Lecture 6

Internet Protokolle II

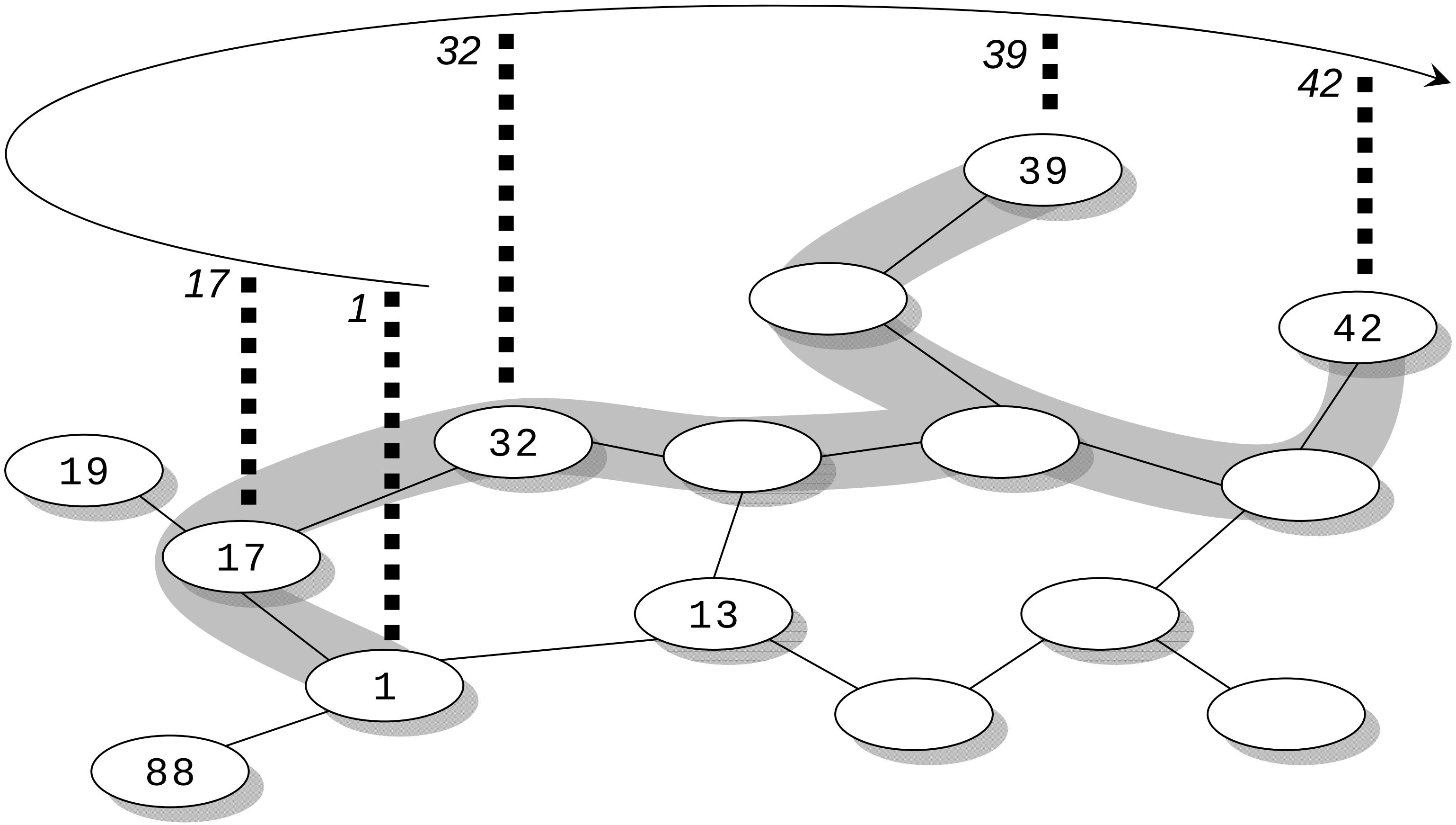
From Ad-hoc Networks
to Sensor Networks

Routing Part III

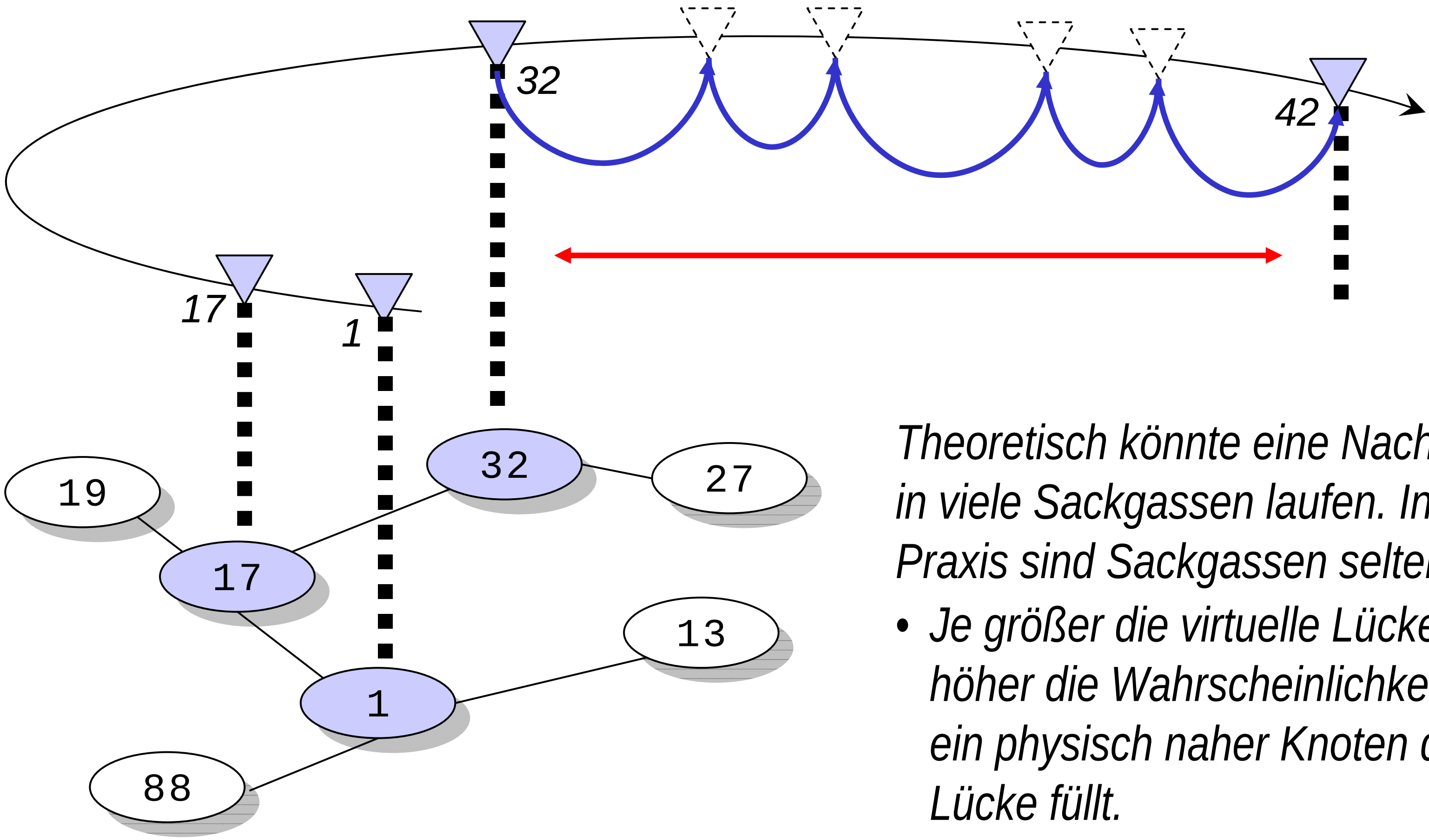
Thomas Fuhrmann

Network Architectures
Computer Science Department
Technical University Munich

Virtual Ring Routing / Scalable Source Routing



SSR – Selbstorganisation (1)

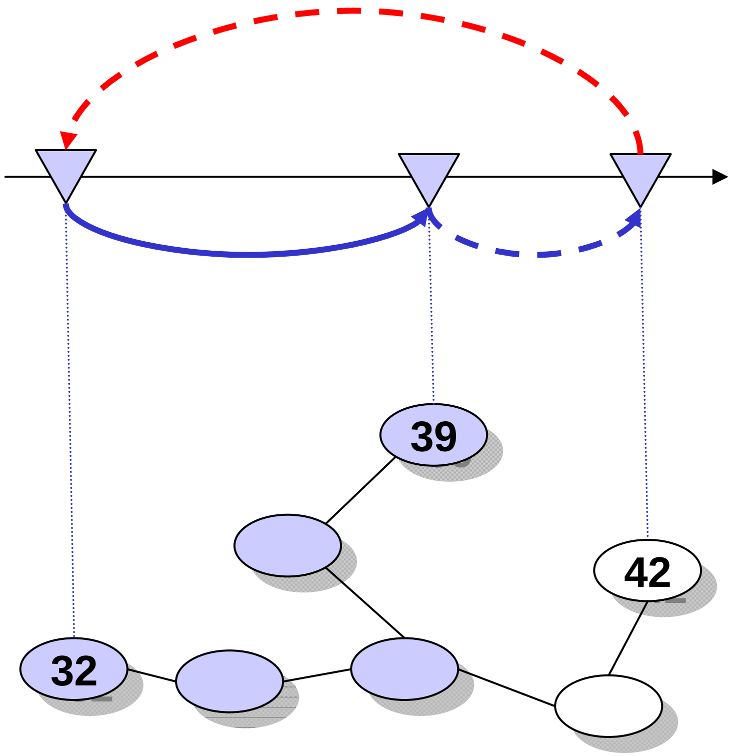


Theoretisch könnte eine Nachricht in viele Sackgassen laufen. In der Praxis sind Sackgassen selten:

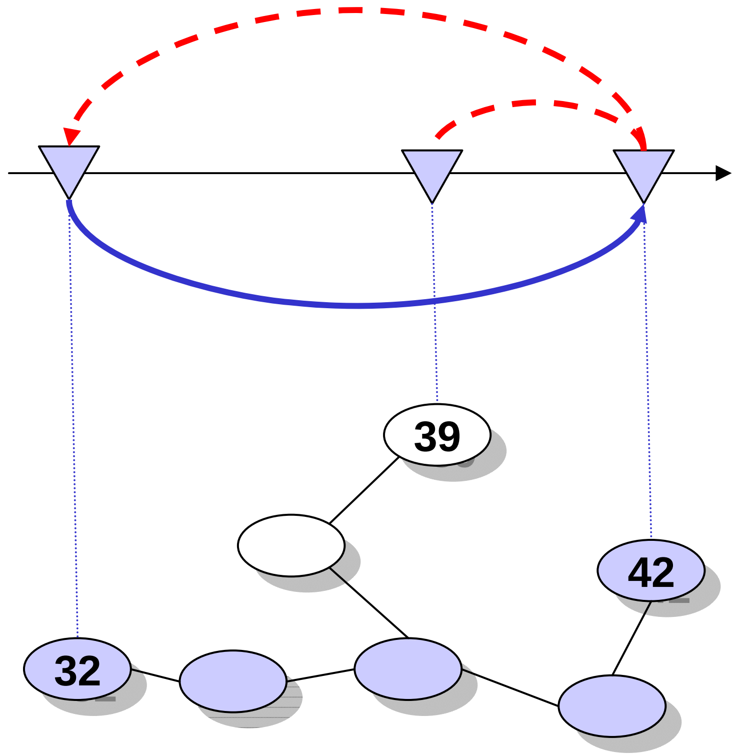
- *Je größer die virtuelle Lücke, desto höher die Wahrscheinlichkeit dass ein physisch naher Knoten die Lücke füllt.*
- *Knoten spezialisieren sich auf ihre virtuelle Nachbarschaft.*

SSR – Selbstorganisation (2)

Nachbarschaftsempfehlungen (indirekte virtuelle Nachbarn)



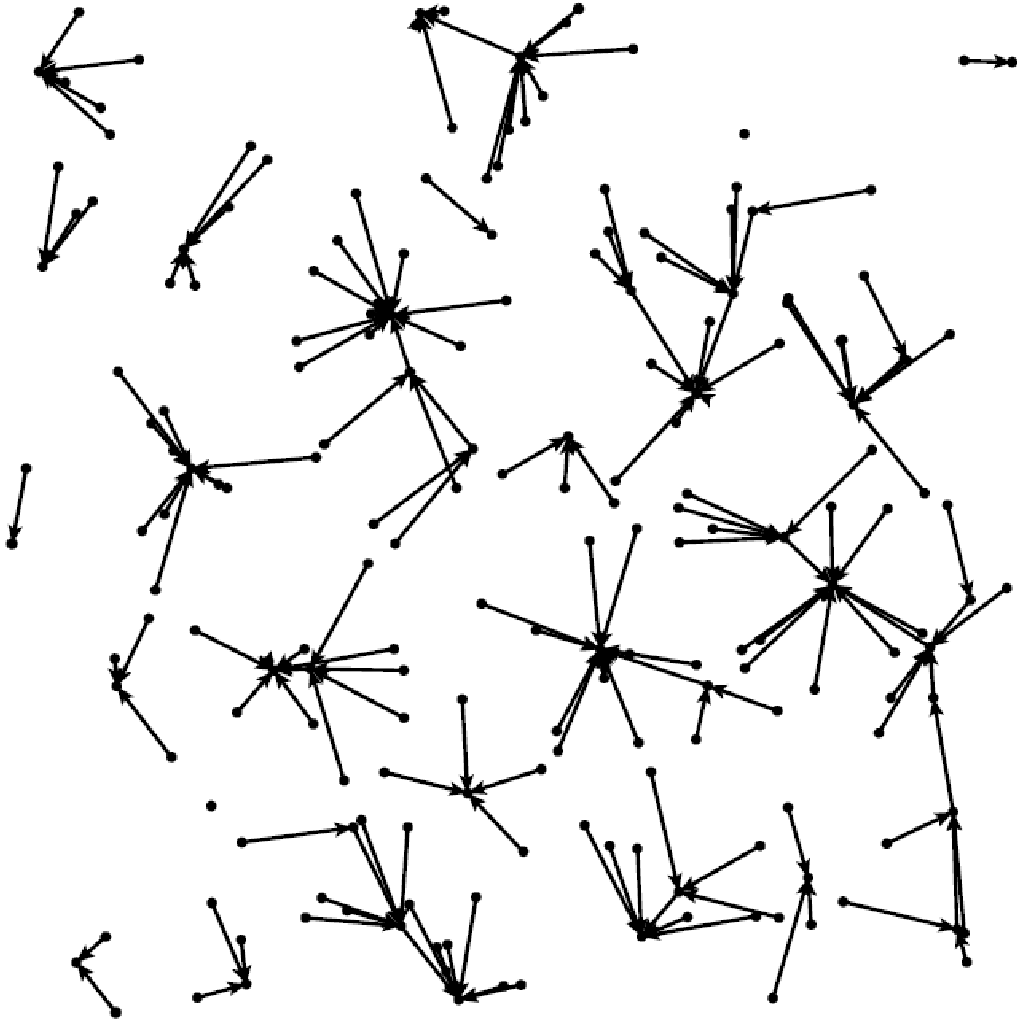
Nachbarschaftsberichtigungen (direkte virtuelle Nachbarn)



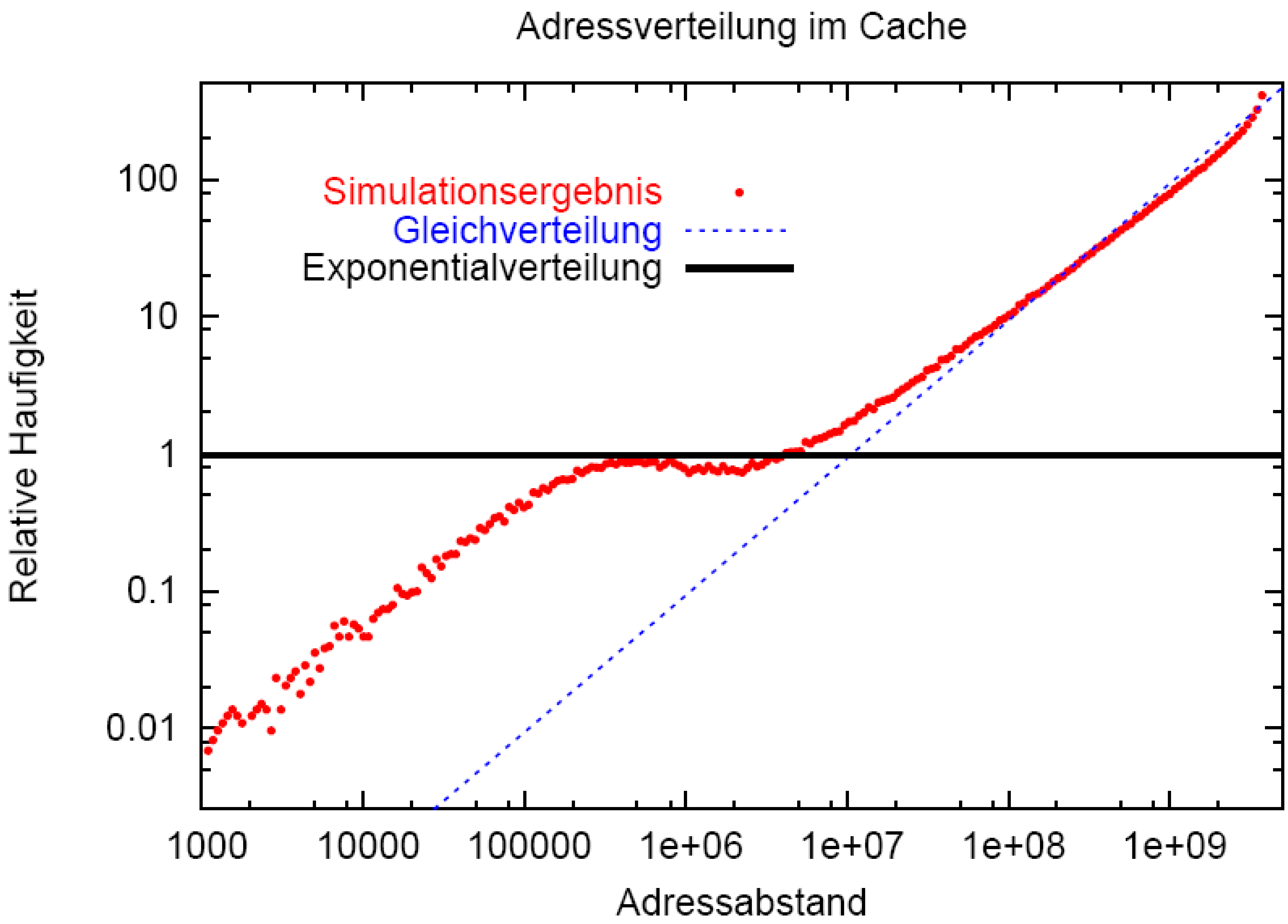
Simulation Results (cont.) – Cluster Formation

Unit disk graph with uniformly random node positions (critical density).

Forwarding to physical neighbor according to routing rule leads to cluster formation.

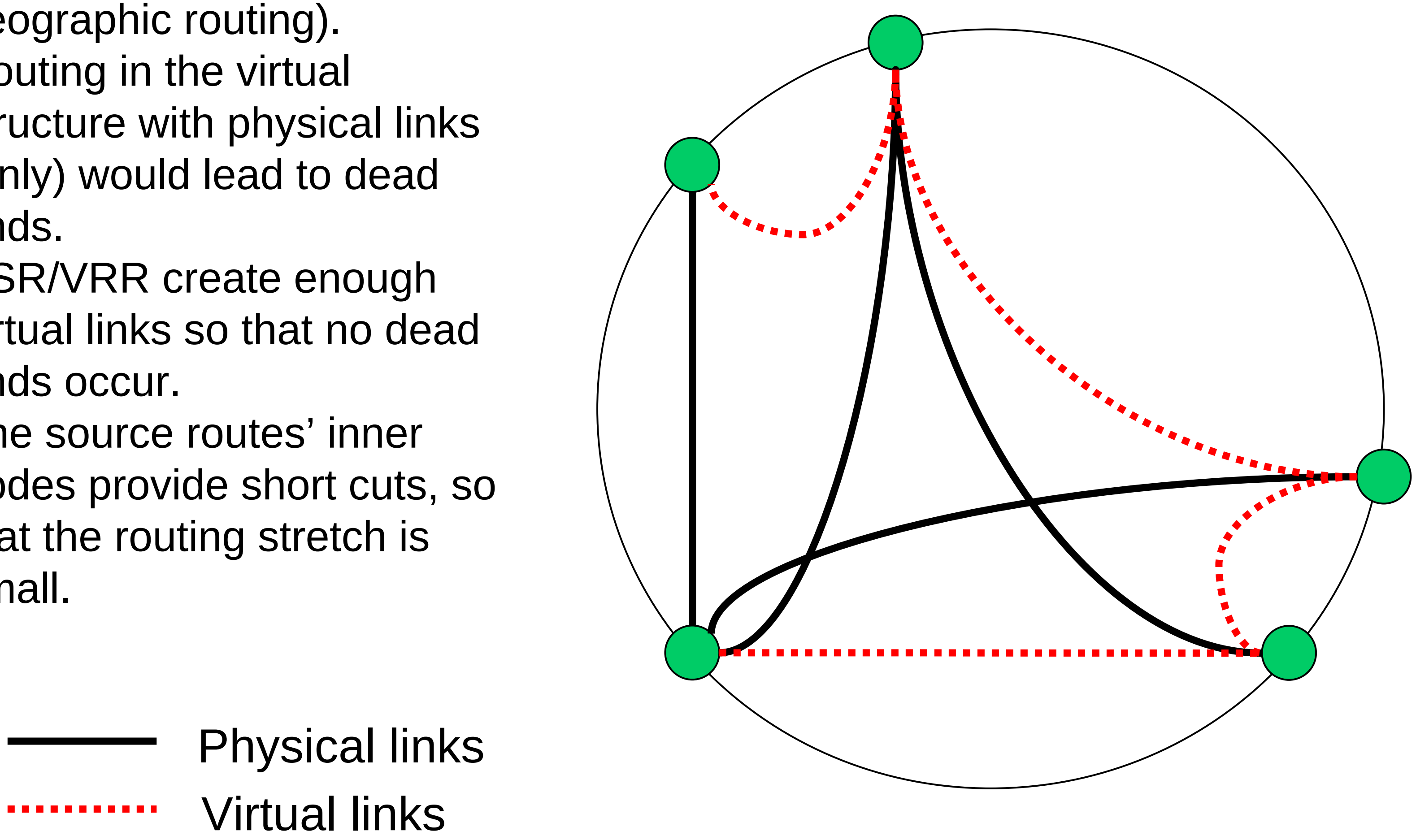


Simulationsergebnisse (cont.) - Adressverteilung

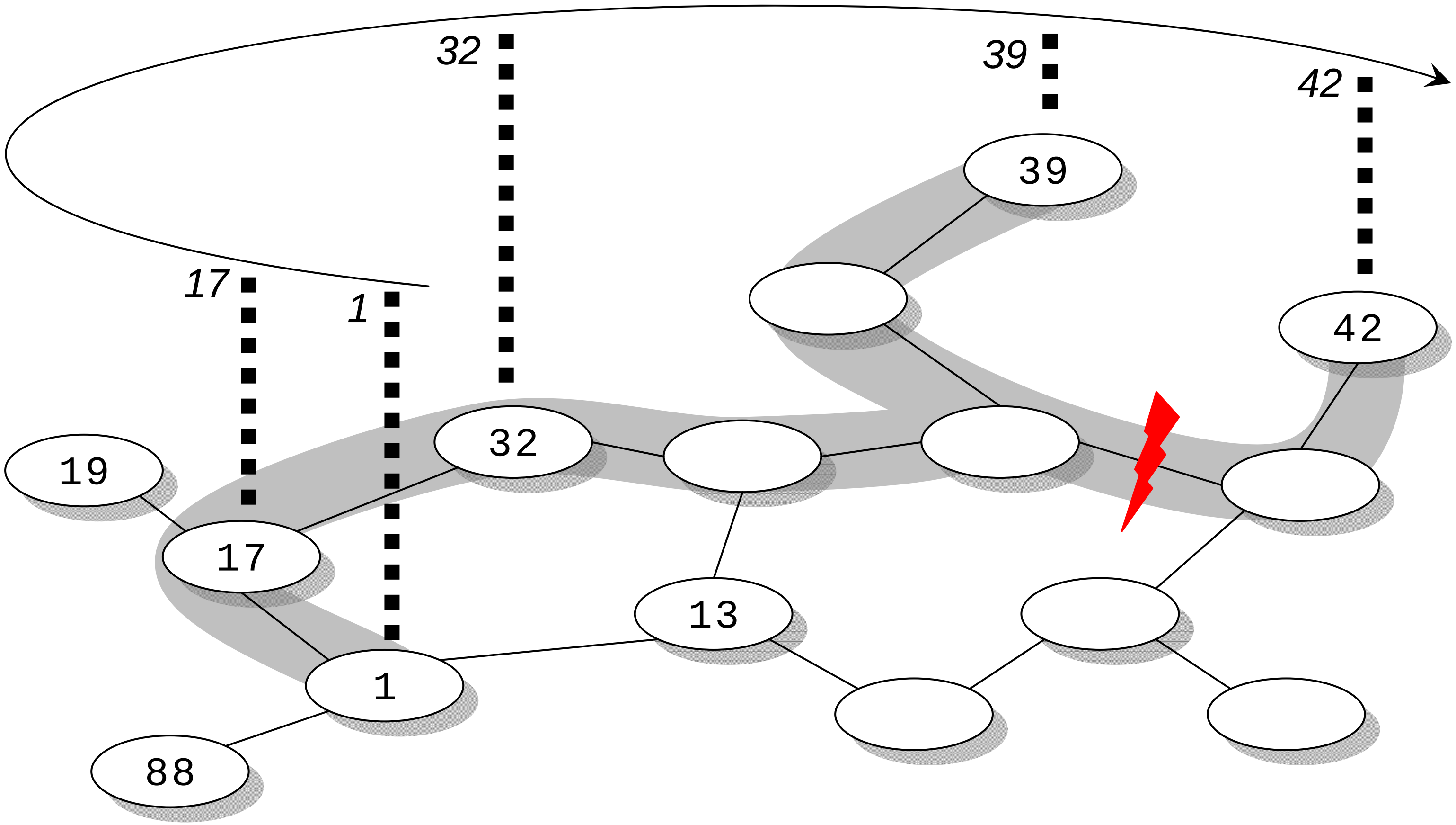


SSR Routing Principle

- Routing in the physical structure is impractical (cf. geographic routing).
- Routing in the virtual structure with physical links (only) would lead to dead ends.
- SSR/VRR create enough virtual links so that no dead ends occur.
- The source routes' inner nodes provide short cuts, so that the routing stretch is small.



Unzuverlässige und Mobile Geräte ...

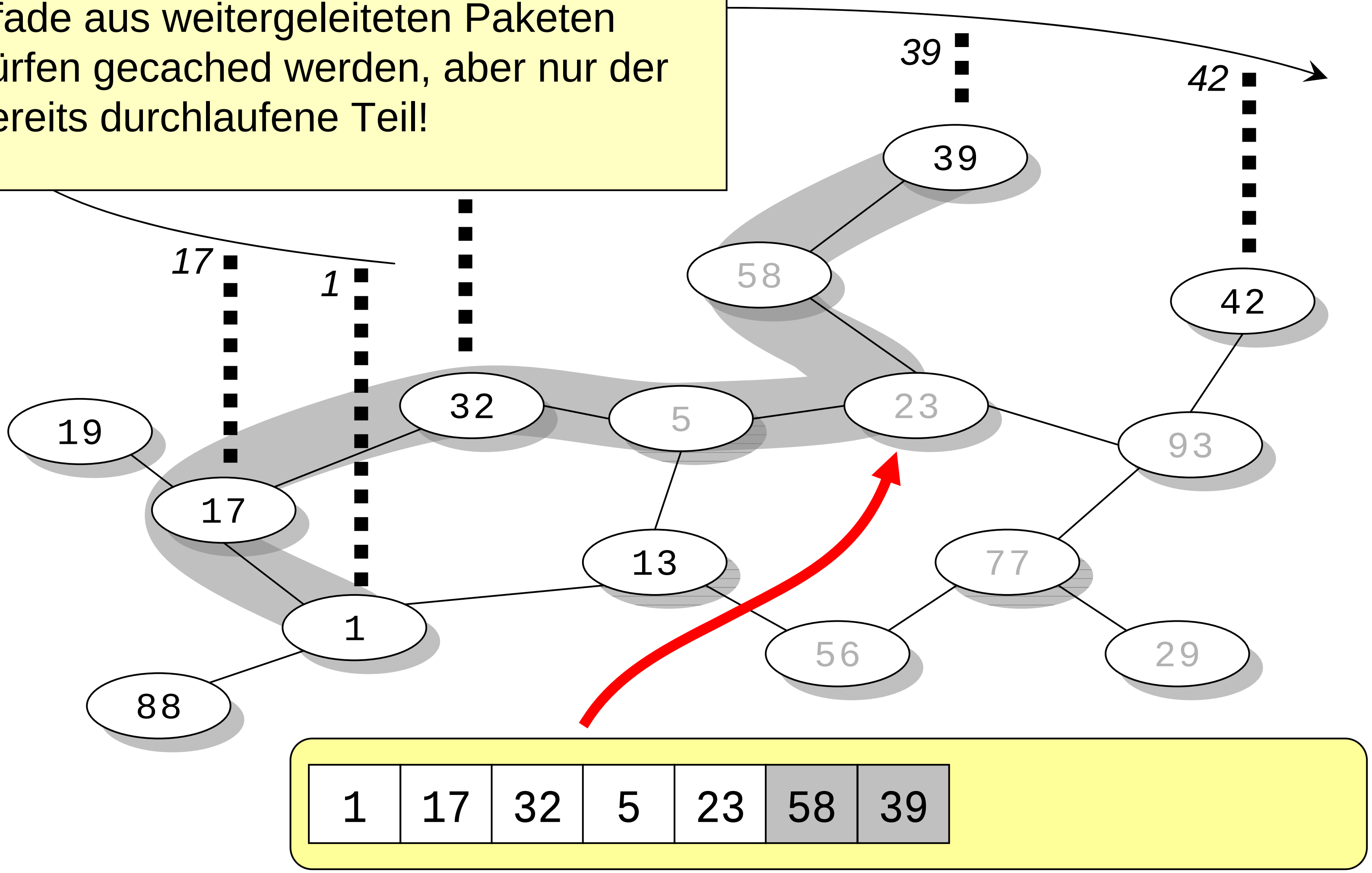


Fuhrmann, Scalable Routing for Sensor Actuator Networks with Churn, SECON 2006.

Fuhrmann et al. Scalable Routing for Hybrid MANETs, WONS 2007

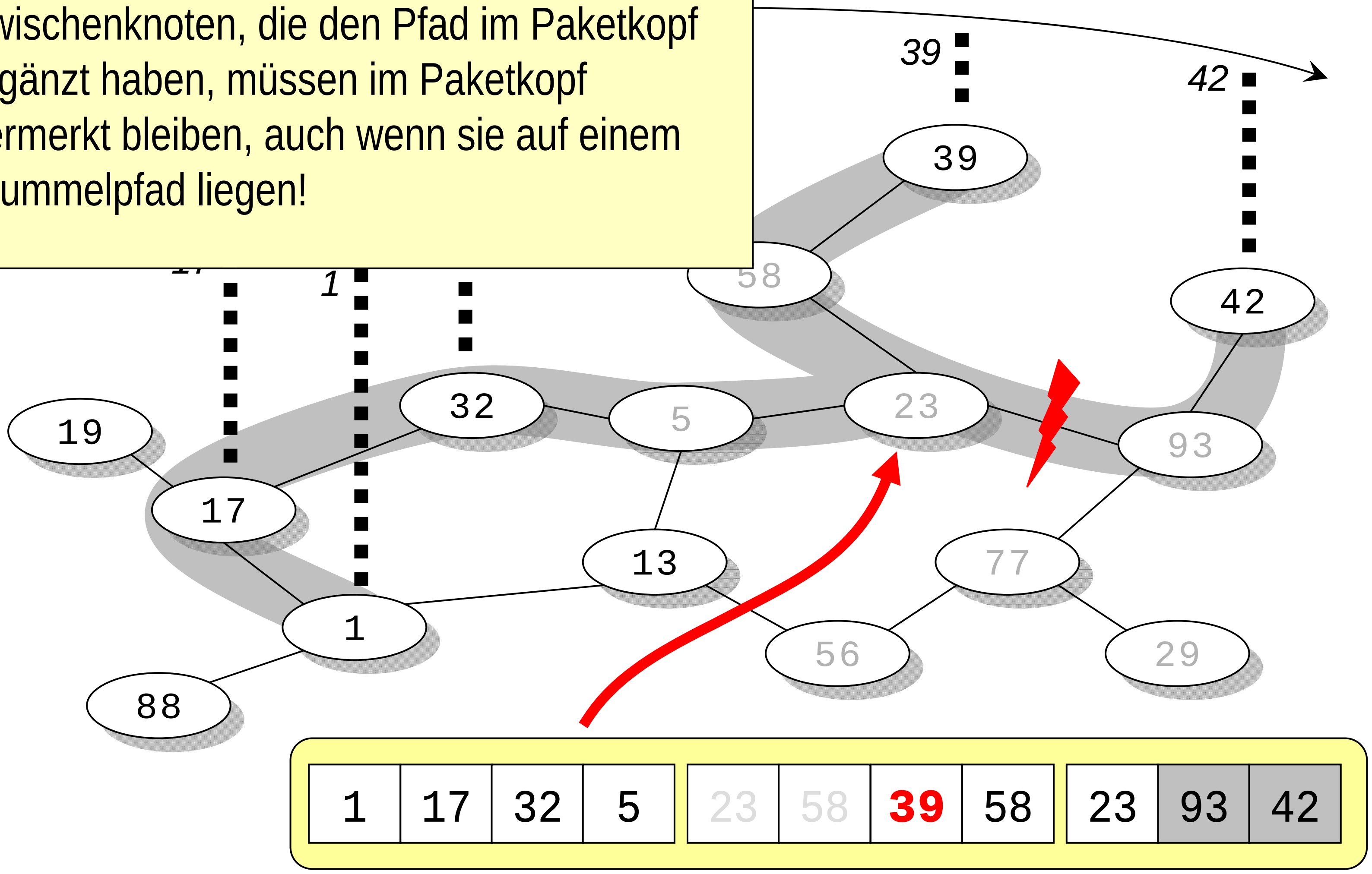
Regel 1: Nur authentische Pfade cachen

Pfade aus weitergeleiteten Paketen dürfen gecached werden, aber nur der bereits durchlaufene Teil!



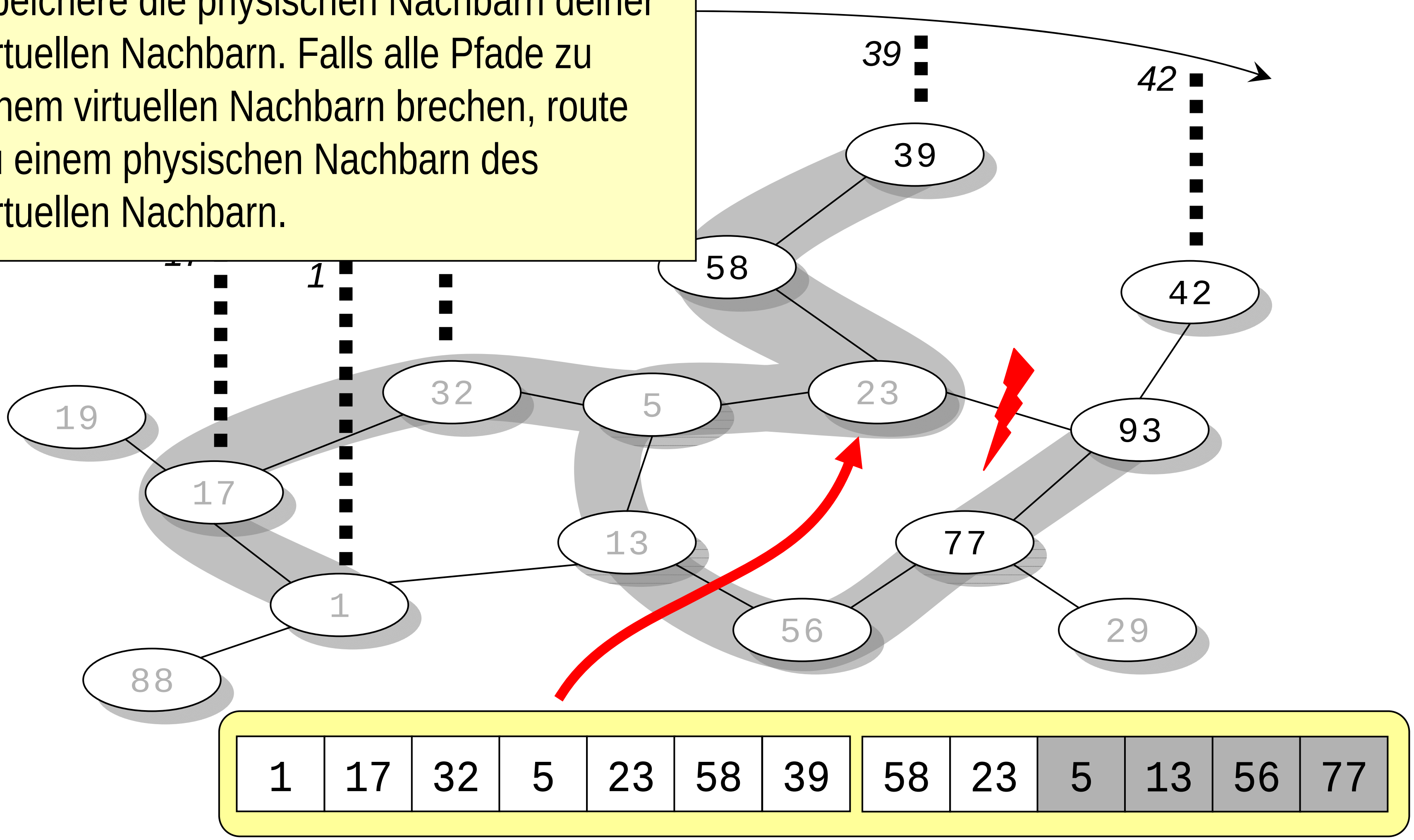
Regel 2: Zwischenknoten behalten

Zwischenknoten, die den Pfad im Paketkopf ergänzt haben, müssen im Paketkopf vermerkt bleiben, auch wenn sie auf einem Stummelpfad liegen!

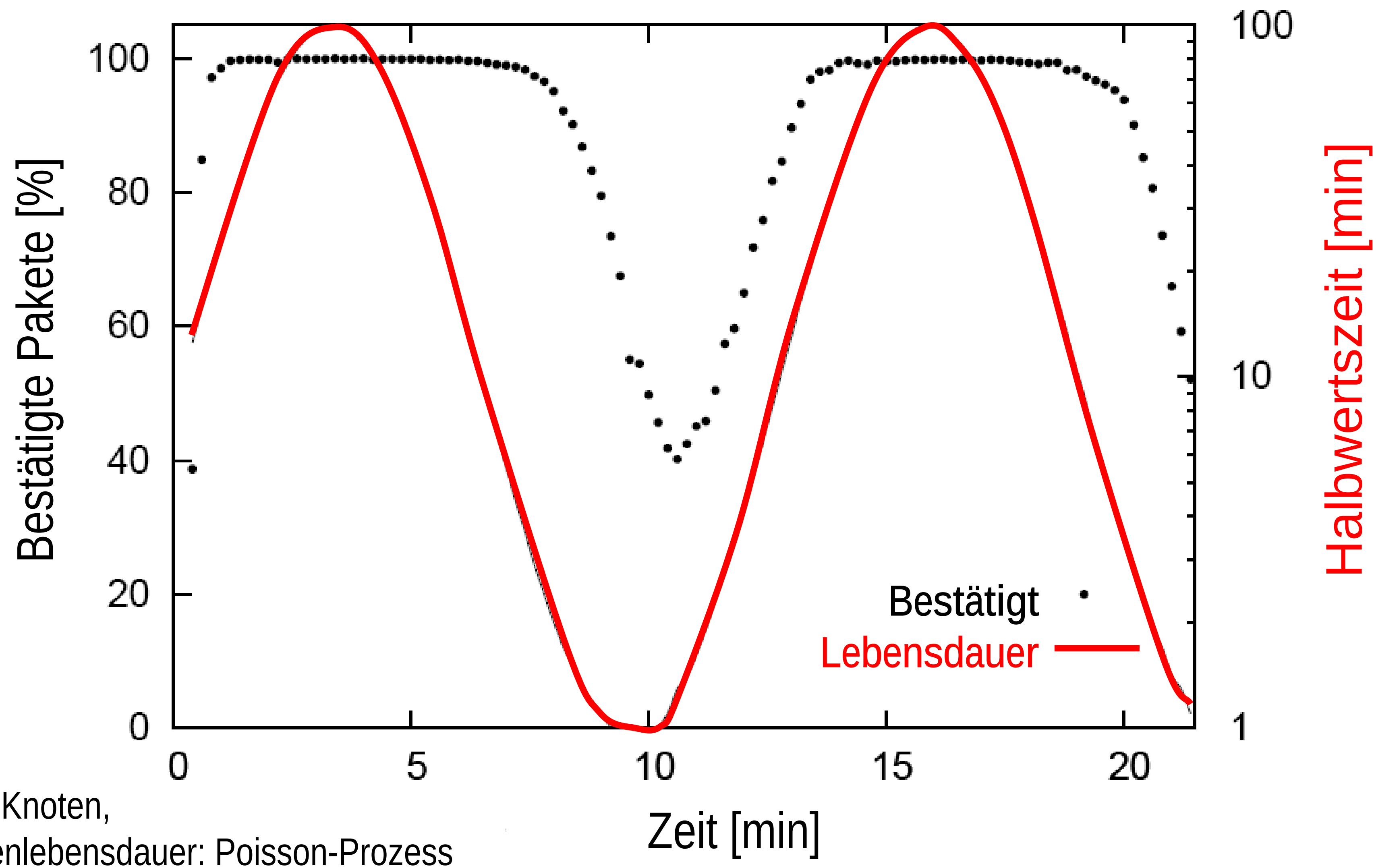


Regel 3: Physische Nachbarn mitbenutzen ...

Speichere die physischen Nachbarn deiner virtuellen Nachbarn. Falls alle Pfade zu einem virtuellen Nachbarn brechen, route zu einem physischen Nachbarn des virtuellen Nachbarn.

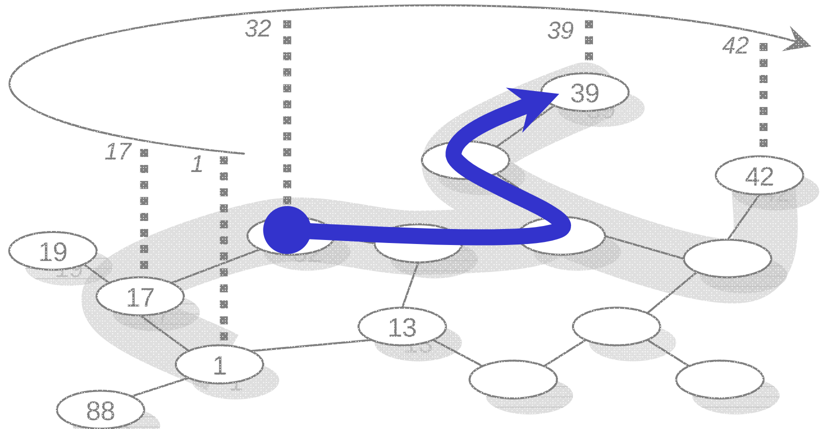


Simulationsergebnisse (cont.) – Node Churn

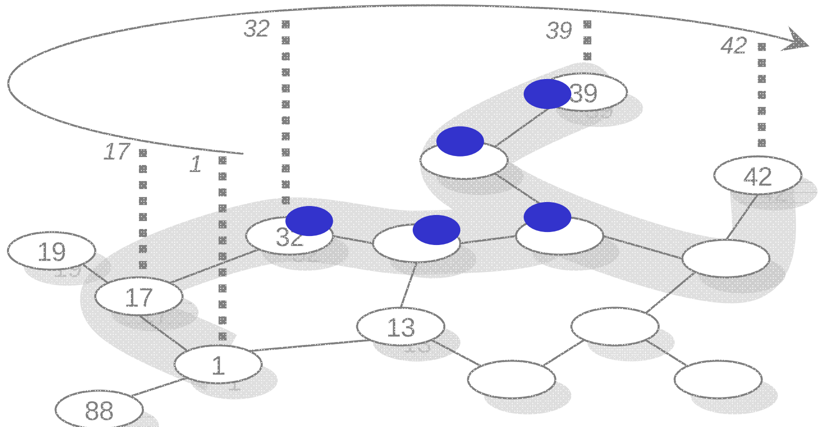


8000 Knoten,
Knotenlebensdauer: Poisson-Prozess

Vergleich SSR und VRR



Fuhrmann, SSR, Networking 2005



Caesar et al. , VRR, SIGCOMM 2006

- Source Routen
- Zustand pro Knoten beschränkt
- Große Paketköpfe durch Source Routen (Reduktion auf lokale Interface IDs mögl.)
- Konsistenz ohne Fluten (neues Verfahren, früher ISPRP vgl. VRR Rep.)

- Tabellen mit Pfadeinträgen
- Zustand pro Knoten potentiell unbeschränkt
- Kleine Paketköpfe
- Konsistenz durch Fluten von Repräsentanten IDs

Vergleichssimulationen zeigen leichten Vorteil von SSR solange Bandbreite nicht saturiert. Zustandbeschränkung bei SSR könnte für Realisierung in Hardware vorteilhaft sein.

Wireless Sensor Networks (WSN)

WSN – A New Perspective on Networks

- Self configuring systems that adapt to unpredictable environment
  - Dynamic, often unpredictable environments preclude pre-configured behavior

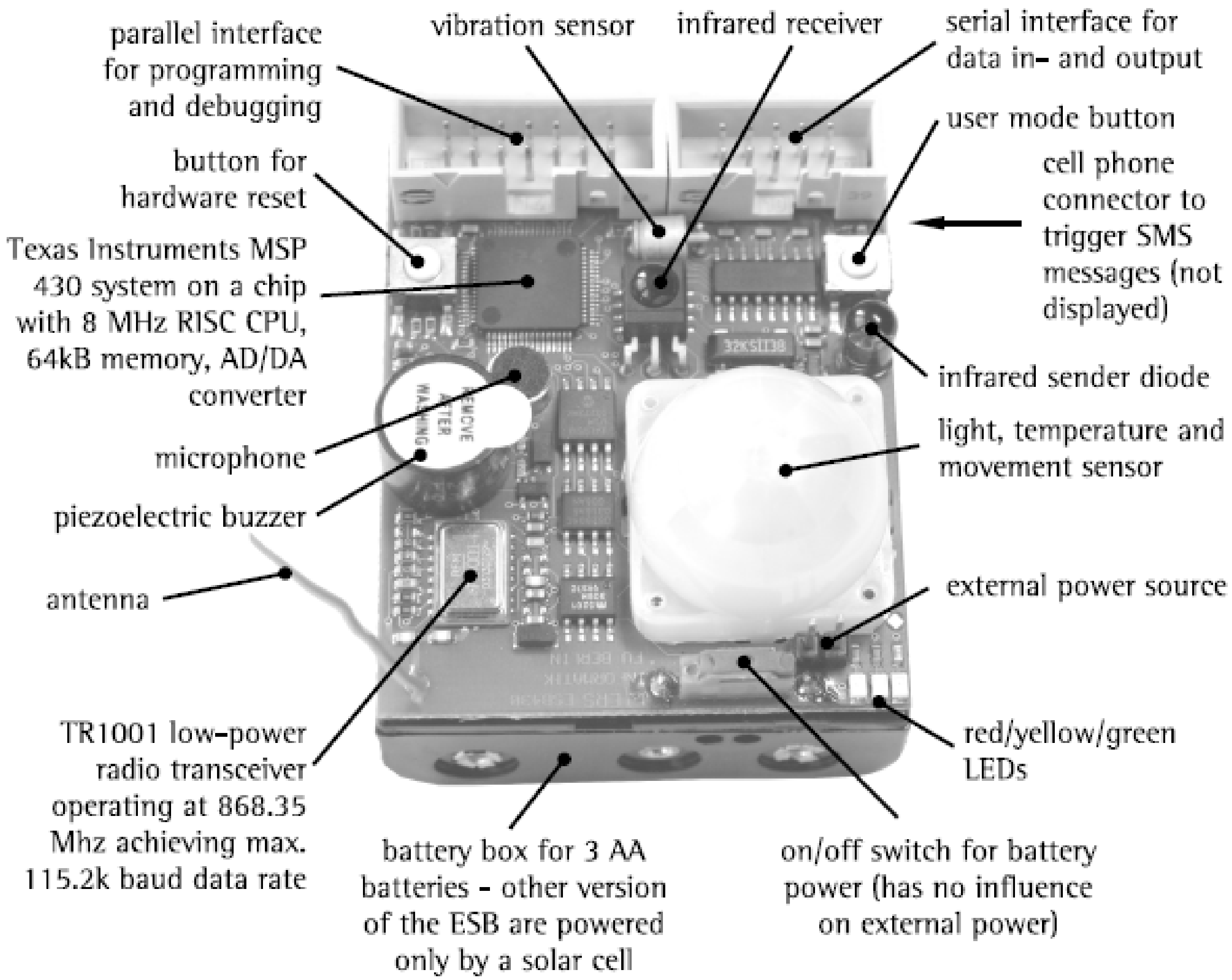
- Leverage data processing inside the network
  - exploit computation near data to reduce communication
  - collaborative signal processing
  - achieve desired global behavior with localized algorithms (distributed control)

- Long-lived, unattended systems
  - energy is a central concern
  - communication is often the primary consumer of energy

WSN Needs a Holistic Approach

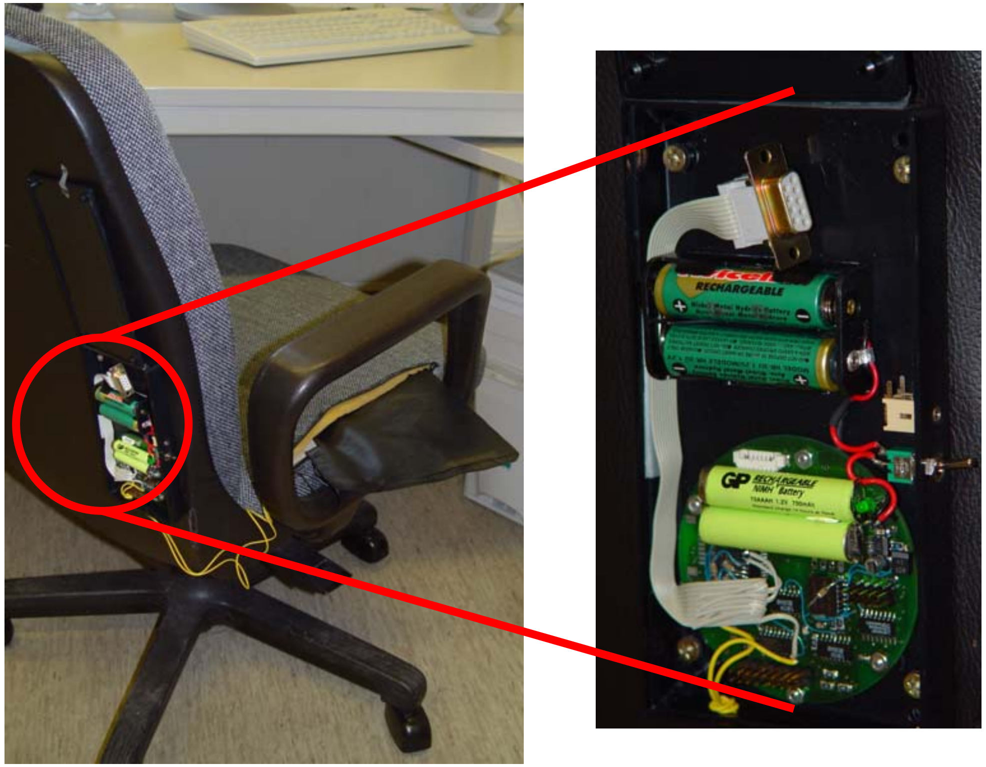
- Embedded in unattended “control systems”
  - Need to act in an environment
- Applications beyond sensing to control and actuation
  - Need application knowledge in system design, e.g. in transportation, precision agriculture, medical monitoring and battlefield app’s
  - Concerns extend beyond traditional networked systems: usability, reliability, safety
- Need systems architecture to manage interactions
  - Layered approach often not sufficient
  - Energy trade-off between computation and communication
  - Often no operating system available

Sensor Network Board



Source: Thomas Haenselmann, FU Berlin

Examples: BlueChair and BlueCUP

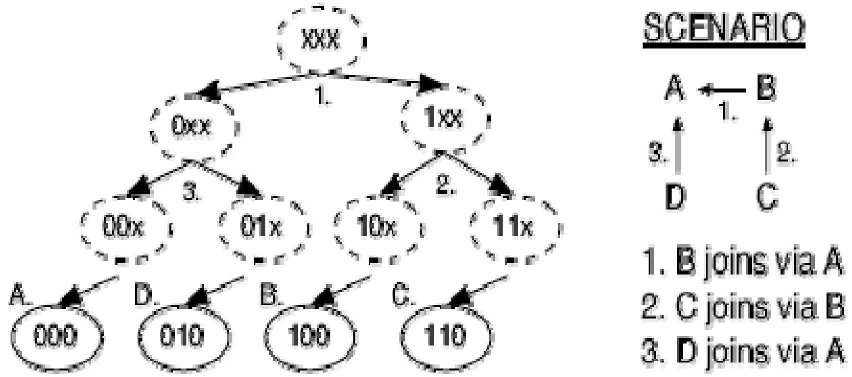


Address Assignment

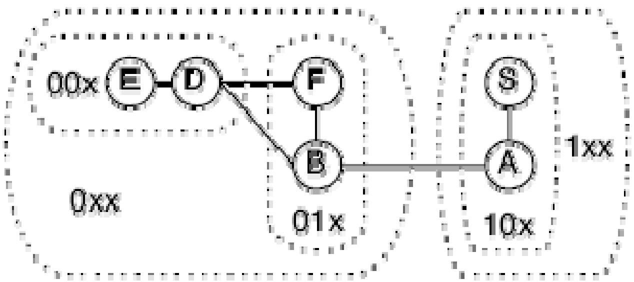
- Assumptions of the node ID in many WSN applications
  - Unique
  - Fixed-length
  - Random
- Problems
  - packet header overhead: Some wireless MAC protocols support only very short frame
  - Independency of physical position and node identification leads to scalability issues (cf. SSR/VRR).
- Example PeerNet [1]: Pushing Peer-to-Peer Down the Stack
  - Separation of the identity and the address
  - Node requests address from a physical neighbor
  - O(logN) state per node for routing
- SIDA [2]: Self-organized ID Assignment in WSN
  - The traffic from remote node causes more traffic.
  - The more distant a node is, the short ID it should have.

Address Assignment Example: PeerNet (1)

- Address Allocation
  – First node has address 000 and manages a range of address from 000 to 111.
  – When asked for address from new coming node, the node slits its address range in half



- Routing table
  – Each node has log(N) routing table entries, which point to its log(N) siblings in the log(N) levels.
    - 1xx is the level-2 sibling of 0xx.
    - 00x is the level-1 sibling of 01x.



ADDRESSES AND ROUTING TABLES

Node D = 001
Level 2 : B
Level 1 : F
Level 0 : E

Node S = 101
Level 2 : A
Level 1 : -
Level 0 : A

Node B = 010
Level 2 : A
Level 1 : D
Level 0 : F

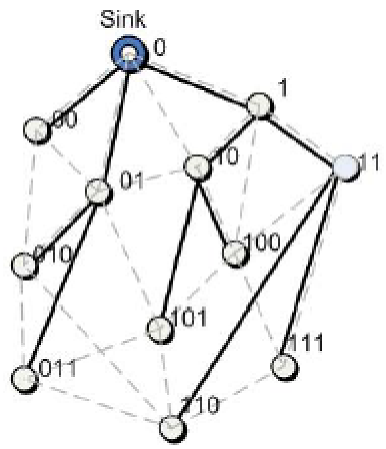
Node A = 100
Level 2 : B
Level 1 : -
Level 0 : S

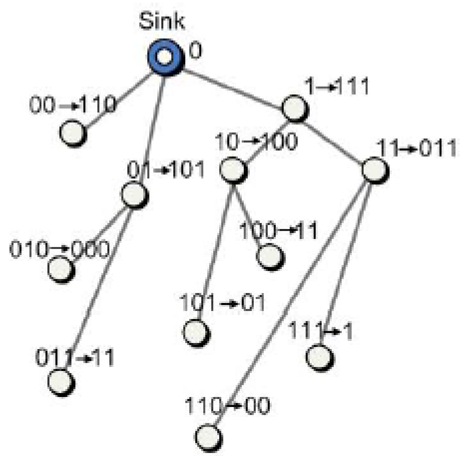
Address Assignment Example: PeerNet (2)

- Routing Process
  - A node compares its own address and the destination one bit at a time. (from the most significant bit)
  - If i-th bit differs, the packet will be forwarded to the i-th sibling.
- Drawbacks
  - Address may change
  - Lookup service is needed

Address Assignment Example: SIDA

- SIDA [2]: Self-organized ID Assignment in WSN
  - The traffic from remote node causes more traffic.
  - The more distant a node is, the short ID it should have.
- Temporary addresses assigned in binary tree.
  - The more faraway nodes to sink has long bit of address
- Permanent address conversion
  - The more faraway nodes to sink has short address





Path Selection Metrics (1)

- Hop Count
  - is the most commonly used metric in routing protocols, e.g.,AODV, RIP. These routing protocols using hop count as metric imply that the links have similar properties in the network. If the link property, e.g., capacity varies largely, this metric won't result in good performance.
- Bandwidth
  - lets the high-capacity links to have smaller weights and be more attractive to be selected.
- Expected Transmission Count (ETX)
  - is the expected total transmission count along the path. Since some link could be lossy, and it cannot be indicated by hop count, ETX is used to capture this characteristic of wireless links.

Path Selection Metrics (2)

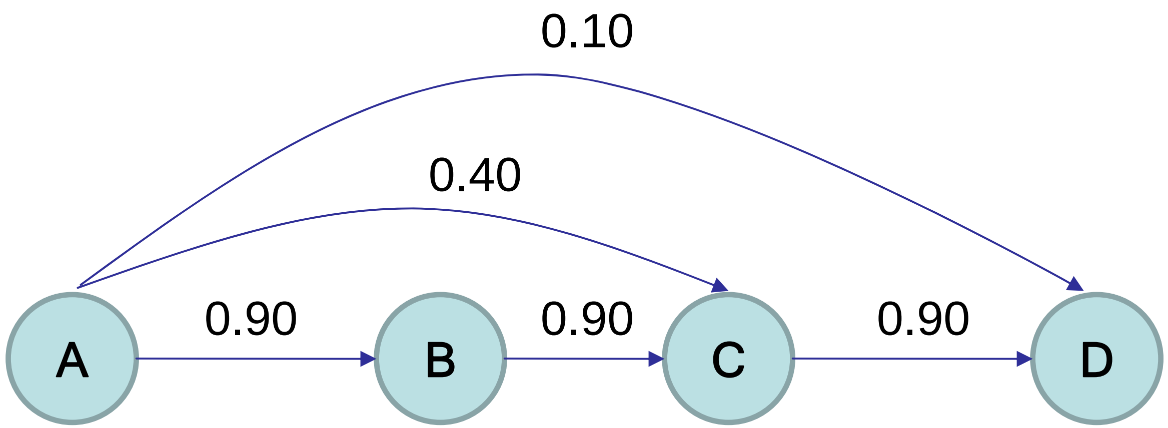
- Expected Transmission Time (ETT)
  - is proposed to improve ETX metric with the consideration of the different link data rate. However, for a wireless network, the inter- and intra-interference are also important characteristics, which should be considered in the metric.
- Weighted Cumulative ETT (WCETT)
  - was proposed for wireless networks, in which nodes support multiple physical channels. This metric is actually the ETT added by the maximal channel repeat times along the path. If only one channel is used in the network, it is equal to ETT.
- Metric of Interference and Channel-switching (MIC)
  - considers the intra flow interference as well as the inter-flow interference in a wireless network. It contains two parts: Interference-aware Resource Usage (IRU) and Channel Switching Cost (CSC). IRU is defined as ETT weighted by its physical neighbor number; CSC describes how diversified the channels are assigned: the more they are diversified, the higher the metric.

Path Selection Metrics (3)

- Exclusive Expected Transmission Time (EETT[6])
  - improves MIC by taking the fact into account that interference range is always much larger than the transmission range. EETT groups the links into interference sets and sums the ETT for each set. This metric considers just the intra-flow interference rather than inter-flow interference.
- Interference Aware Routing Metric (iAWARE[7])
  - is also an improvement of MIC. MIC considers the inter-flow interference just dependent on the physical neighbor number, while iAWARE also takes the Signal to Interference-plus-Noise Ratio (SINR) from each neighbor into account.
- WCETT-Load Balancing (WCETT-LB[8])
  - is another enhancement of WCETT; it introduces the congestion state of node into the routing metric. The congestion state is in turn represented by the node's relative queue length.

Opportunistic Routing

- In WSN, lossy link is common



Simple network example with delivery ratio

- Diff. metrics result in diff. paths
- Pre-determined routes work not well in Wireless network
- Wireless link has diff. property with wired link

Opportunistic Routing (1)

- Extremely Opportunistic Routing (ExOR[9])
  - Not using a single route
  - Determining the path on the fly
  - Global knowledge of the link quality
    - Matrix containing the loss rate between every 2 nodes
  - Three stages
    - Selecting the forwarding candidates
    - Acknowledging transmissions
    - Deciding whether to forward a received packet
- Candidates selection
  - Identifying the shortest path to the destination from the matrix
    - Taking also consideration of the link delivery rate
  - The first node in the path as the highest priority candidate
  - Temporarily delete that node from the matrix
  - Find again the shortest path and the node with second highest priority.
  - And so forth.

Opportunistic Routing (2)

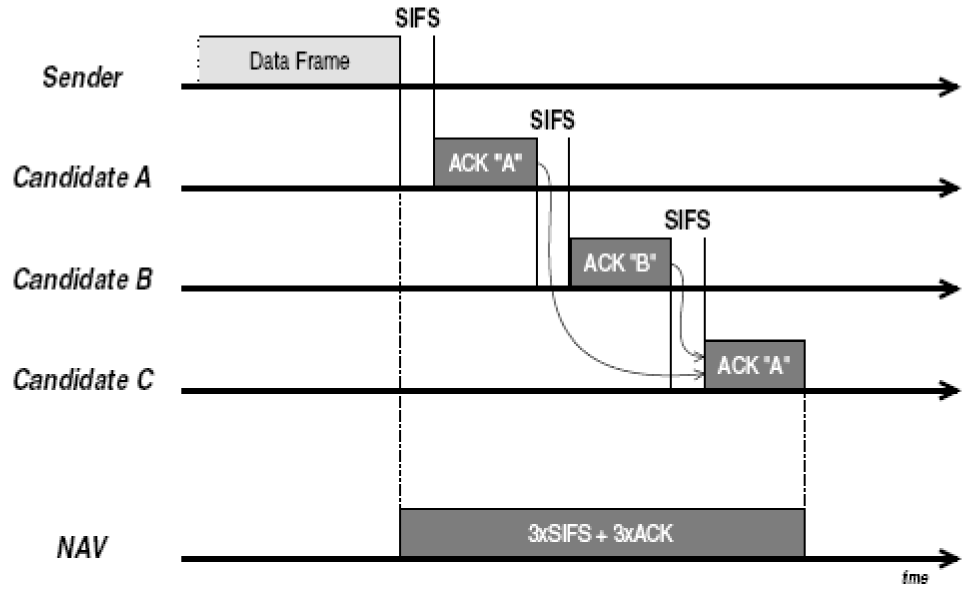


Figure 2: **Typical ExOR acknowledgment sequence.**

- Acknowledgments
  - Modified MAC 802.11
  - Candidate with higher priority answers earlier
  - Each ACK includes the node id with highest priority, which is overheard from other ACKs.

Opportunistic Routing (3)

- Example
  - A wants to send a packet to D
  - "D, C, B" are candidates in the priority order
  - D doesn't received the packet, but B and C do.
  - D sends no ACK,
  - C sends an ACK to A.
    - Suppose this ACK is received by B, but not by A
  - B sends ACK back to A, indicating that C has received that packet.
  - A received ACK from B
  - Now C forwards the packet
  - B discard the packet

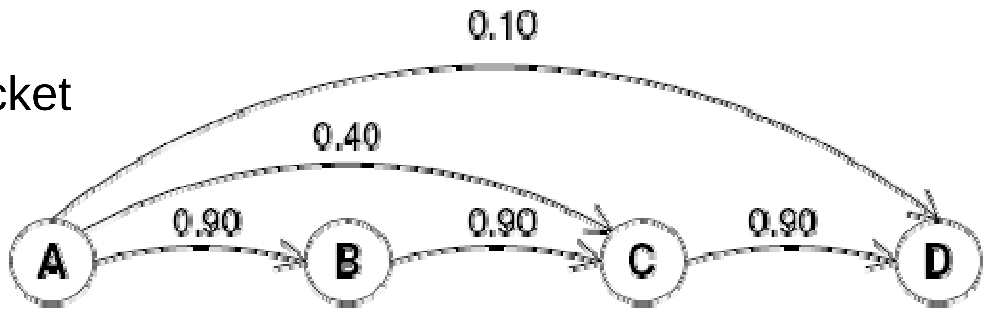


Figure 1: Simple network example, with delivery ratios.

Questions?

Thomas Fuhrmann

Department of Informatics
Self-Organizing Systems Group
c/o I8 Network Architectures and Services
Technical University Munich, Germany

fuhrmann@net.in.tum.de