➢ What are the intended receivers?
   - A *single receiver*?
   - *Multiple receivers*?
     • In close vicinity? Spread out?
   - Mobile?

➢ Which routing structures are available?
   - Unicast routing along a *single path*?
   - Routing with *multiple paths* between source/destination pairs?
   - No routing structure at all – rely on *flooding/gossiping*?
Single packet to single receiver over single path

- Single, multi-hop path is given by some routing protocol

- Issues: Which node
  - Detects losses (using which indicators)?
  - Requests retransmissions?
  - Carries out retransmissions?
Detecting & signaling losses in single packet delivery

- Detecting loss of a single packet:
  Only positive acknowledgements (ACK) feasible
    - Negative acks (NACK) not an option – receiver usually does not know a packet should have arrived, has no incentive to send a NACK

- Which node sends ACKs (avoiding retransmissions)?
  - At each intermediate node, at MAC/link level
    • Usually accompanied by link layer retransmissions
    • Usually, only a bounded number of attempts
  - At the destination node
    • Transport layer retransmissions
    • Problem: Timer selection
Carrying out retransmissions

- For link layer acknowledgements: Neighboring node

- For transport layer acknowledgements:
  - Source node → end-to-end retransmissions
Example schemes: HHR and HHRA

- **Hop-by-hop reliability (HHR)**
  - Idea: Locally improve probability of packet transmission, but do not use packet retransmission
  - Instead, simply repeat packet a few times – a repetition code
  - Choose number of repetitions per node such that resulting end-to-end delivery probability matches requirements

- **Hop-by-hop reliability with Acknowledgements (HHRA)**
  - Node sends a number of packets, but pauses after each packet to wait for acknowledgement
  - If received, abort further packet transmissions
Multiple paths

- Types of: disjoint or braided
- Usage: default and alternative routes
- Usage: simultaneous
  - Send same packet
  - Send redundant fragments
- Example: ReInForM
Multiple paths: Disjoint or braided

Disjoint paths

Secondary path

Braided paths

Wireless Sensor Networks

13.02.2007 Lecture No. 26 - 27
Using multiple paths

- **Alternating use**
  - Send packet over the currently “selected” path
  - If path breaks, select alternative path
  - Or/and: repair original path locally

- **Simultaneous use**
  - Send the complete packet over some or all of the multiple paths simultaneously
  - Send packet fragments over several paths
    - But endow fragments with redundancy
    - Only some fragments suffice to reconstruct original packet
Conclusion

- Transport protocols have considerable impact on the service rendered by a wireless sensor networks
- Various facets – no “one size fits all” solution in sight
- Still a relatively unexplored areas

- Items not covered
  - Relation to coverage issues
  - TCP in WSN? Gateways?
  - Aggregation? In-network processing?
Thank you
and thanks to Holger Karl for the slides