Ad Hoc Networking

Christian Bettstetter (TU München)
Hannes Hartenstein (NEC Europe / Universität Karlsruhe)
Martin Mauve (Universität Düsseldorf)

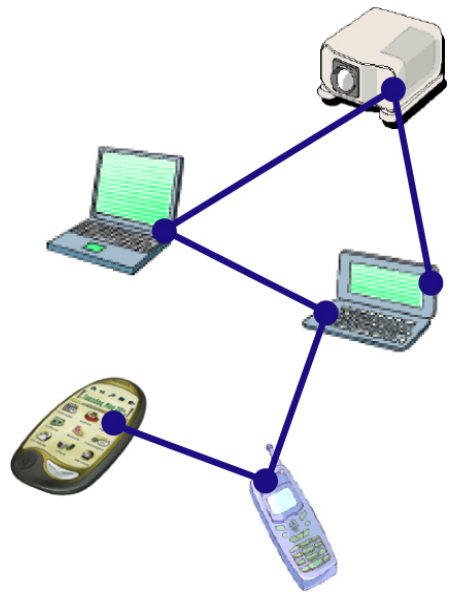
christian.bettstetter@ei.tum.de
hannes.hartenstein@ccrle.nec.de
mauve@cs.uni-duesseldorf.de

Principles, Applications, and Challenges

Christian Bettstetter, TU München

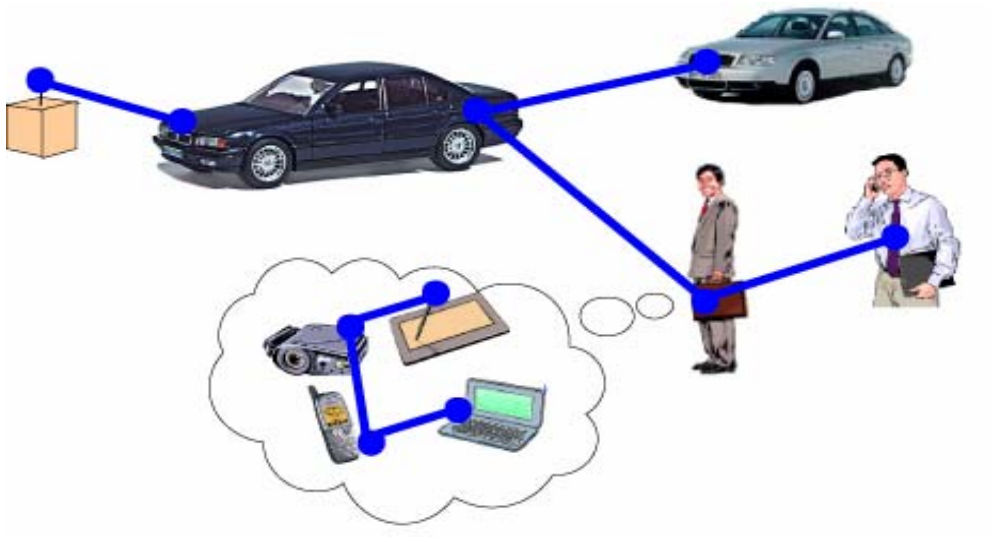
The Basic Principle of Ad Hoc Networking

- Mobile device communicate in peer-to-peer fashion
- Self-organizing network without the need of fixed network infrastructure
- Multi-hop communication
- Decentralized, mobility-adaptive operation



"The art of networking without a network"
[Frodigh et al.]

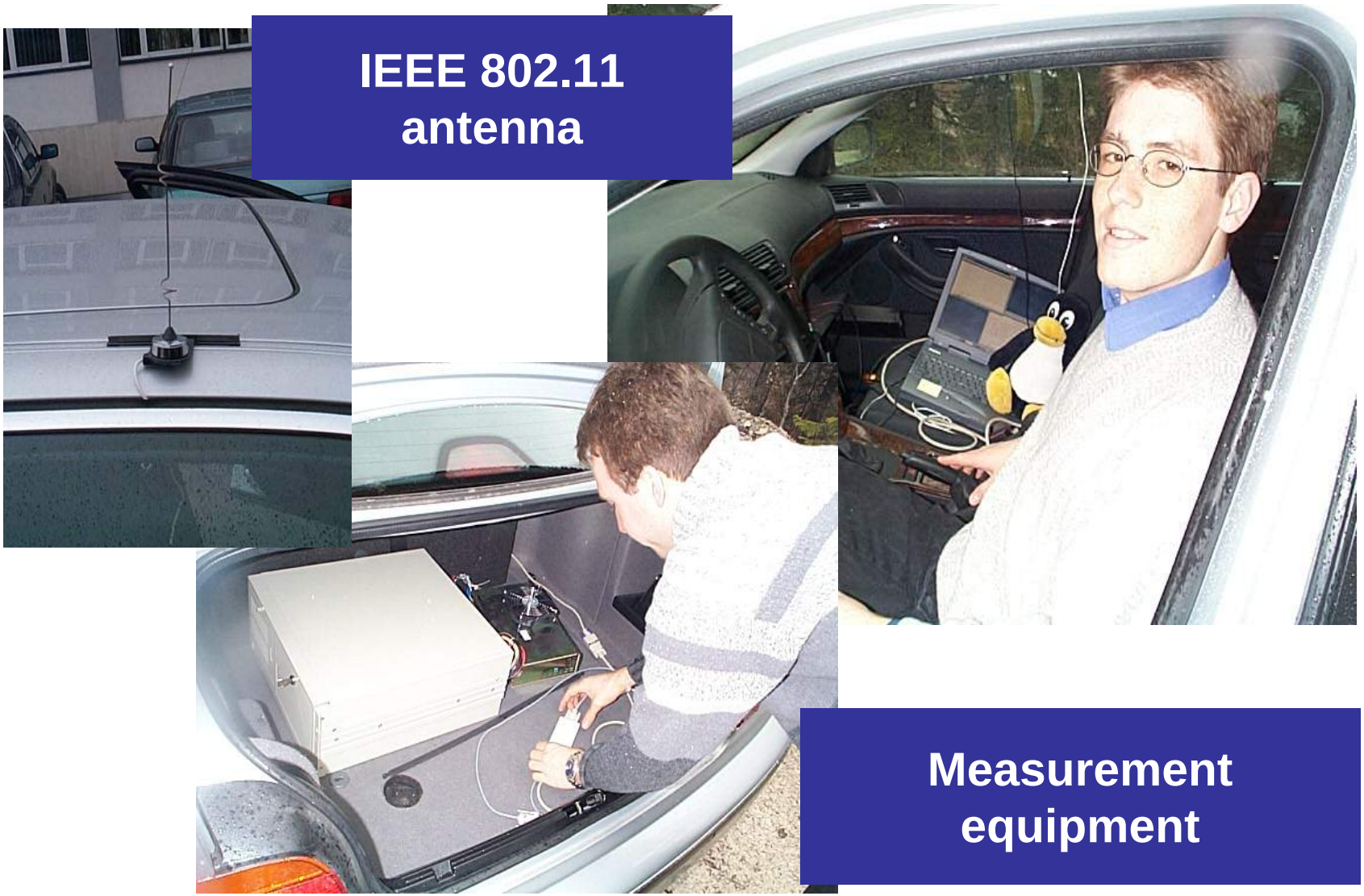
Applications: Vehicular Networks



Applications

- Accident warning
- Floating car data
- Multihop extensions of Infostations

Field experiment: TUM and BMW

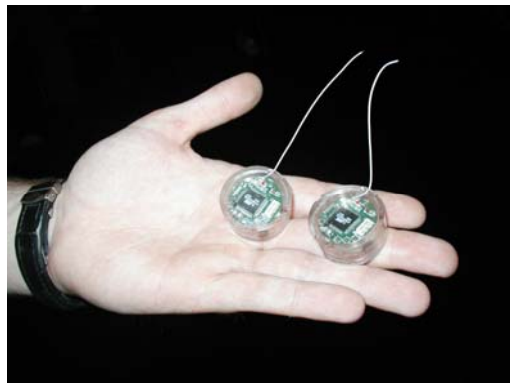


Pictures by Ch. Schwingenschlögl and T. Kosch

Applications: Wireless Sensor Networks

Tiny, low-power sensors

- measure temperature
- detect vibrations
- detect chemical substances
- make photos
- ...



UC Berkeley

Applications: Wireless Sensor Networks

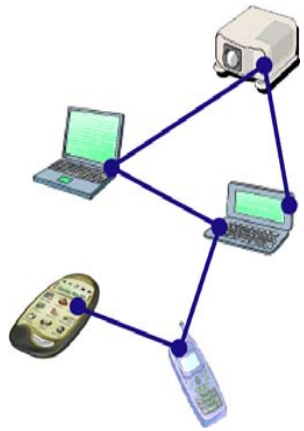
Applications

- Environmental monitoring (“sensor dust”): habitat monitoring
- Emergency sector: intrusion detection, detection of bushfires, earthquake warning
- Medical sector: monitoring of body functions and implants
- Biological sector: animal tracking, undersea exploration
- Industrial sector: remote sensing in power plants
- Home automation: remote monitoring of electricity, water, gas
- Aerospace sector: sensor-equipped robots on a planet

MIT Technology Review, Feb 2003:
“Top 10 technologies that will change our world”

Ad Hoc Networks: Pros and Cons

Key Advantages

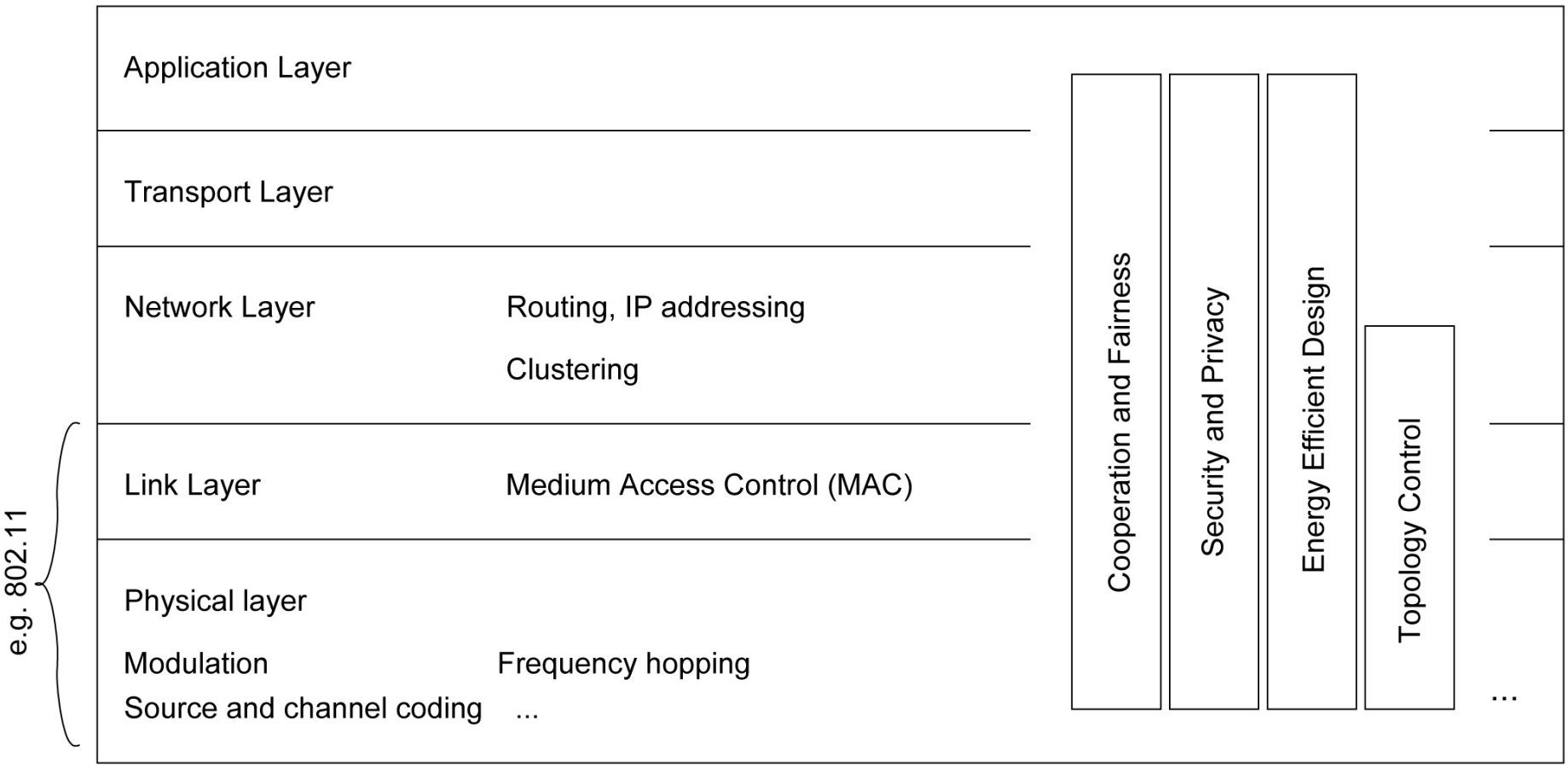


- No expensive infrastructure must be installed
- Use of unlicensed frequency spectrum
- Quick distribution of information around sender

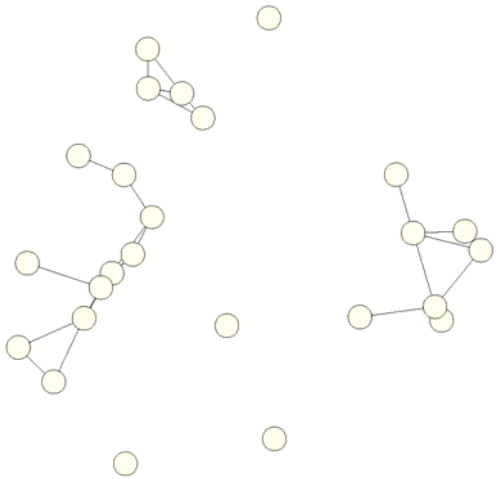
Key Challenges

- All network entities may be mobile $\Rightarrow$ very dynamic topology
- Network functions must have high degree of adaptability (mobility, outage)
- No central entities $\Rightarrow$ operation in completely distributed manner

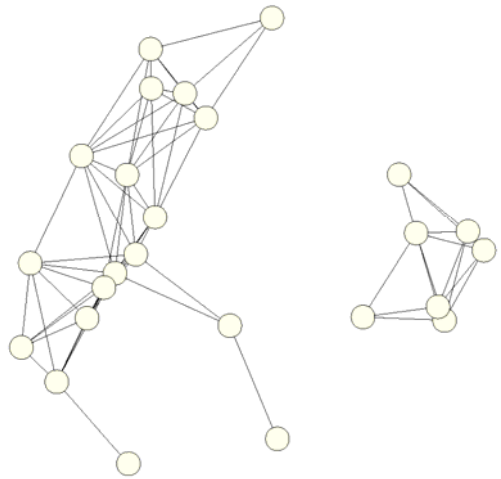
Research Issues on All Layers



High versus low transmission power



(a) Ad hoc network with low transmission power



(b) Ad hoc network with high transmission power

Transmission power	low	high
Interference between nodes	low	high
Spatial reuse of radio resources	good	bad
Number of hops from source to dest.	many	few
Relaying load per node	high	low
Message queuing delay from source to dest.	high	low
Connectivity	bad	good

from C. Bettstetter PhD thesis

Outline of the Remainder of the Tutorial

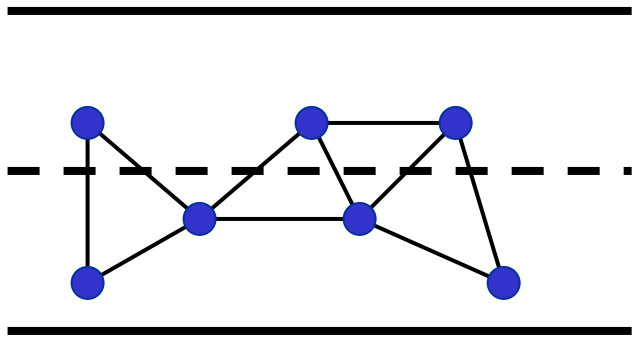
- Routing
- Information diffusion in sensor networks
- Medium access control (MAC)
- Security
- Clustering
- Connectivity
- Interworking with fixed IP networks
- Future research directions

(Topology-based) Routing in Mobile Ad Hoc Networks

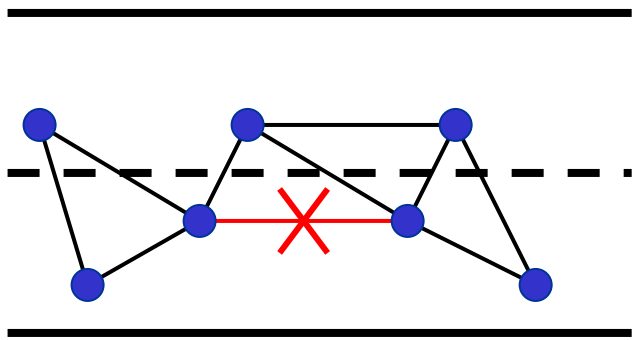
Martin Mauve, University of Düsseldorf

Why is Routing for Ad-Hoc Networks a Problem?

- Well known from the Internet:
  - link state routing (OSPF)
  - distance vector routing (RIP)
- Proactive approach:
  - always maintain all routes



- Problem:
  - topology changes ⇒ significant network traffic
  - even when the route is not used



Flooding!

Unicast Routing Protocols

- Many protocols have been proposed
- Some have been invented specifically for MANETs
- Others are adapted from previously proposed protocols for wired networks
- No single protocol works well in all environments
  - some attempts made to develop adaptive protocols

Routing Protocols

- Proactive protocols
  - Determine routes independent of traffic pattern
  - Traditional link-state and distance-vector routing protocols are proactive
- Reactive protocols (this tutorial)
  - Maintain routes only if needed
- Hybrid protocols
  - Combine proactive and reactive elements
- Position-based (this tutorial)
  - Use the geographic position of nodes for forwarding decisions

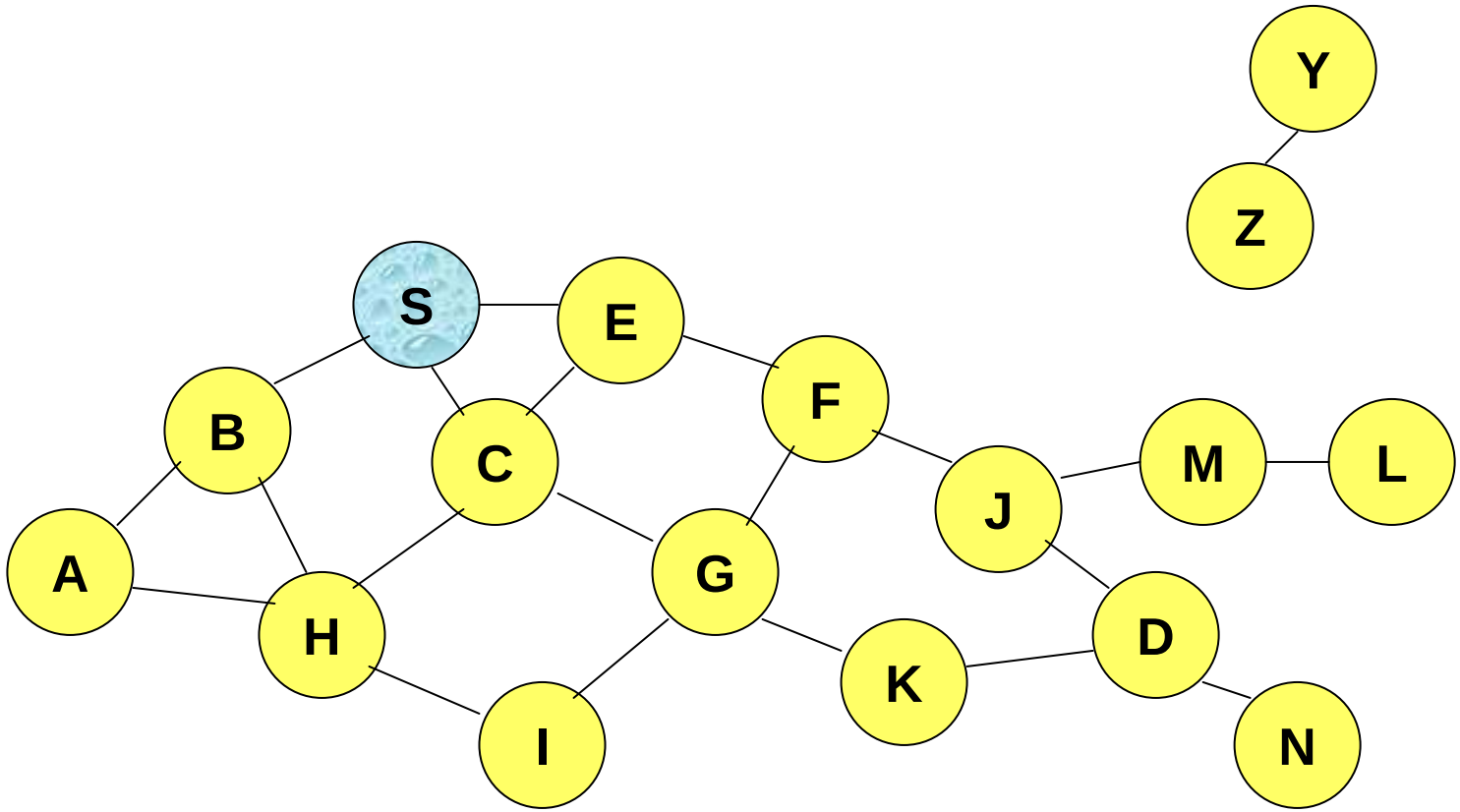
Trade-Off

- Latency of route discovery
  - Proactive protocols may have lower latency since routes are maintained at all times
  - Reactive protocols may have higher latency because a route from X to Y will be found only when X attempts to send to Y
- Overhead of route discovery/maintenance
  - Reactive protocols may have lower overhead since routes are determined only if needed
  - Proactive protocols can (but not necessarily) result in higher overhead due to continuous route updating
- Which approach achieves a better trade-off depends on the traffic and mobility patterns

Flooding for Data Delivery

- Sender S broadcasts data packet P to all its neighbors
- Each node receiving P forwards P to its neighbors
- Sequence numbers used to avoid the possibility of forwarding the same packet more than once
- Packet P reaches destination D provided that D is reachable from sender S
- Node D does not forward the packet

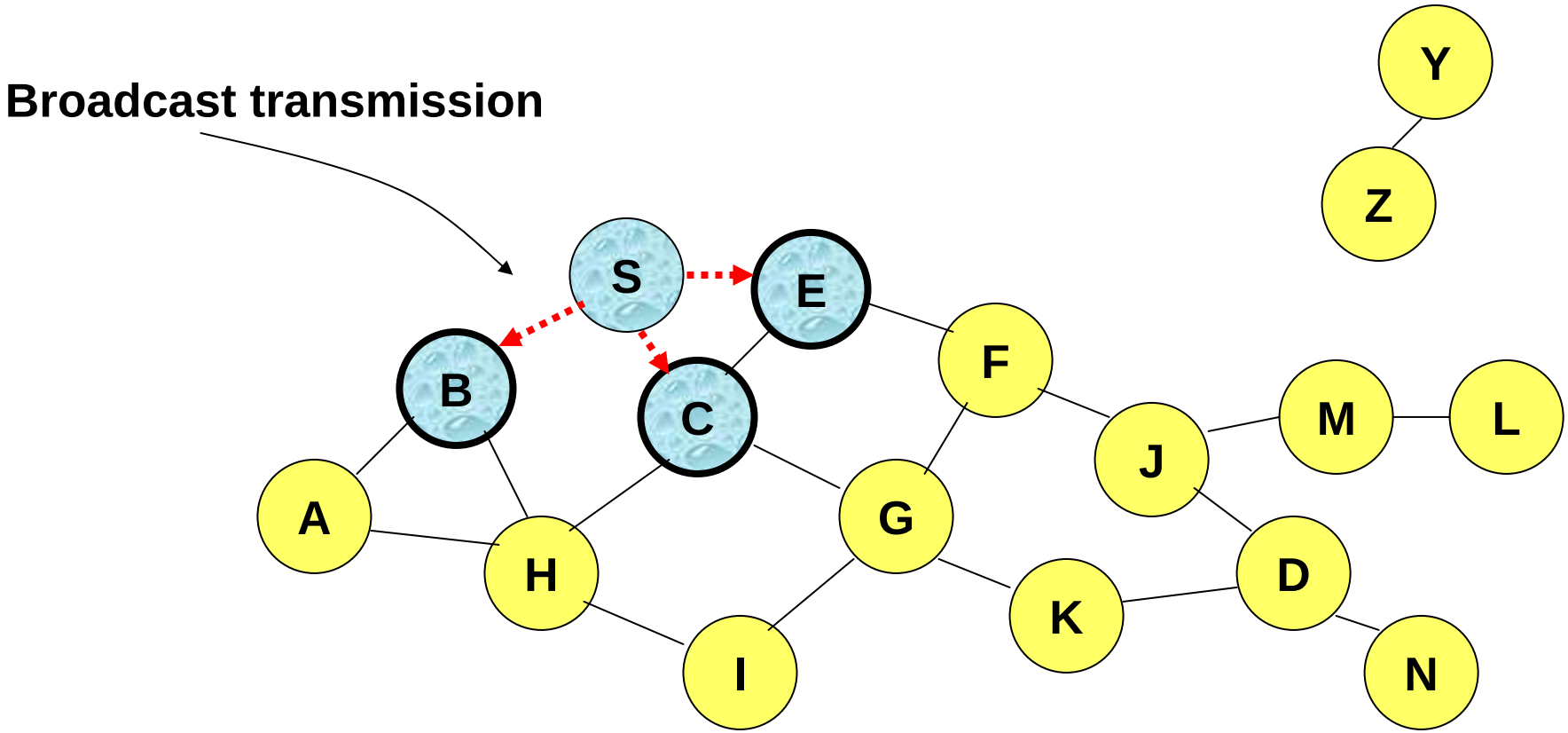
Flooding for Data Delivery



Represents a node that has received packet P

Represents that connected nodes are within each other's transmission range

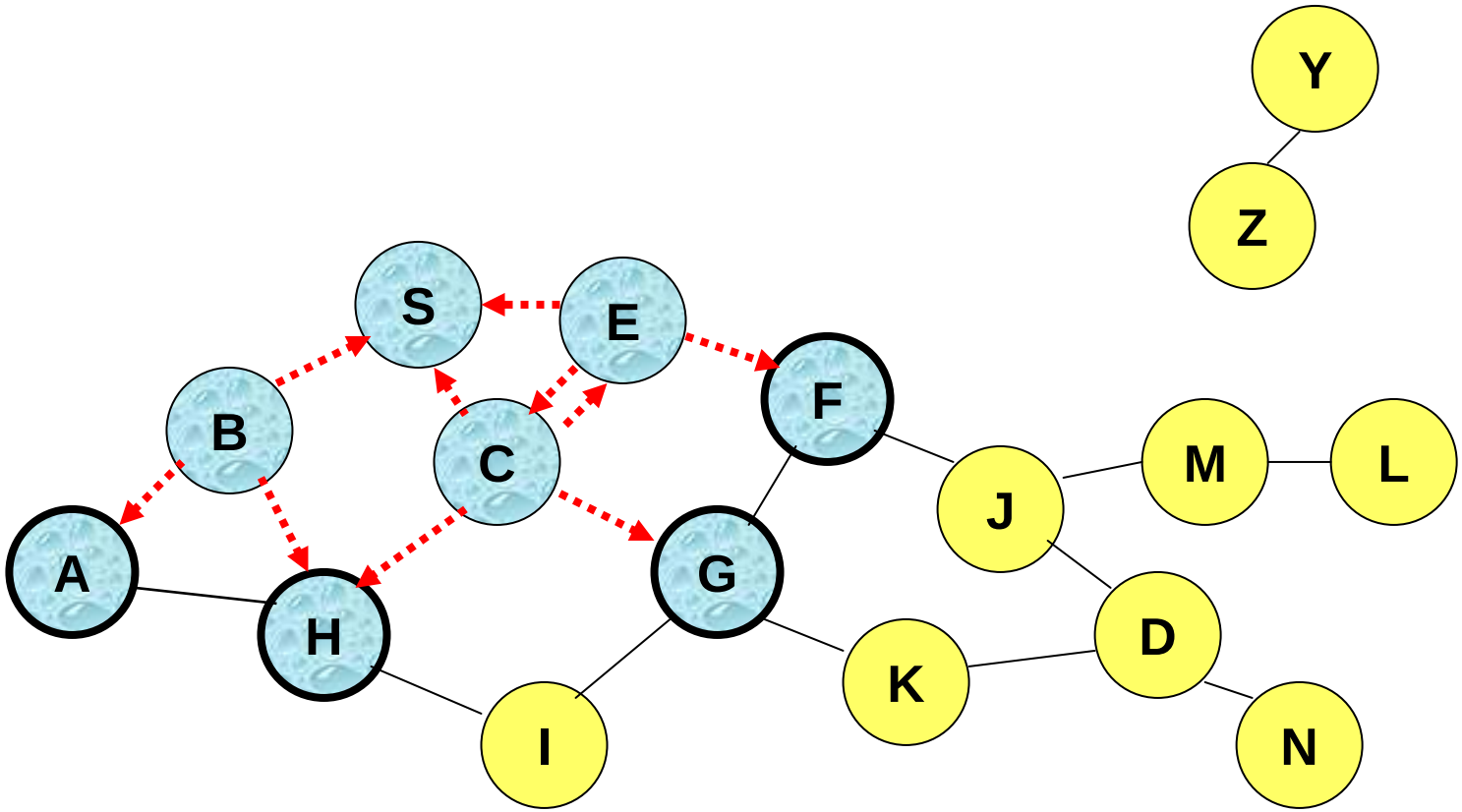
Flooding for Data Delivery



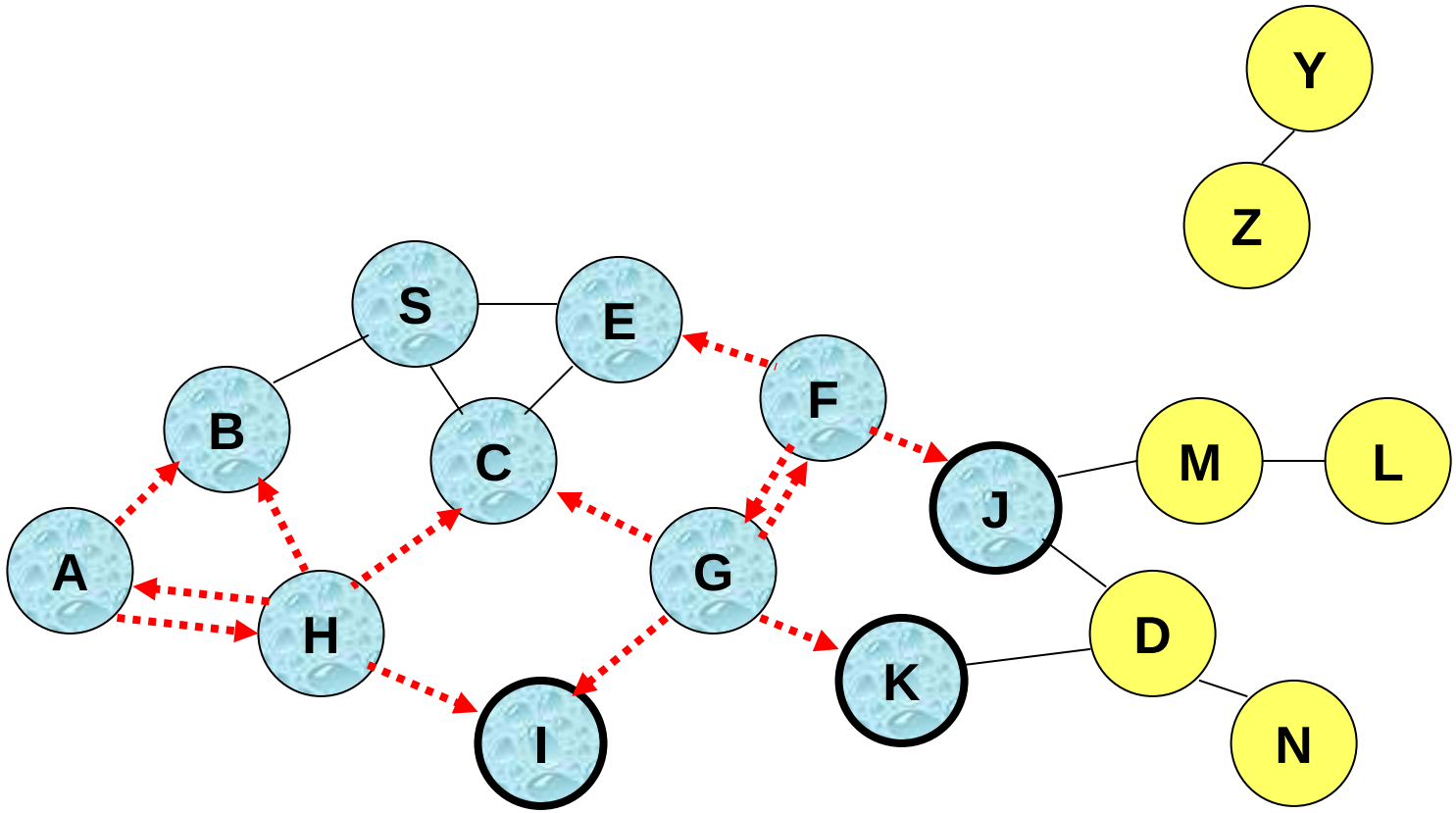
Represents a node that receives packet P for the first time

Represents transmission of packet P

Flooding for Data Delivery

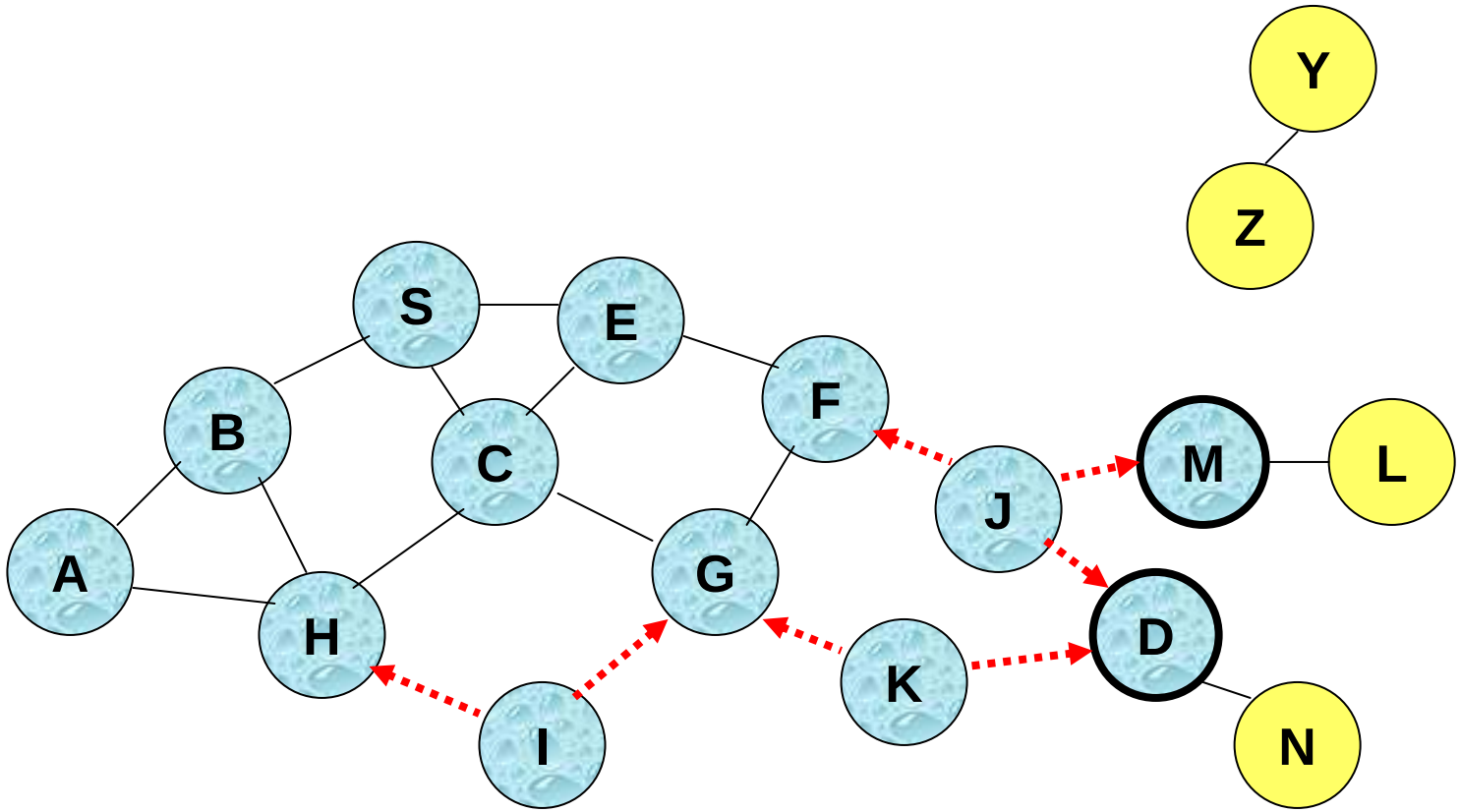


Flooding for Data Delivery



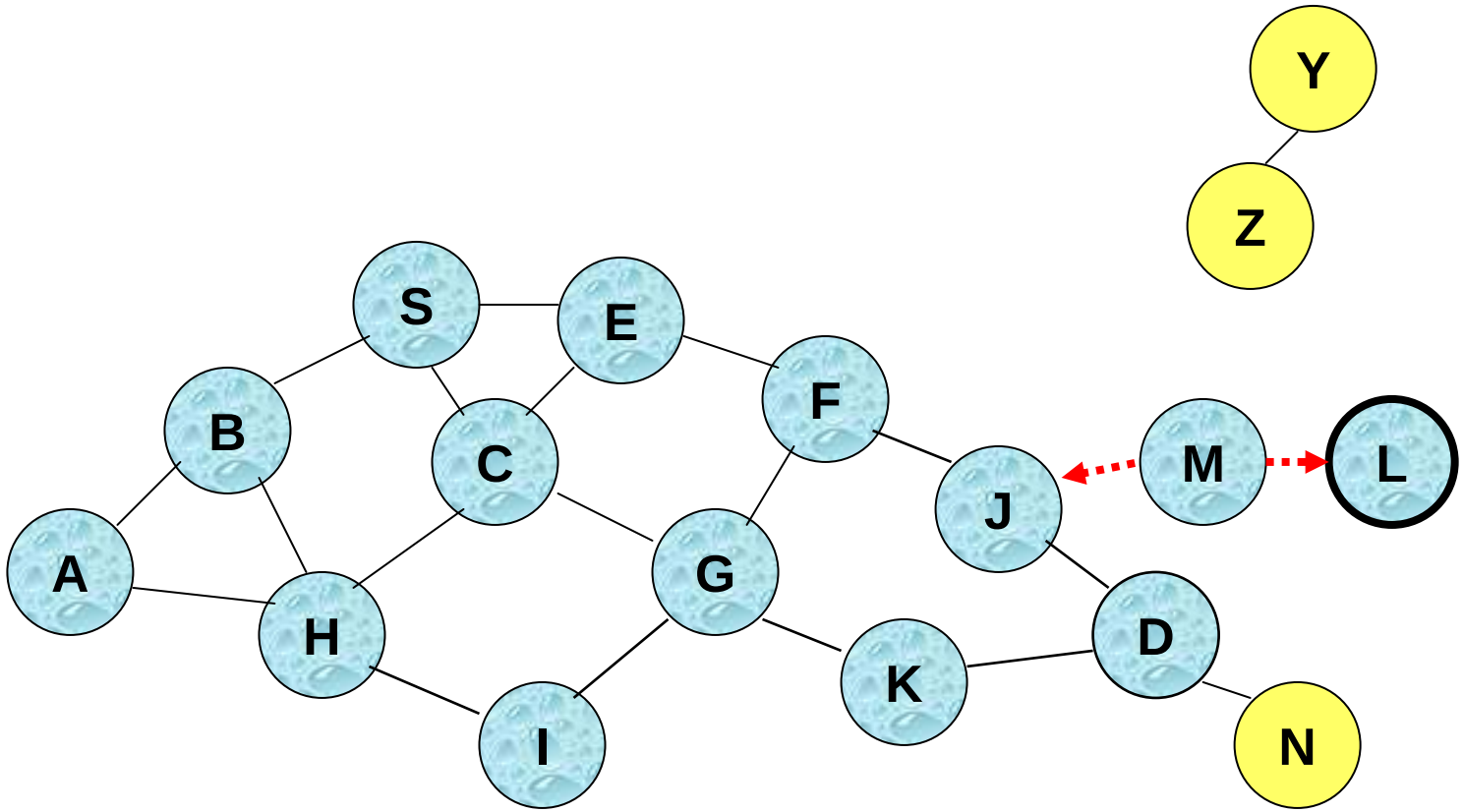
- **Node C receives packet P from G and H, but does not forward it again, because node C has already forwarded packet P once**

Flooding for Data Delivery



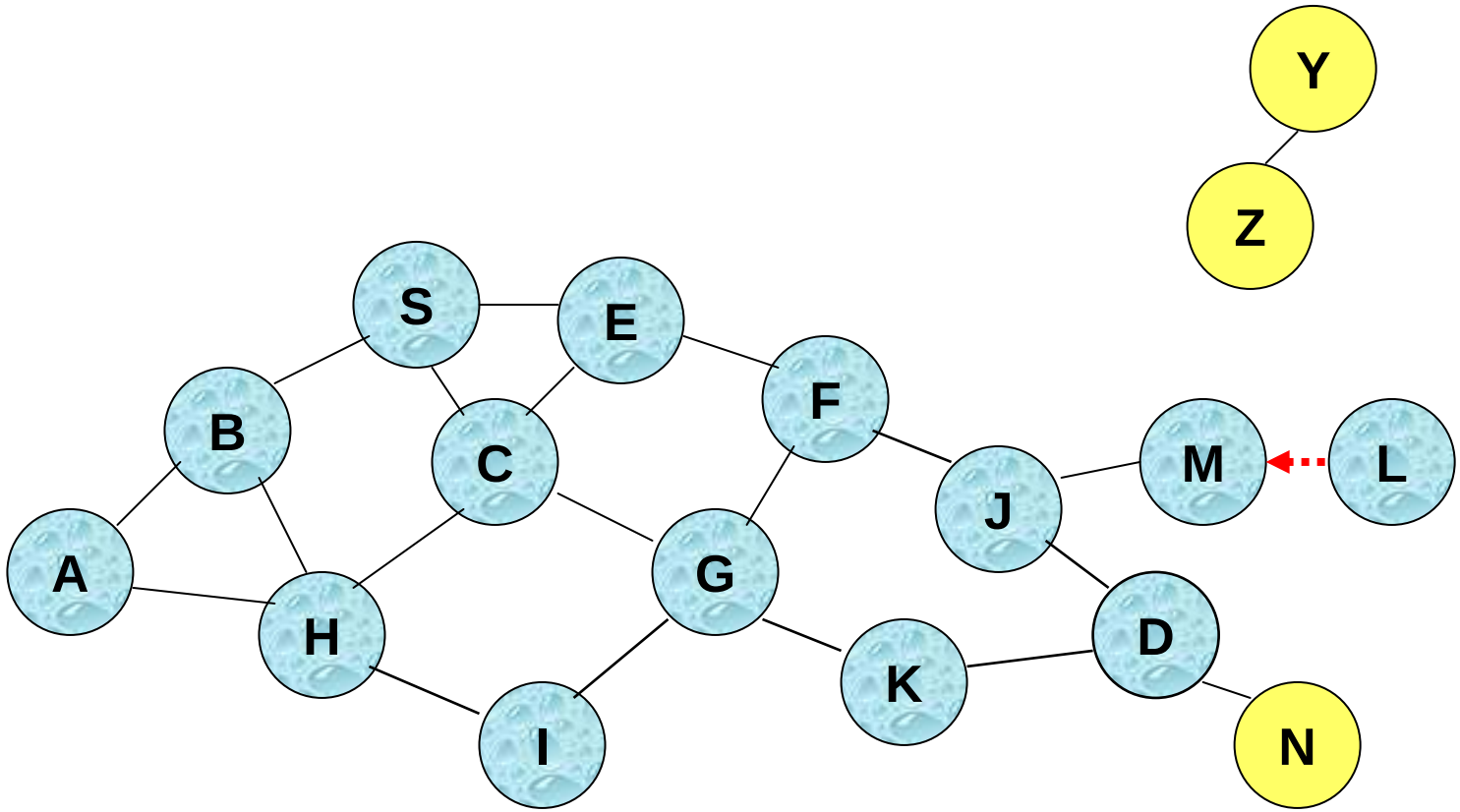
- **Node D receives packet P from two neighbors: potential for collision, packet may get lost despite flooding**

Flooding for Data Delivery



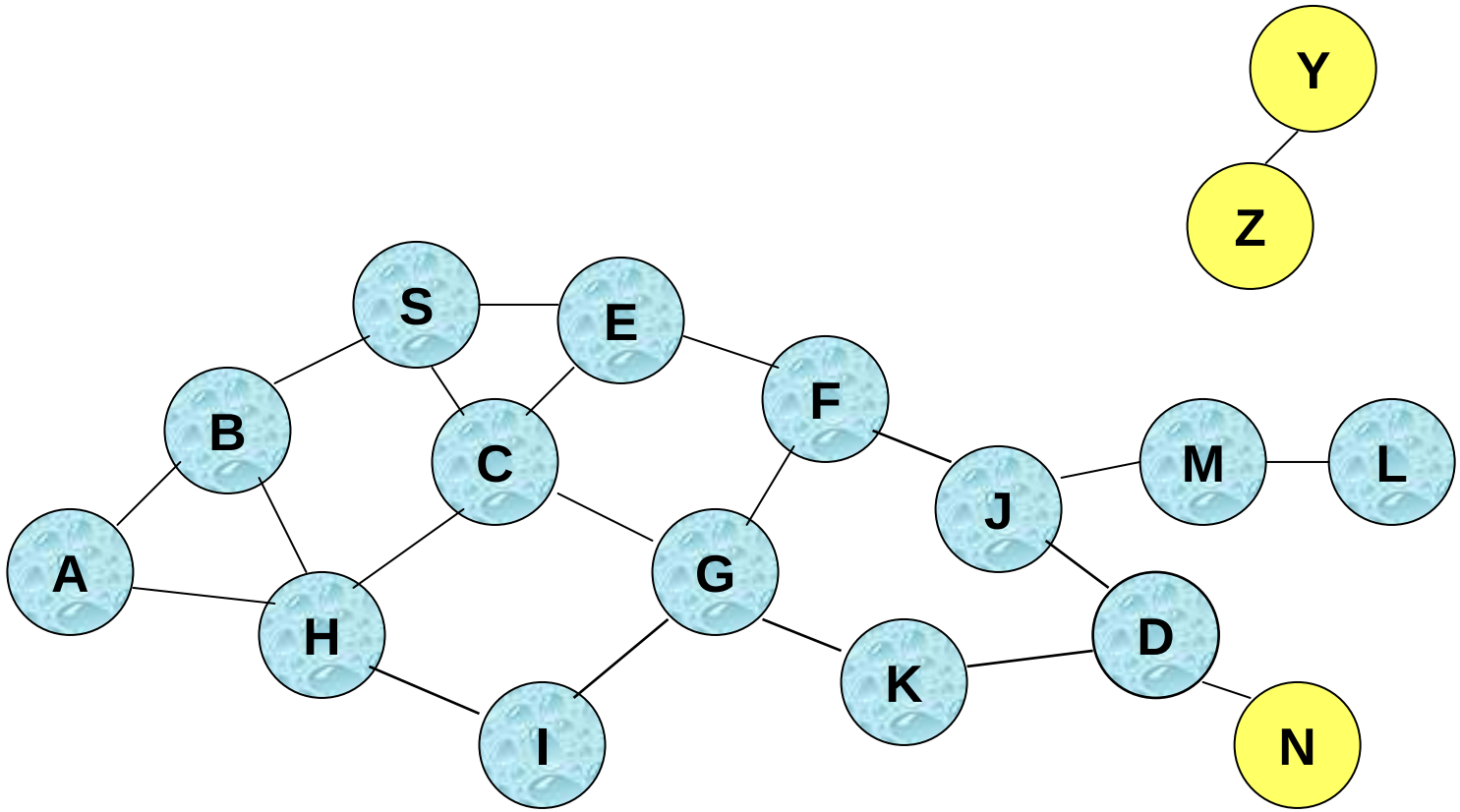
- **Node D does not forward packet P, because node D is the intended destination of packet P**

Flooding for Data Delivery



- **Flooding completed**
- **Nodes unreachable from S do not receive packet P (e.g., node Z)**
- **Nodes for which all paths from S go through the destination D also do not receive packet P (example: node N)**

Flooding for Data Delivery



- **Flooding may deliver packets to too many nodes (in the worst case, all nodes reachable from sender may receive the packet) => High Overhead**

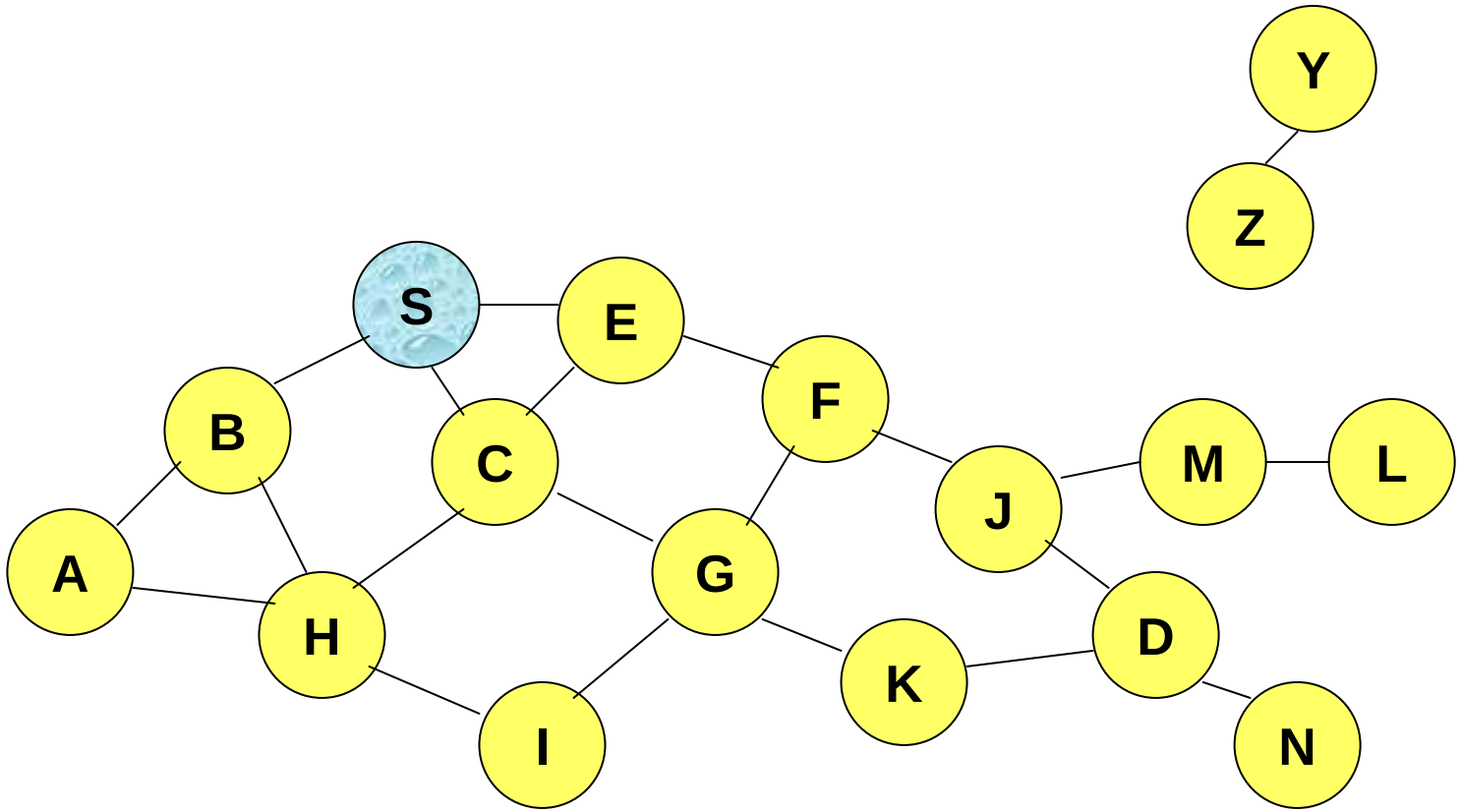
Flooding of Control Packets

- Many protocols perform (potentially *limited*) flooding of control packets, instead of data packets
- The control packets are used to discover routes
- Discovered routes are subsequently used to send data packet(s)
- Overhead of control packet flooding is amortized over data packets transmitted between consecutive control packet floods

Ad-Hoc On Demand Distance Vector Routing (AODV)

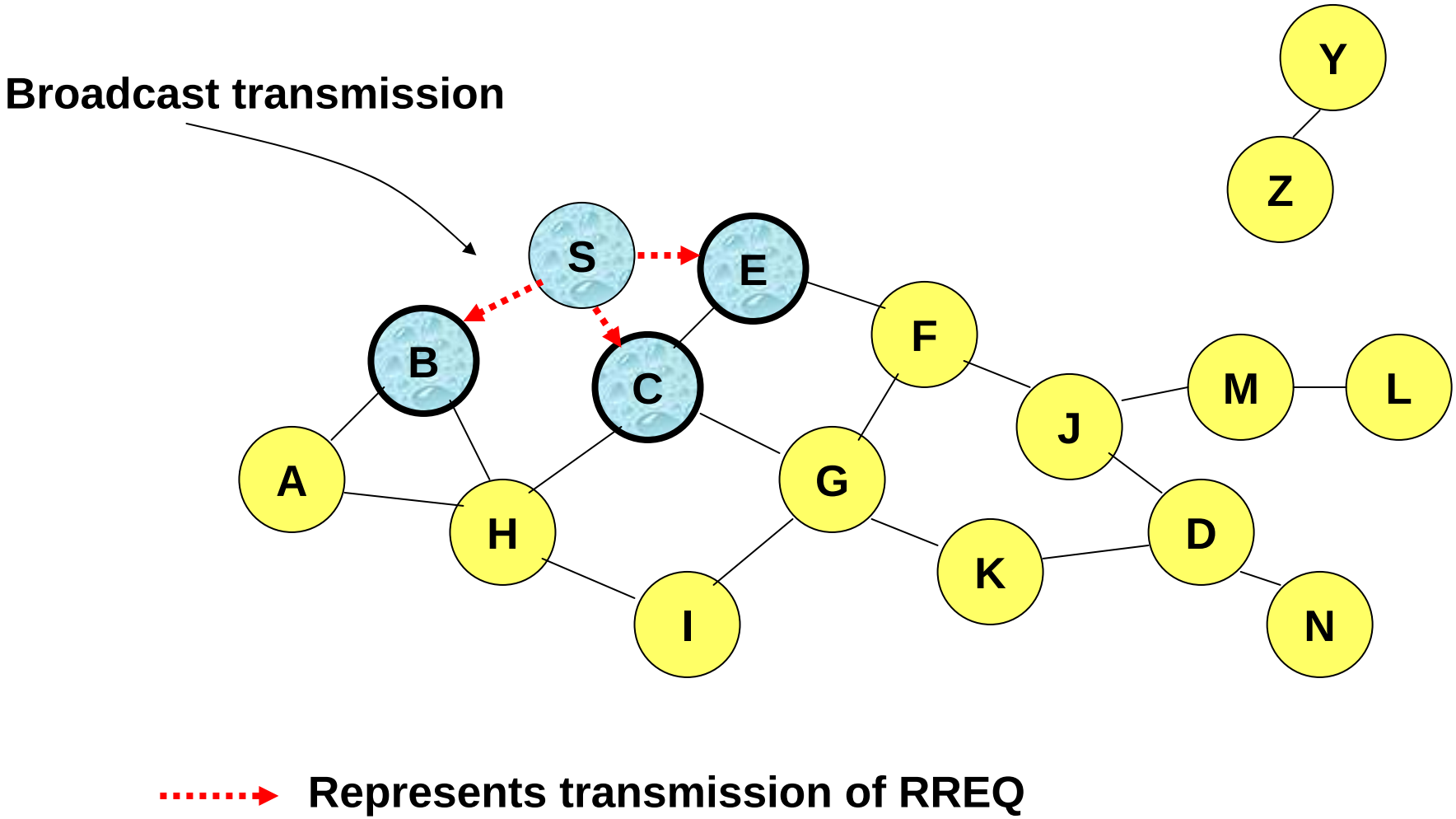
- Route Requests (RREQ) are flooded on demand
- When a node re-broadcasts a Route Request, it sets up a reverse path pointing towards the source
  - AODV assumes symmetric (bi-directional) links
- When the intended destination receives a Route Request, it replies by sending a Route Reply
- Route Reply travels along the reverse path set-up when Route Request is forwarded
- A detailed description of AODV can be found in [PR99a], a comparison with other protocols in [BMJ+98a] and [JLH+99a]

Route Requests in AODV

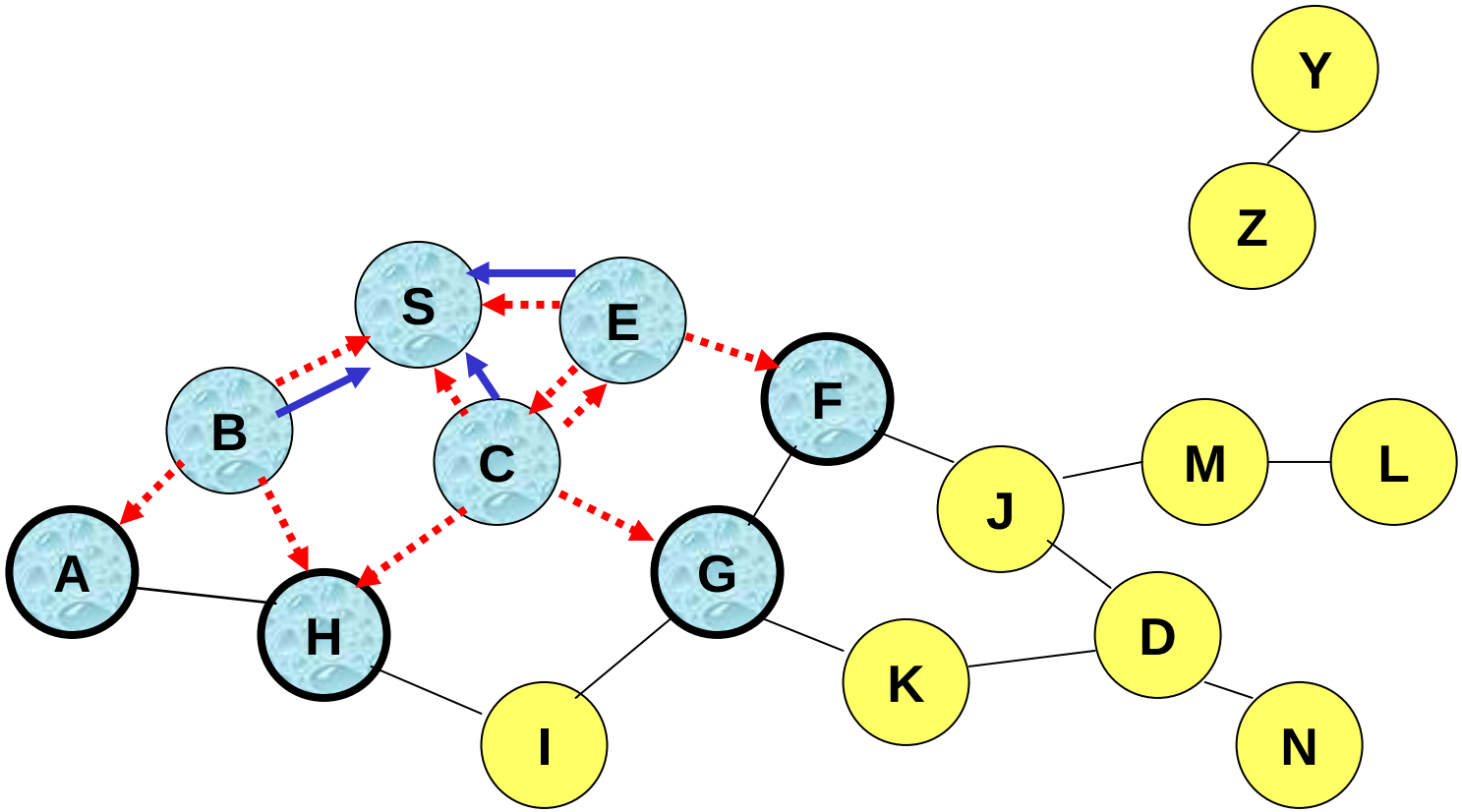


Represents a node that has received RREQ for D from S

Route Requests in AODV

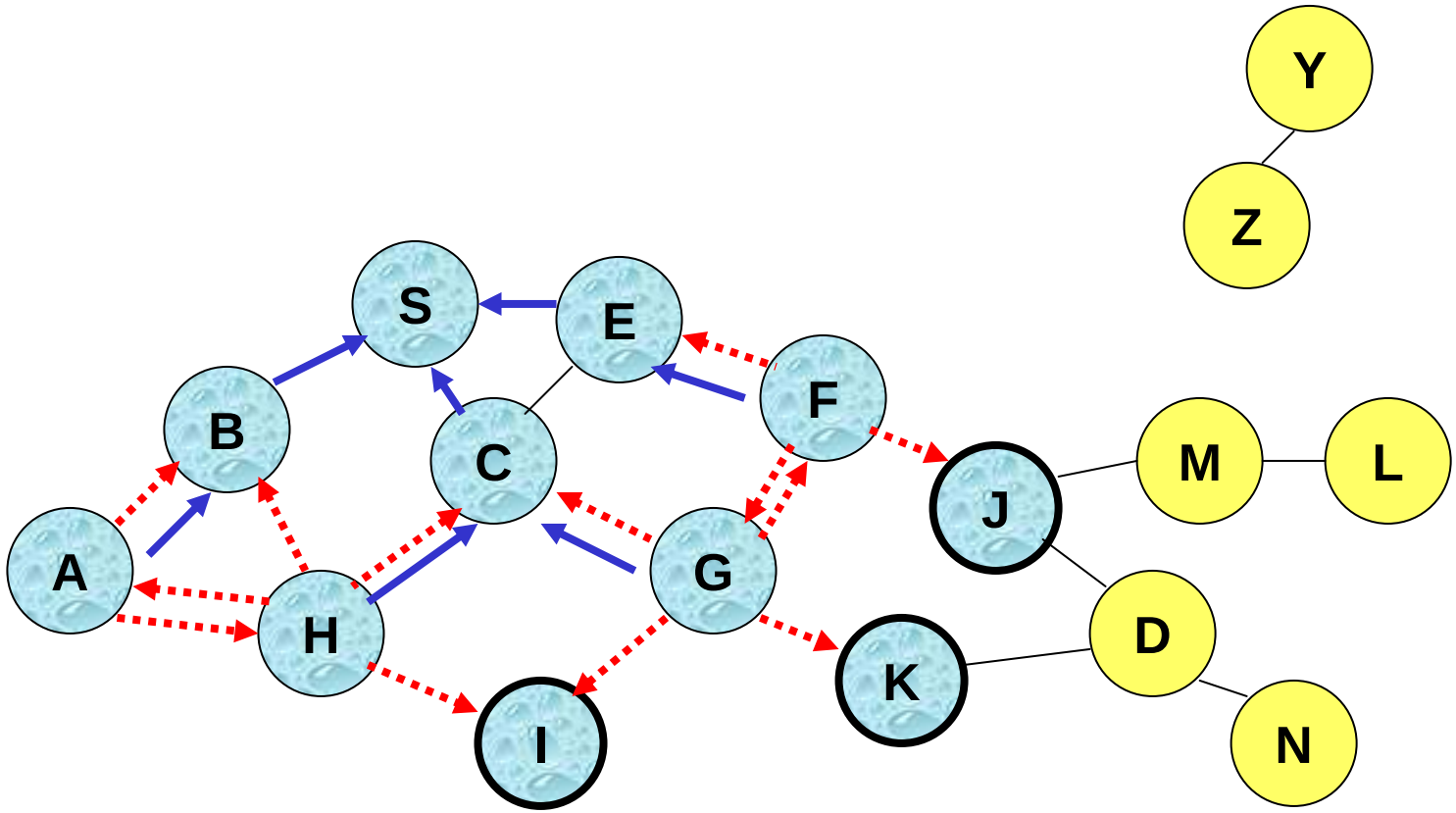


Route Requests in AODV



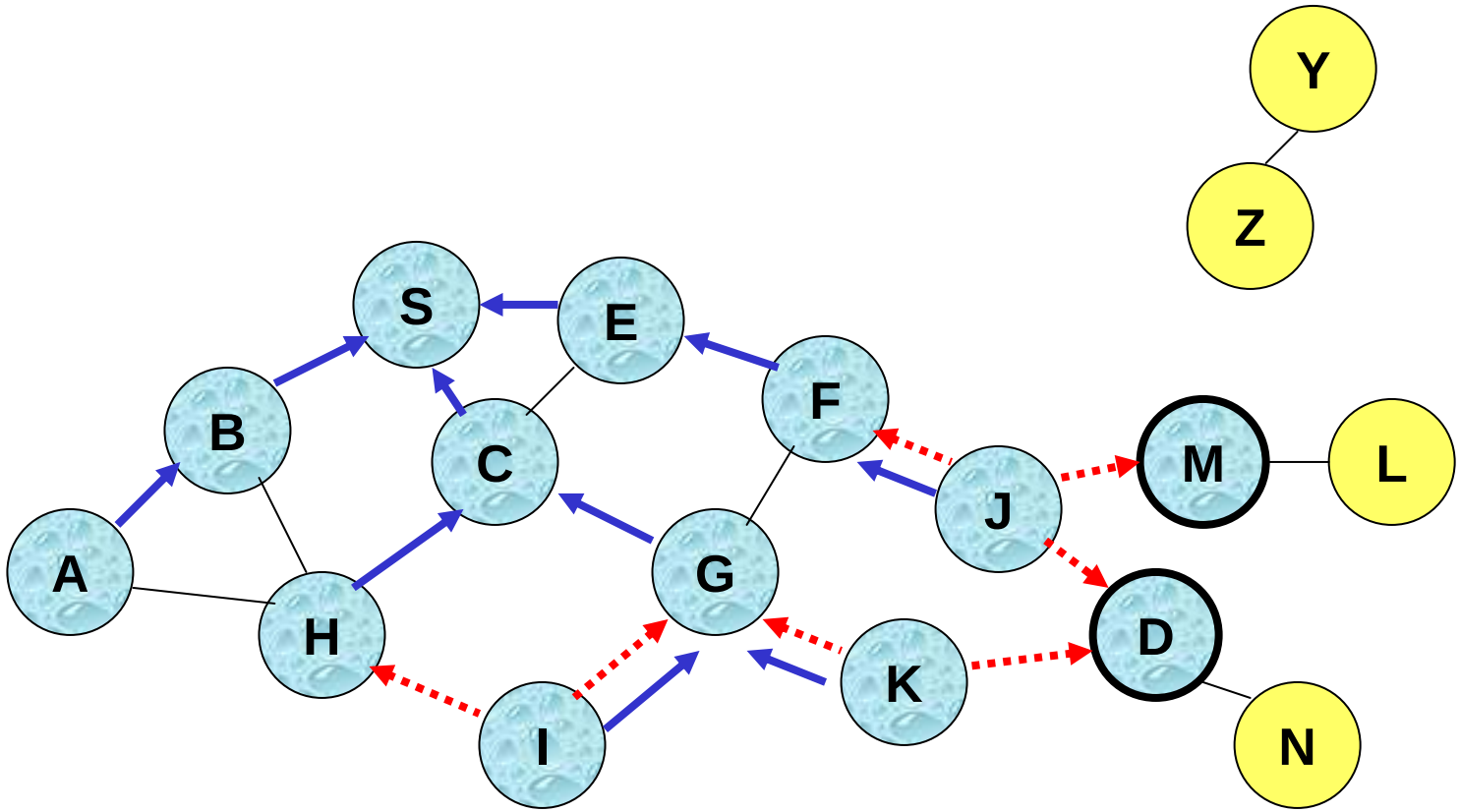
Represents links on Reverse Path

Reverse Path Setup in AODV

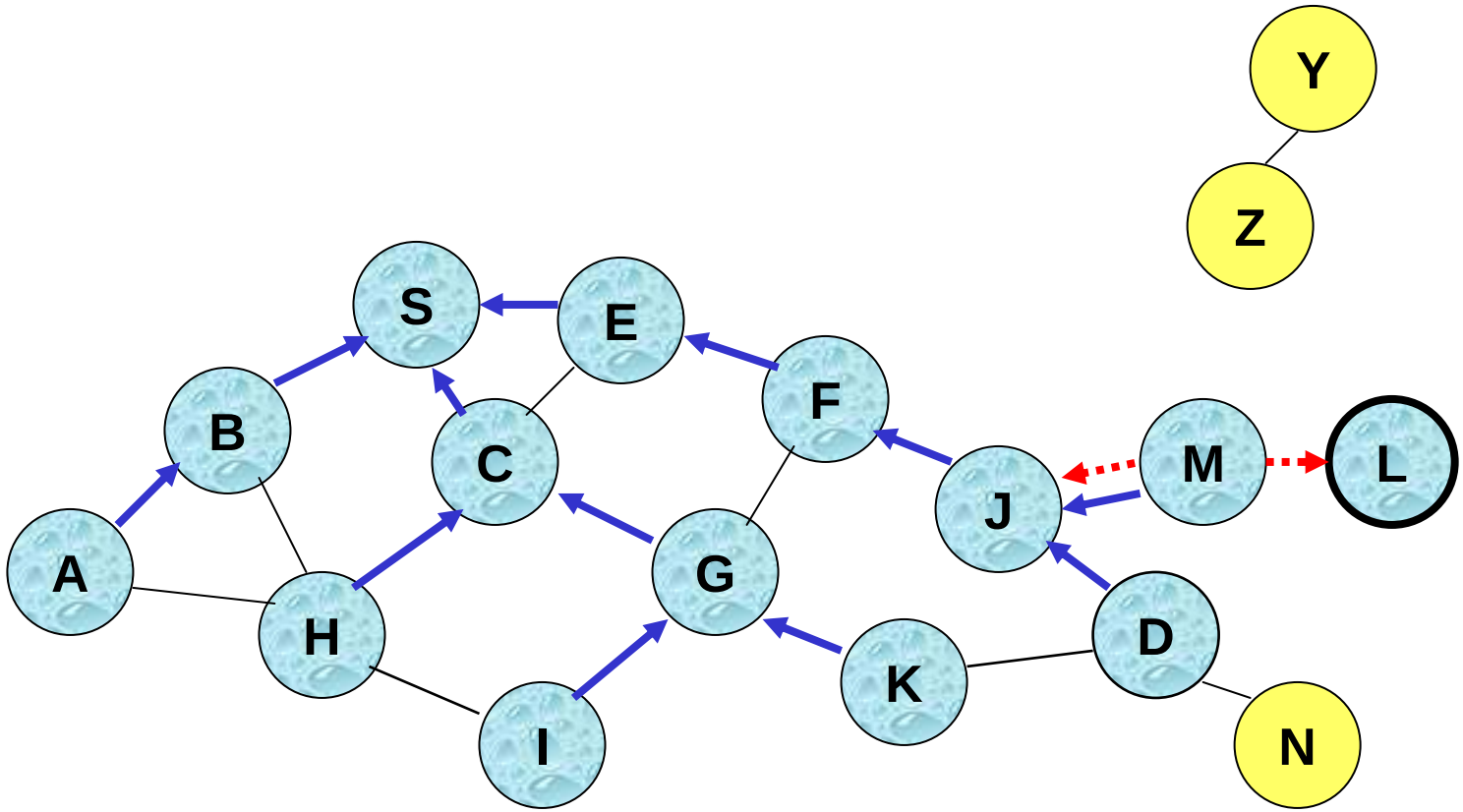


- **Node C receives RREQ from G and H, but does not forward it again, because node C has already forwarded RREQ once**

Reverse Path Setup in AODV

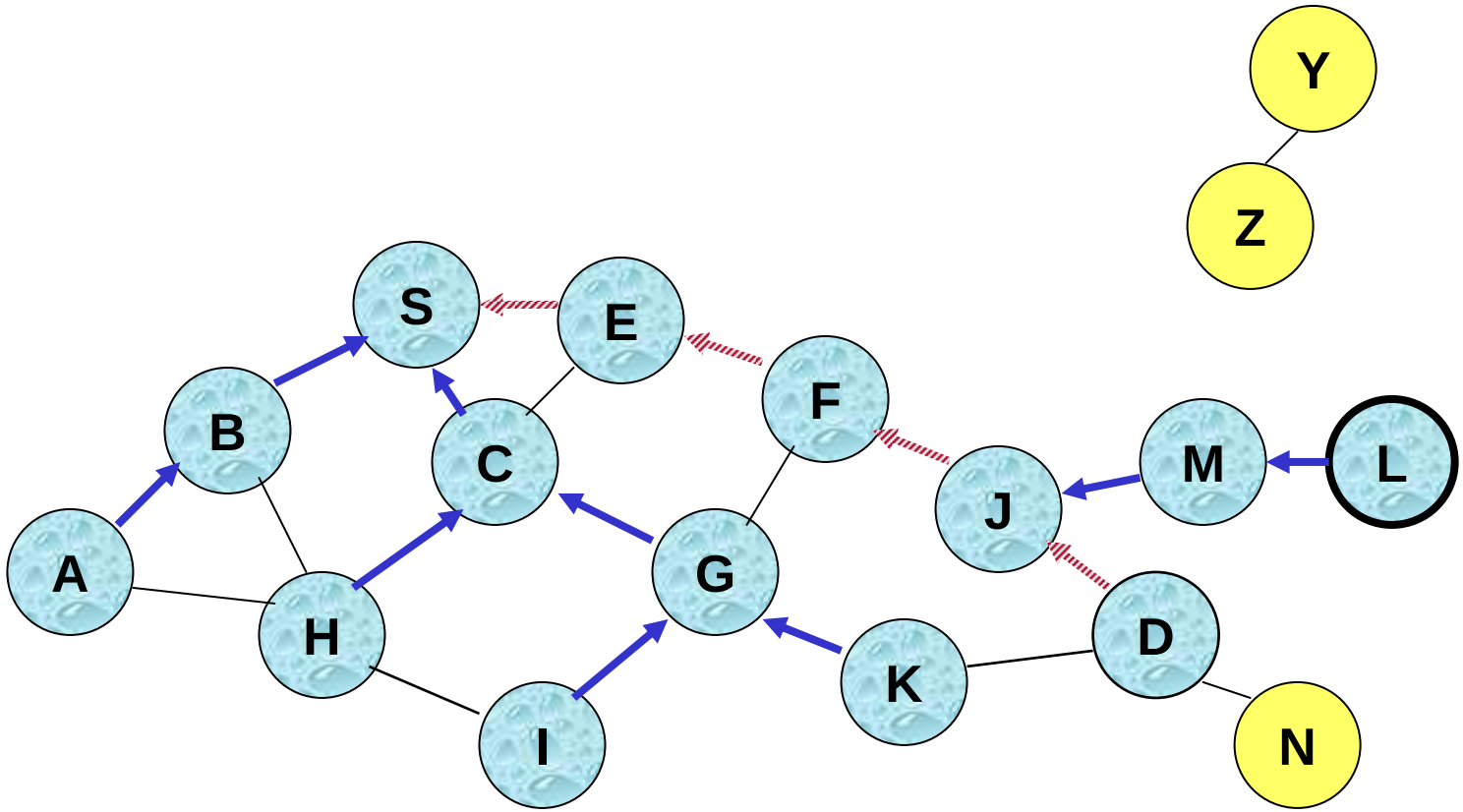


Reverse Path Setup in AODV



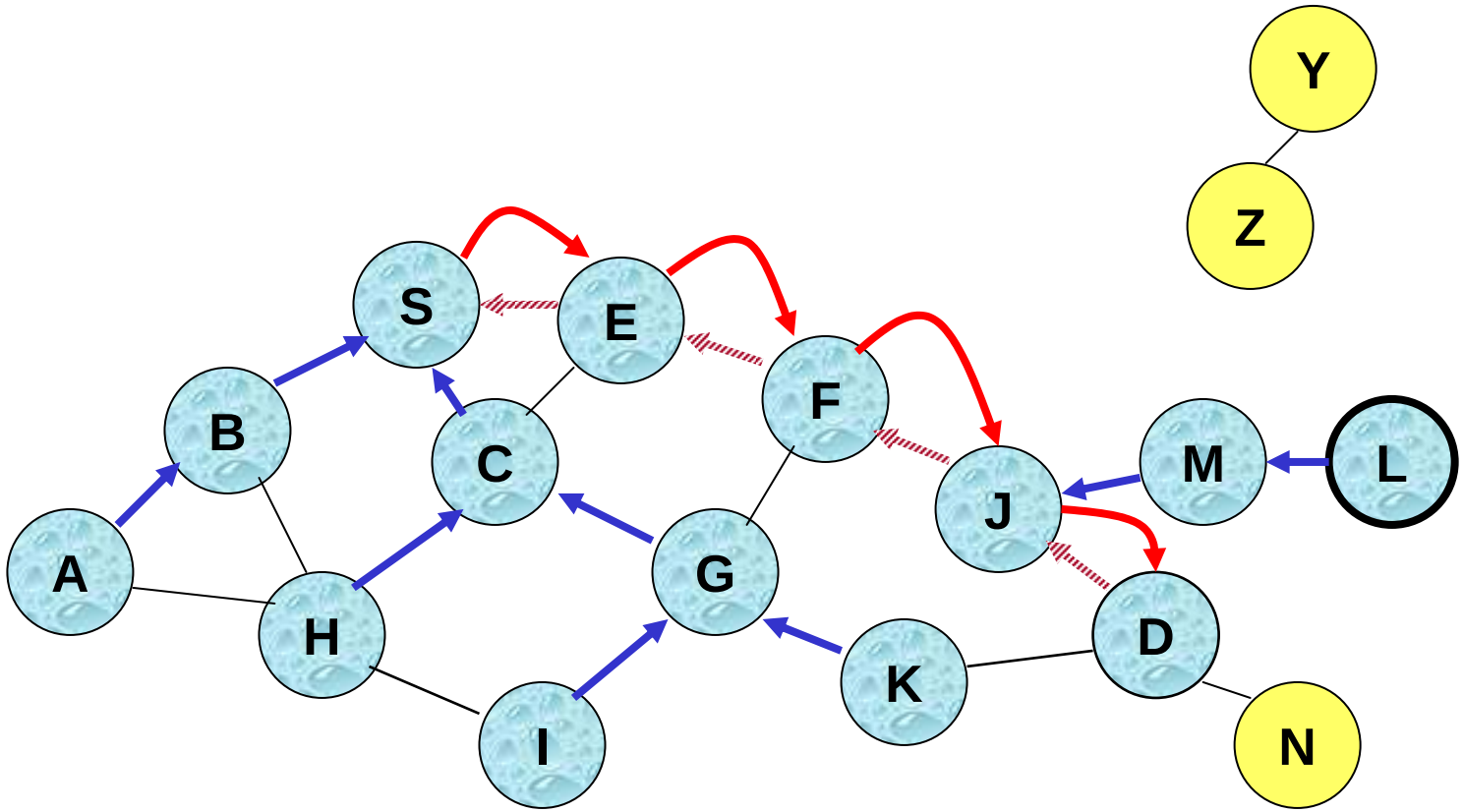
- **Node D does not forward RREQ, because node D is the intended target of the RREQ**

Route Reply in AODV



Represents links on path taken by RREP

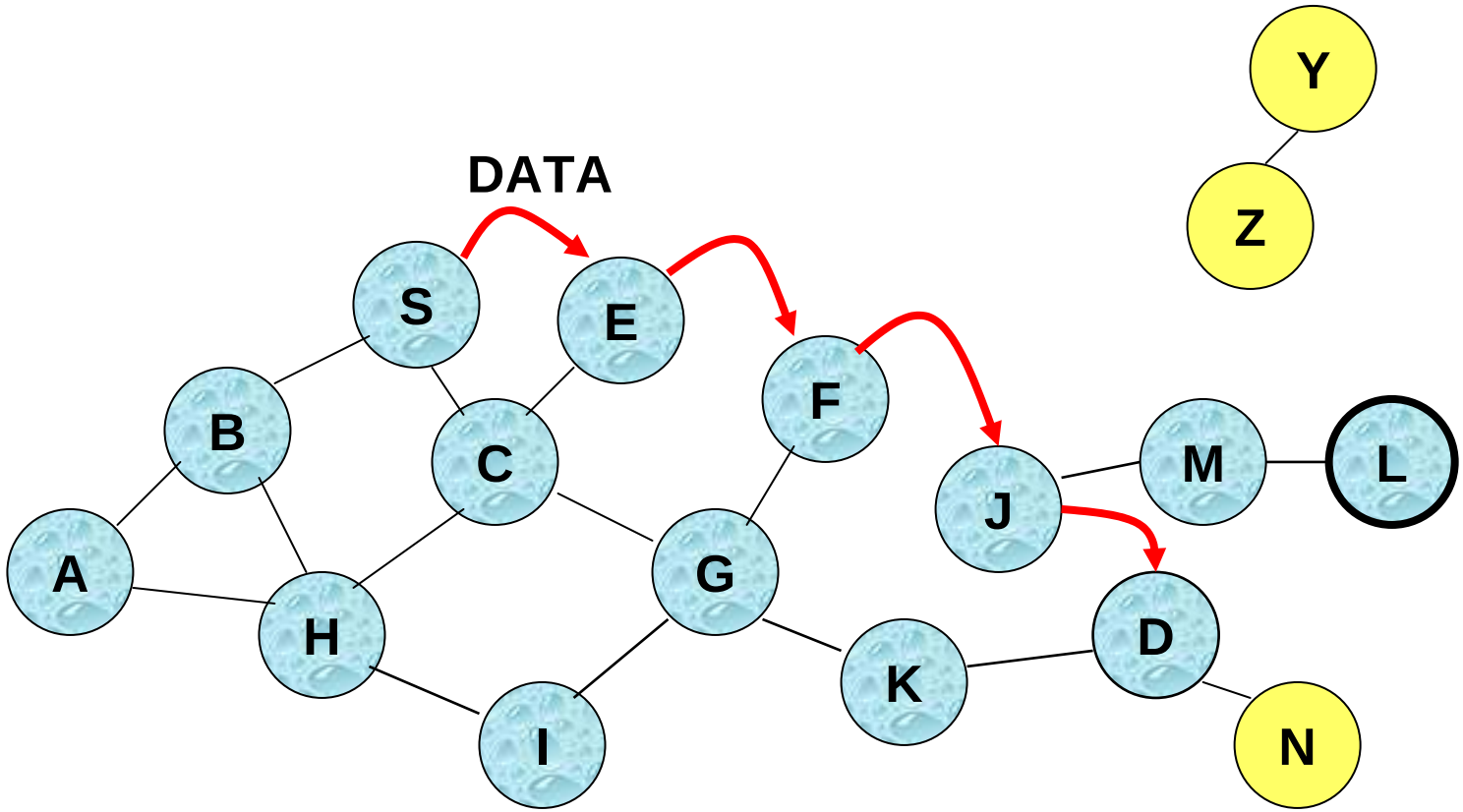
Forward Path Setup in AODV



Forward links are setup when RREP travels along the reverse path

Represents a link on the forward path

Data Delivery in AODV



Routing table entries used to forward data packets.

Timeouts

- A routing table entry maintaining a reverse path is purged after a timeout interval
  - timeout should be long enough to allow RREP to come back

- A routing table entry maintaining a forward path is purged if *not used* for a *active_route_timeout* interval
  - if no is data being sent using a particular routing table entry, that entry will be deleted from the routing table (even if the route may actually still be valid)

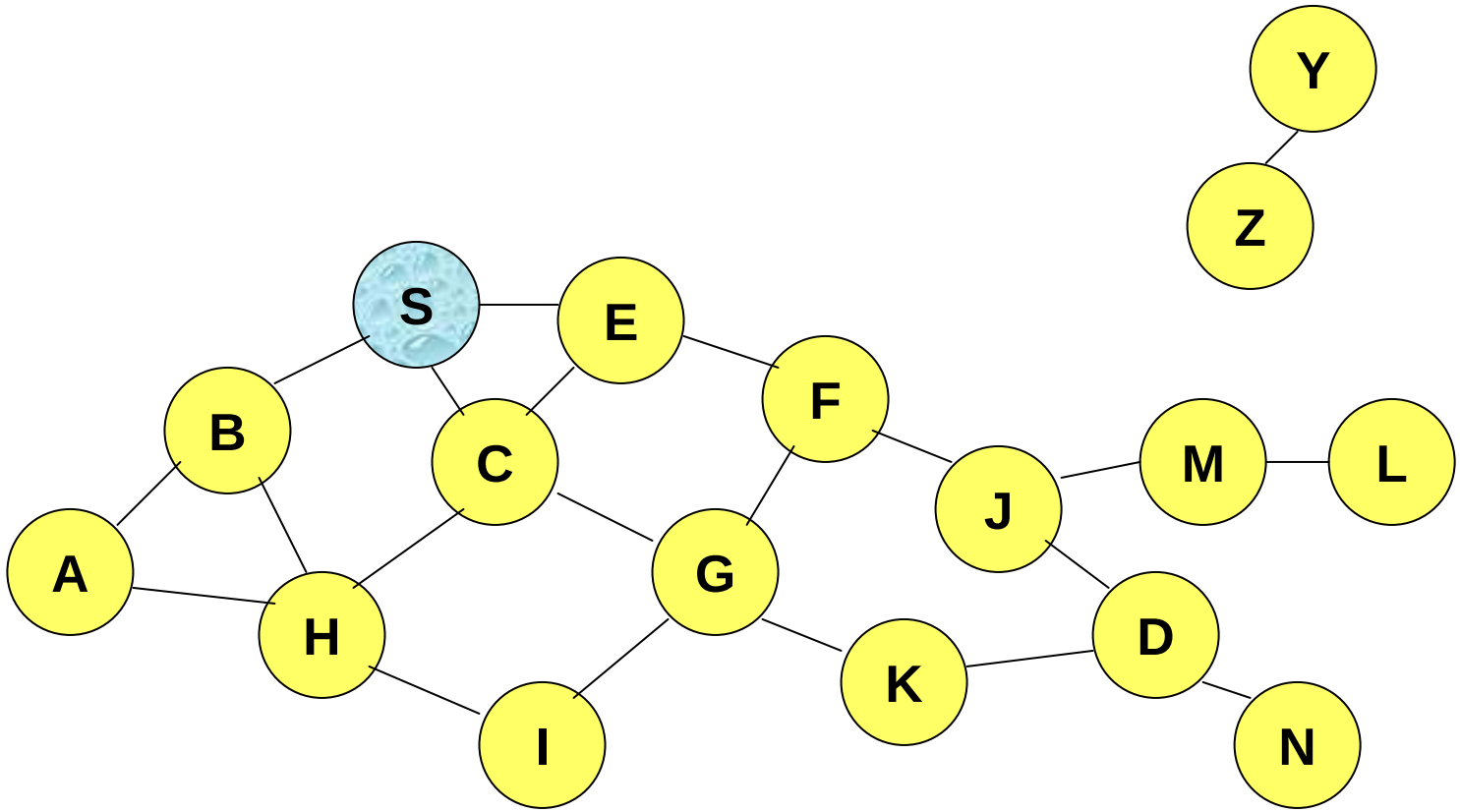
Link Failure Reporting

- A neighbor of node X is considered active for a routing table entry if the neighbor sent a packet within *active_route_timeout* interval which was forwarded using that entry
- When the next hop link in a routing table entry breaks, all active neighbors are informed
- Link failures are propagated by means of Route Error messages

Dynamic Source Routing (DSR) [Johnson96]

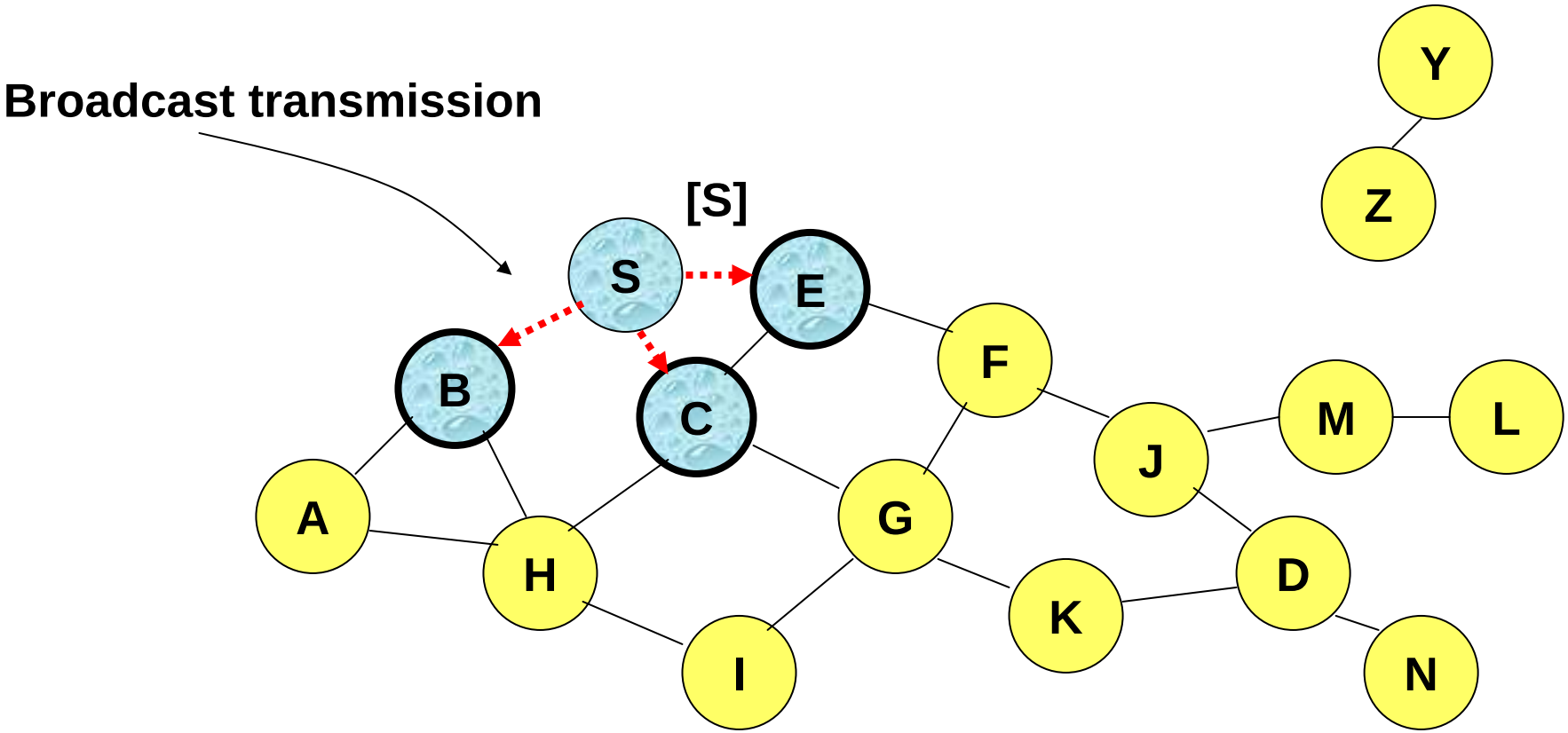
- When node S wants to send a packet to node D, but does not know a route to D, node S initiates a route discovery
- Source node S floods Route Request (RREQ)
- Each node appends own identifier when forwarding RREQ
- A detailed description of AODV can be found in [JM96a], a comparison with other protocols in [BMJ+98a] and [JLH+99a]

Route Discovery in DSR



Represents a node that has received RREQ for D from S

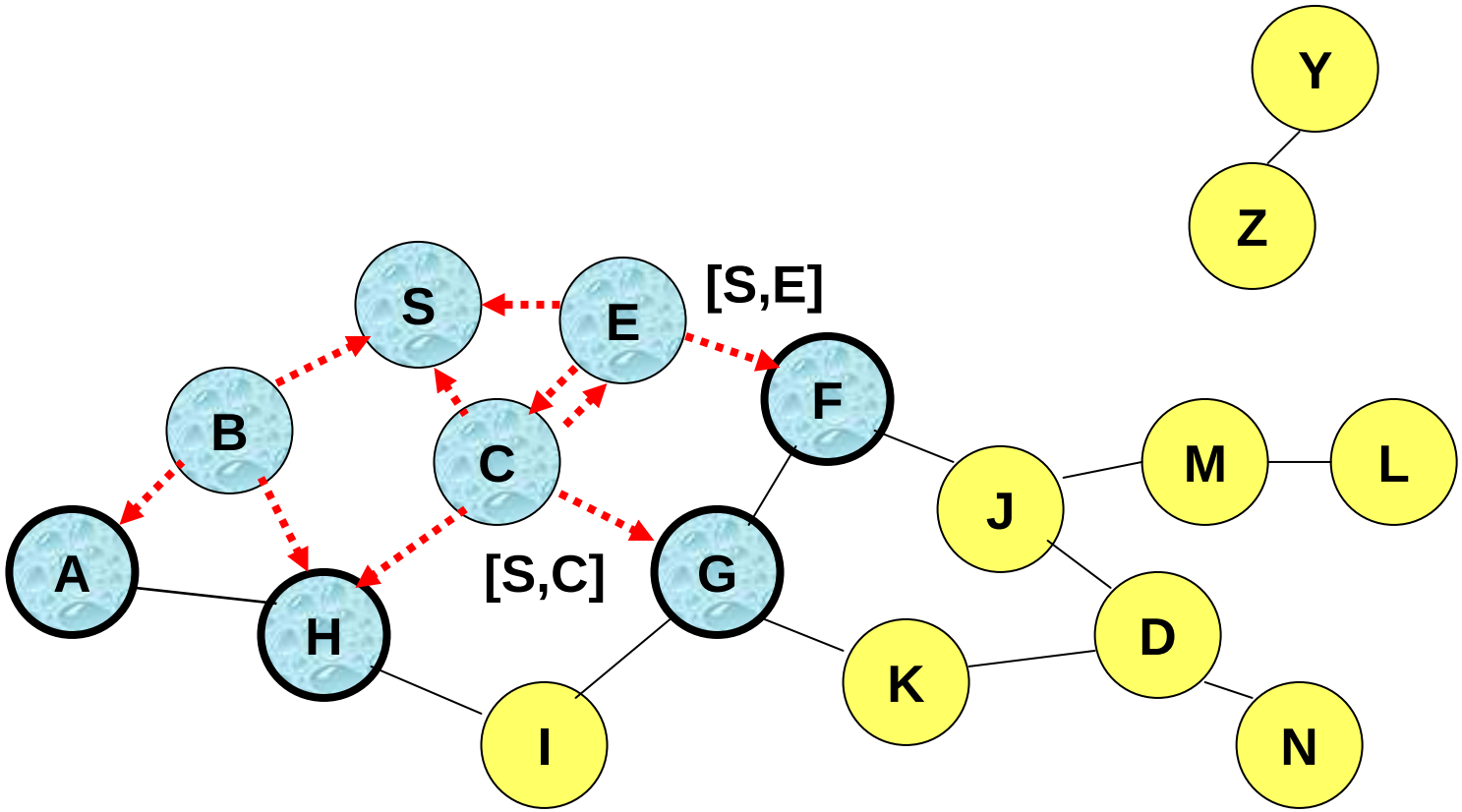
Route Discovery in DSR



Represents transmission of RREQ

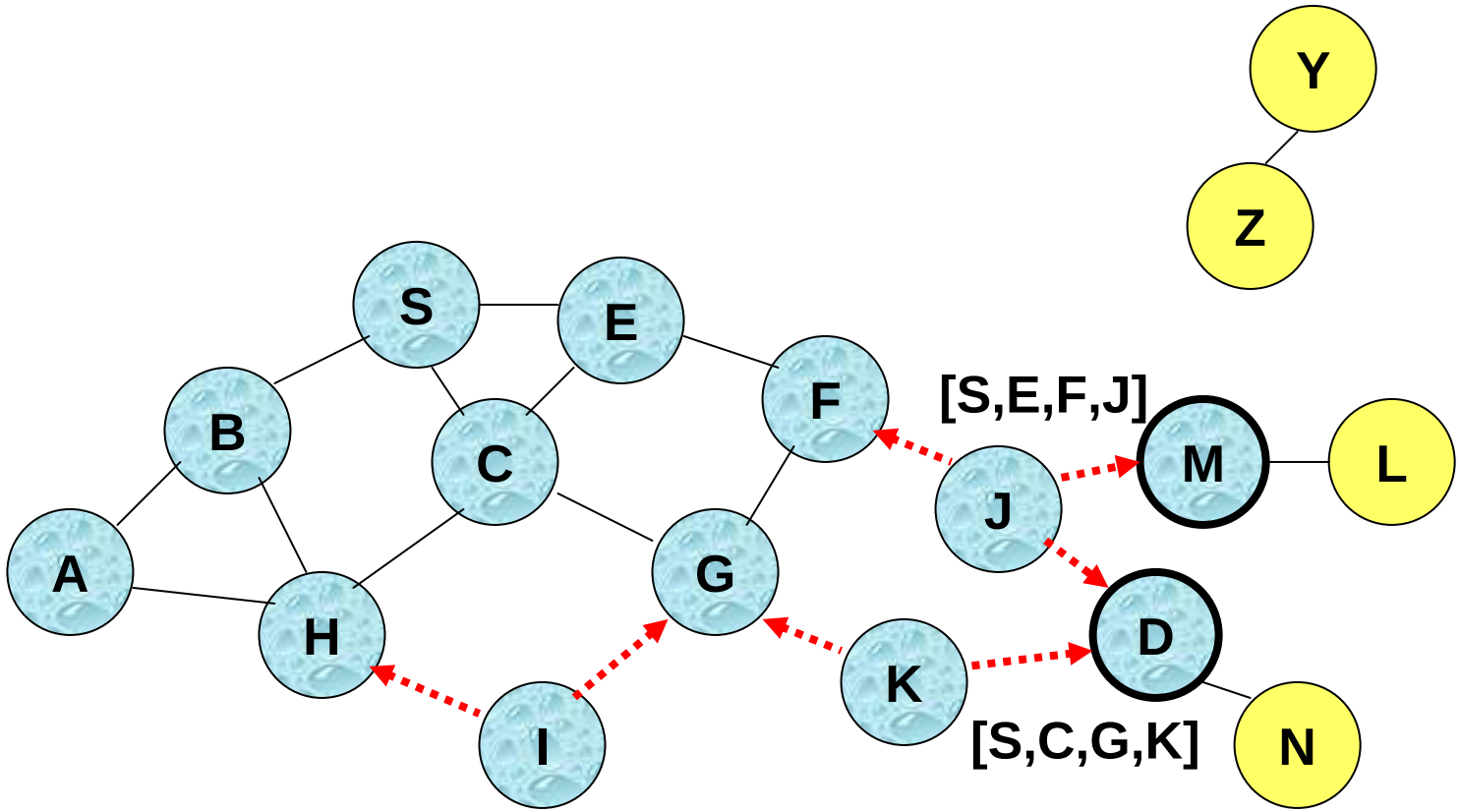
[X,Y] Represents list of identifiers appended to RREQ

Route Discovery in DSR



- **Node H receives packet RREQ from two neighbors:**
  potential for collision

Route Discovery in DSR

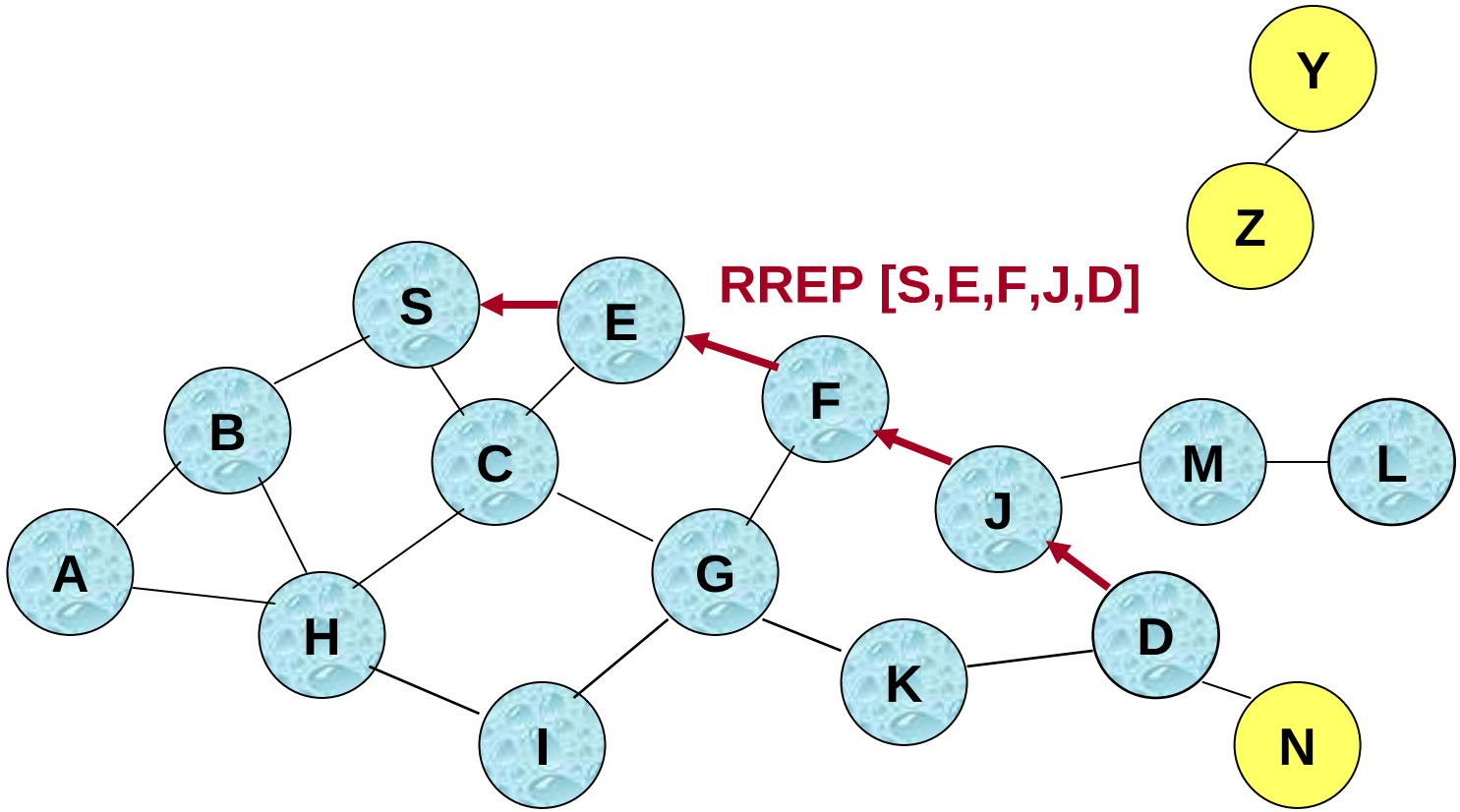


- **Nodes J and K both broadcast RREQ to node D**
- **Since nodes J and K are hidden from each other, their transmissions may collide**

Route Discovery in DSR

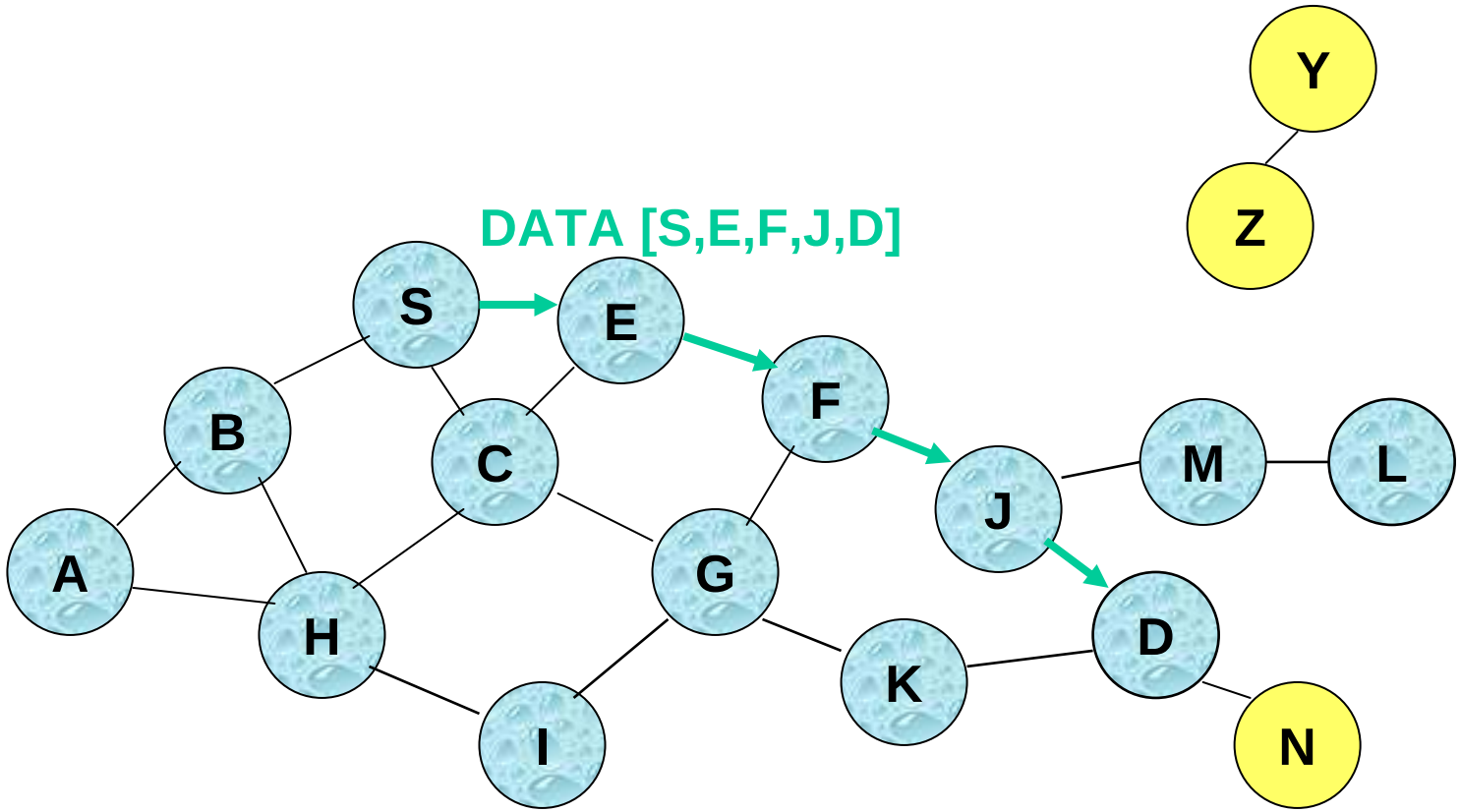
- Destination D on receiving the first RREQ, sends a Route Reply (RREP)
- RREP is sent on a route obtained by reversing the route appended to received RREQ
- RREP includes the route from S to D on which RREQ was received by node D

Route Reply in DSR



← **Represents RREP control message**

Data Delivery in DSR



Packet header size grows with route length

Discussion AODV vs. DSR

- Both are reactive and maintain routes only on demand
- Both can be optimized by route caching:
  - route information is cached by all nodes
  - intermediate nodes may reply to route requests
  - DSR is slightly more aggressive with caching
- Status:
  - AODV is currently an experimental IETF/manet RFC [PBD03a]
  - DSR is currently an IETF/manet Internet Draft [JMH03a]
- Key Problems:
  - AODV requires per-route state in intermediate nodes
  - DSR requires extra header space
  - AODV MAY have an edge since often bandwidth is the limiting resource

References

- [BMJ+98a] J. Broch, D. Maltz, D. Johnson, Y. Hu, and J. Jetcheva, „ A Performance Comparison of Multi-Hop Wireless Ad Hoc Network Routing Protocols“, In "Proceedings of the fourth annual ACM/IEEE International Conference on Mobile computing and networking (MobiCom '98)", pp. 85-97, Dallas, Texas, October 1998.
- [JLH+99a] P. Johansson, T. Larsson, N. Hedmann, B. Mielczarek, and M. Degermark, „Scenario-Based Performance Analysis of Routing Protocols for Mobile Ad-Hoc Networks“, In "Proceedings of the fifth annual ACM/IEEE International Conference on Mobile computing and networking (MobiCom '99)", pp. 195-206, Seattle, Washington, August 1999.
- [JM96a] D. Johnson, and D. Maltz, „ Dynamic Source Routing in Ad Hoc Wireless Networks“, In "Mobile Computing", Kluwer Academic Publishers, 1996.
- [JMH03a] D. Johnson, D. Maltz, Y. Hu. The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR), Internet Draft, work-in-progress. April 2003.
- [PBD03a] C. Perkins, E. Belding-Royer, S. Ad hoc On-Demand Distance Vector (AODV) Routing. RFC 3561. July 2003.
- [PR99a] C. Perkins, and E. Royer, „ Ad-Hoc On-Demand Distance Vector Routing“, In " Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications (WMCSA) ", pp. 1405-1413, New Orleans, LA, February 1999.
- [RT99a] E. Royer, and C. Toh, „ A Review of Current Routing Protocols for Ad-Hoc Mobile Wireless Networks“, In "IEEE Personal Communications", pp. 46-55, April 1999.

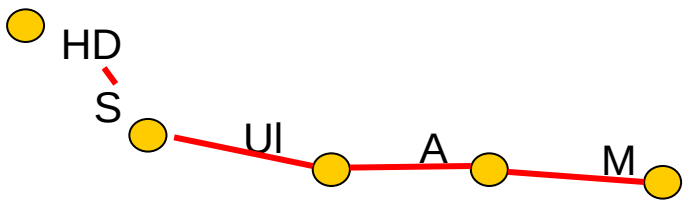
Geographic Unicast Routing

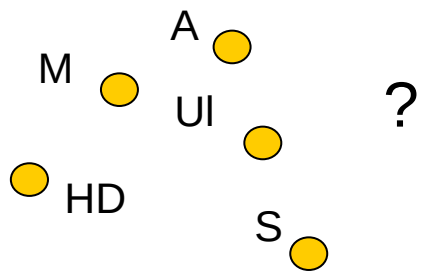
Hannes Hartenstein, NEC Europe Network Labs

Problems of topology-based approaches

- In highly mobile networks:
  - Proactive approaches: signaling load (too) high
  - Proactive/reactive approaches: routes break (too) often

Concept ‘route’





- In large networks (e.g. sensor networks):
  - scaling problems
    - Proactive approaches: see above
    - Reactive approaches: large amount of state information either in packet header or in routing tables

Positional information

- ... might help!
- Basic assumption for position-based (geographic) routing: each node knows its own position
- ‚Absolute' instead of ‚relative' information:
  - Instead of topological information ("node A is neighbor of B"):
  - "Node A is located at a distance of 120m from node B, direction 73^{o} w.r.t. current driving direction of A."
- 'Strong assumption'

Positioning

- With a satellite navigation infrastructure
  - Global Positioning System (GPS):

    Requirement: GPS receiver receives signals from at least 3 GPS-satellites.
    Accuracy: [w/o SA] approx. +/- 25m spatial, +/- 200ns temporal

    Basic principle: fully synchronized system, satellites exactly know where they are; estimation of distance via signal propagation delay.
  - Differential GPS (DGPS): via stationary reference nodes.
  - Navigational systems: make us of digital maps to ‘match coordinates’.
- Without (satellite navigation) infrastructure
  - Two building blocks:
    - Distance estimation between two nodes
    - Protocol to build coordinate system
  - Distance estimation: not an easy task since ad hoc networks usually not ‘perfectly’ synchronized.

    Signal propagation delay:

    ‘back-of-the-envelope calculation’: 300 000 000m/s

    $\rightarrow$ 300m/μs

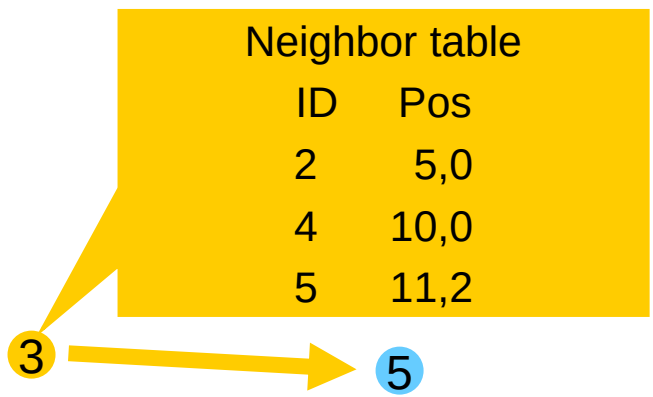
    Radar (UWB) might be approprate
  - Protocols:
    - ‘GPS-free positioning in mobile ad hoc networks’ [CHH01]
    - ‘Scalable and Distributed GPS Free Positioning for Sensor Networks’ [IS03]

Position-based routing: basics

- Each node knows its position
- Nodes know positions of their direct neighbors (via ‘Beaconing’)
  - ‘Beacon’: message that is periodically broadcasted to on-hop neighbors
- Location services provides positional information of potential communication partner

Greedy packet forwarding

Dest.: 6 at position (15,1)



1 Source

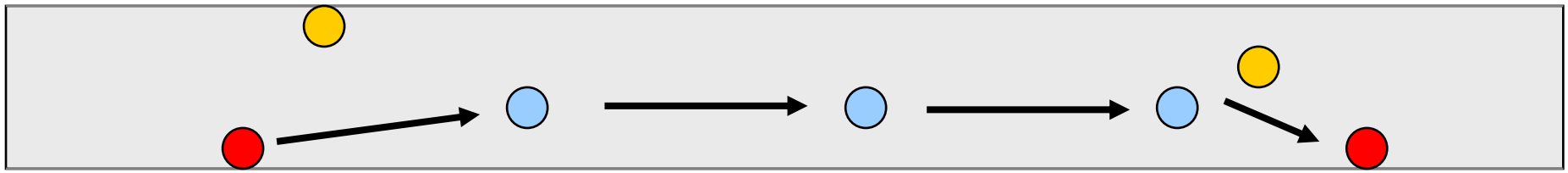
2

4

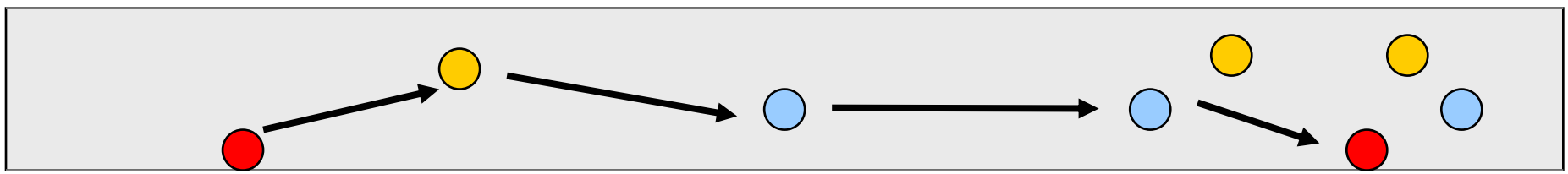
6 Destination

Position-based routing: advantages

Time t



Time t+1s



- No setup/maintenance of routes required
- Next hops are determed ‘on the fly’
- Can therefore cope with highly dynamic networks
- Supports geocast [NI97]

Position-based routing: building blocks

Positioning

- Get own position

Position Service

- Get current position of an (arbitrary) node

Forwarding Strategy

- Determine next hop
  - based on own position, neighbor‘s positions, position of the destination, maybe also based on source’s position.

Position (location) service

- Distributed service, can be classified w.r.t.:
  - Number of nodes that run the service (called position server)
  - for a position server: for ‘how many’ nodes does the server maintain current position information.
- Operation:
  - Position Update (node to server)
  - Position Request

class	*example*	*traditional classification*
all-for-one	**RLS**	**reactive**
all-for-some	**HomeZone, Grid LS**	**proactive/reactive**
some-for-some	**Quorum systems**	**proactive/reactive**
all-for-all	**DREAM**	**proactive**

Position service: examples

- Reactive Location Service (RLS) [KFHM02]
  - Each node respons to position request targeting their own ID
  - Similar to *route discovery* of a reactive topological approach, e.g. DSR or AODV

- Homezone (Terminodes Project) [GH99]
  - Replaces a GSM ‘home location register’: Hash function ***f(ID)*** determines a geographic region, in which all nodes have to maintain the current positional information on the node with identifier ID.

Forwarding strategies (examples)

- ‘Most forward within R’ (MFR) [TK84]
- ‘Greedy forwarding’ [F87]
- ‘Nearest with forward progress’ (NFP) [HL86]
- ‘Compass routing’ [KSU99]

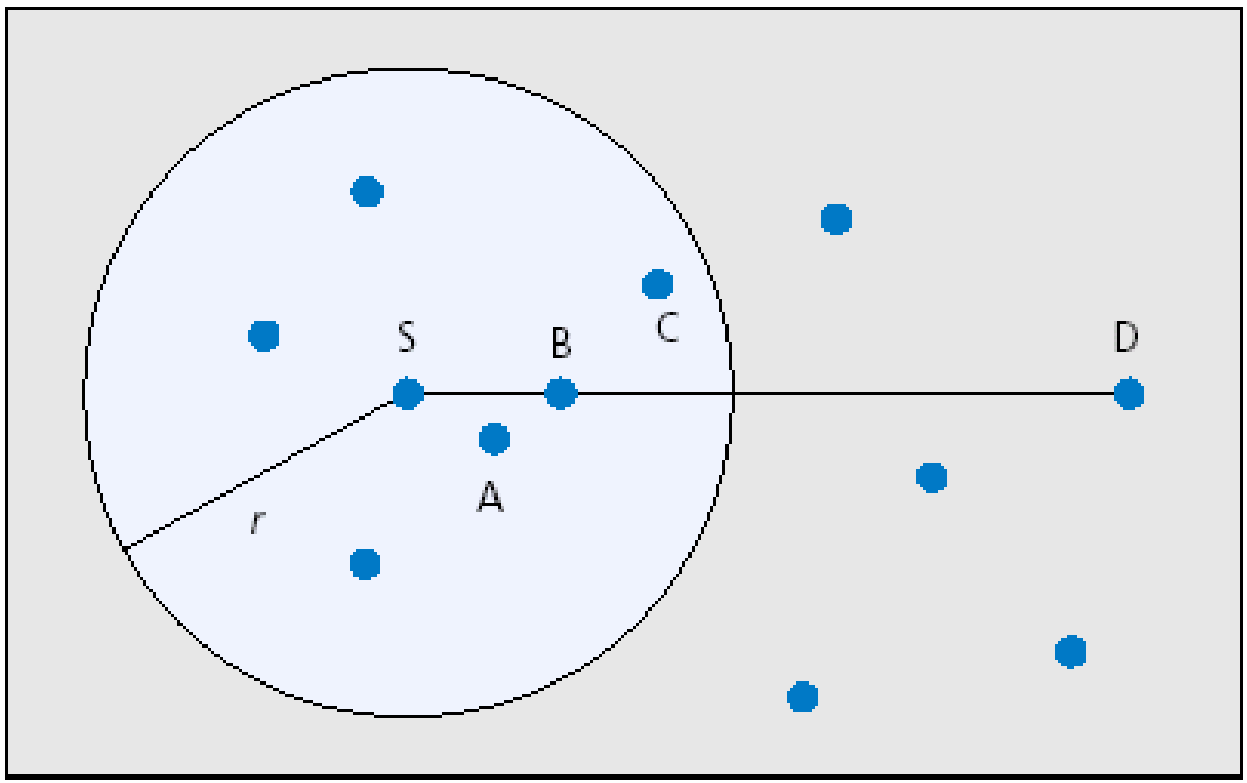


Figure 5. *Greedy routing strategies.*

MFR,Greedy: C

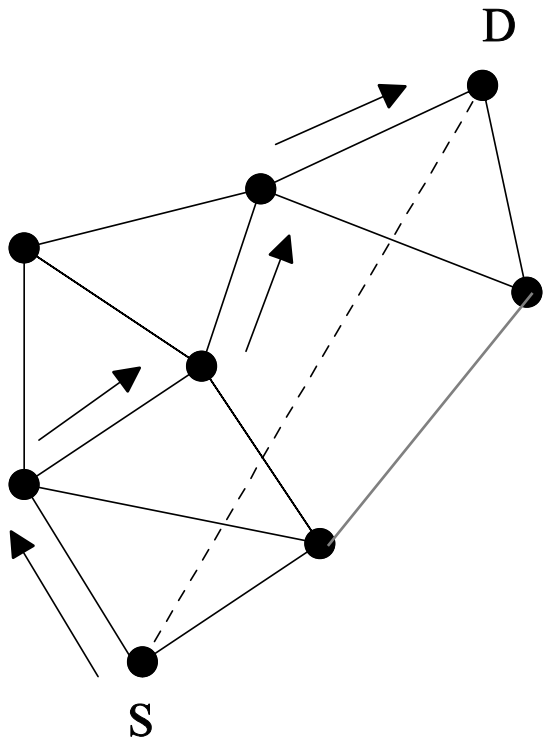
NFP: A

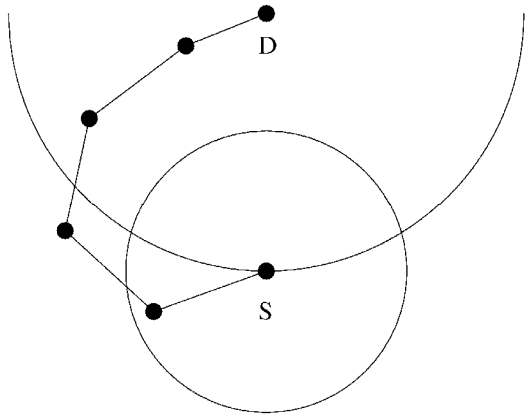
Compass: B

Forwarding when trapped in a local optimum

face-2 [BMSU99]
Perimeter-Routing
[KK00]

Assumption: planar graph



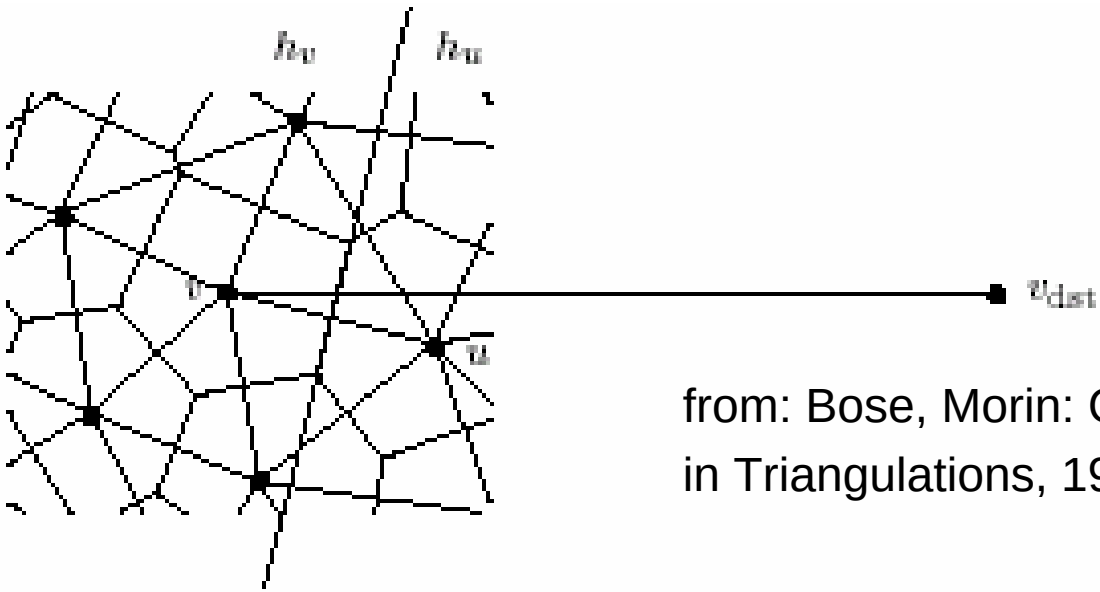


Challenge: ‘Stability’ of planarization in realistic mobile ad hoc networks

- asymmetric links, radio obstacles [see, e.g., B. N. Karp’s work]
- mobility
- position inaccuracy

Theoretical results

- “Online routing in planar graphs”, “Online routing in triangulation”: various papers by Bose et al.
- Example: Theorem. On a Delaunay-triangulation, ‘Greedy Routing’ always finds the destination (but: it’s not competitive) [BM99]



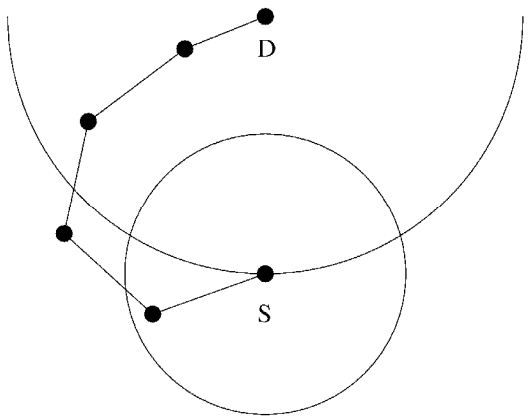
from: Bose, Morin: Online Routing in Triangulations, 1999

- **[KWZ02]: ‚Worst Case Theorem‘: Let *c* denote the length of the shortest route for a given source-destination pair. Every deterministic geographic routing algorithm requires $\Omega(c^2)$ steps to find the optimal route.**
- **[KWZ02]: AFR algorithm is asymptotically optimal.**

Comparison: topology- vs position-based routing

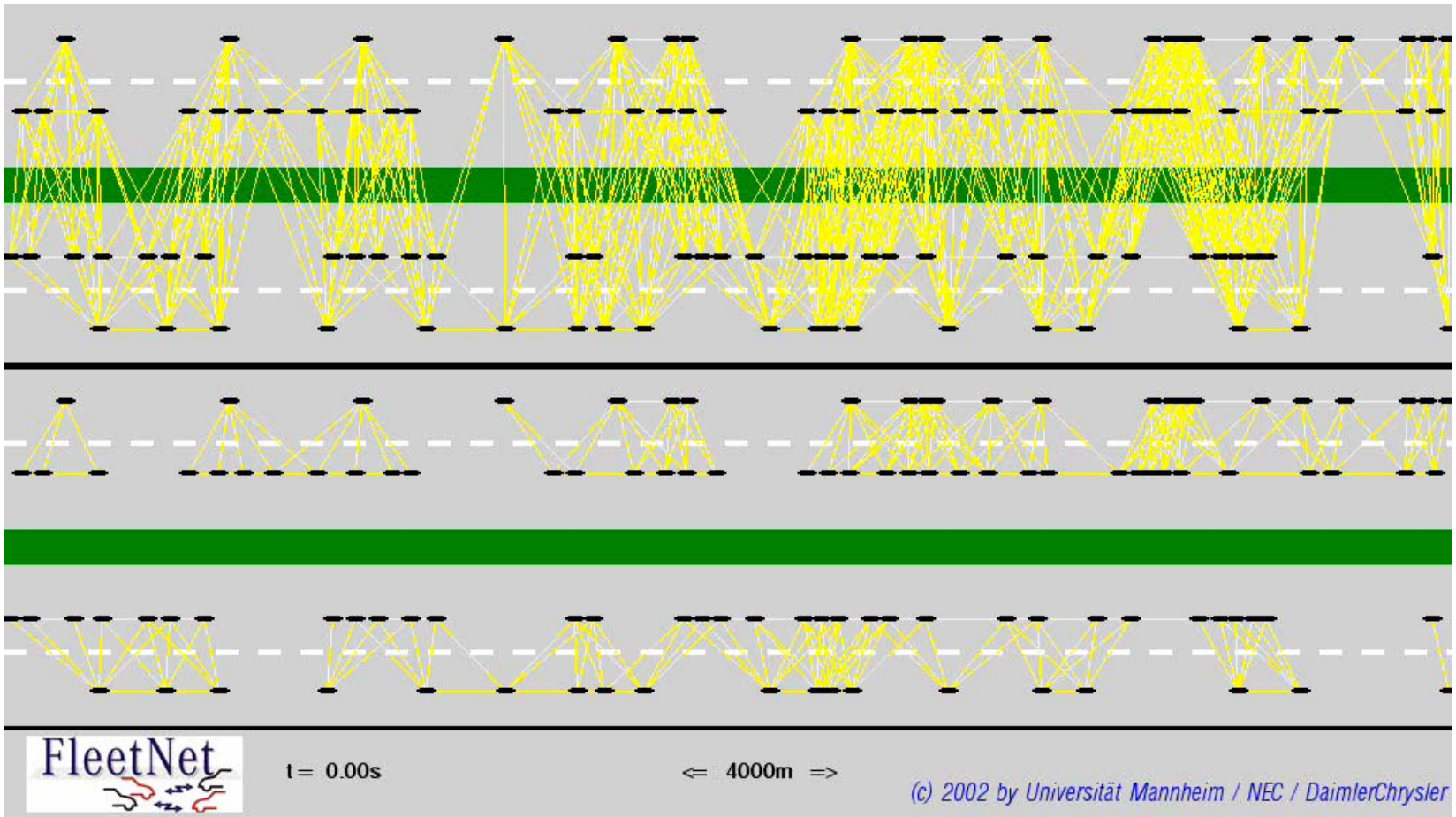
Task	*Topology-based*	*Position-based*
Find node	Route Discovery	Position Service
Deal with mobility of		
- intermediate nodes:	Route Maintenance	Forwarding on the fly
- destination:	Route Maintenance	Dead Reckoning

Challenges for
position-based routing:
(radio-) obstacles and voids!

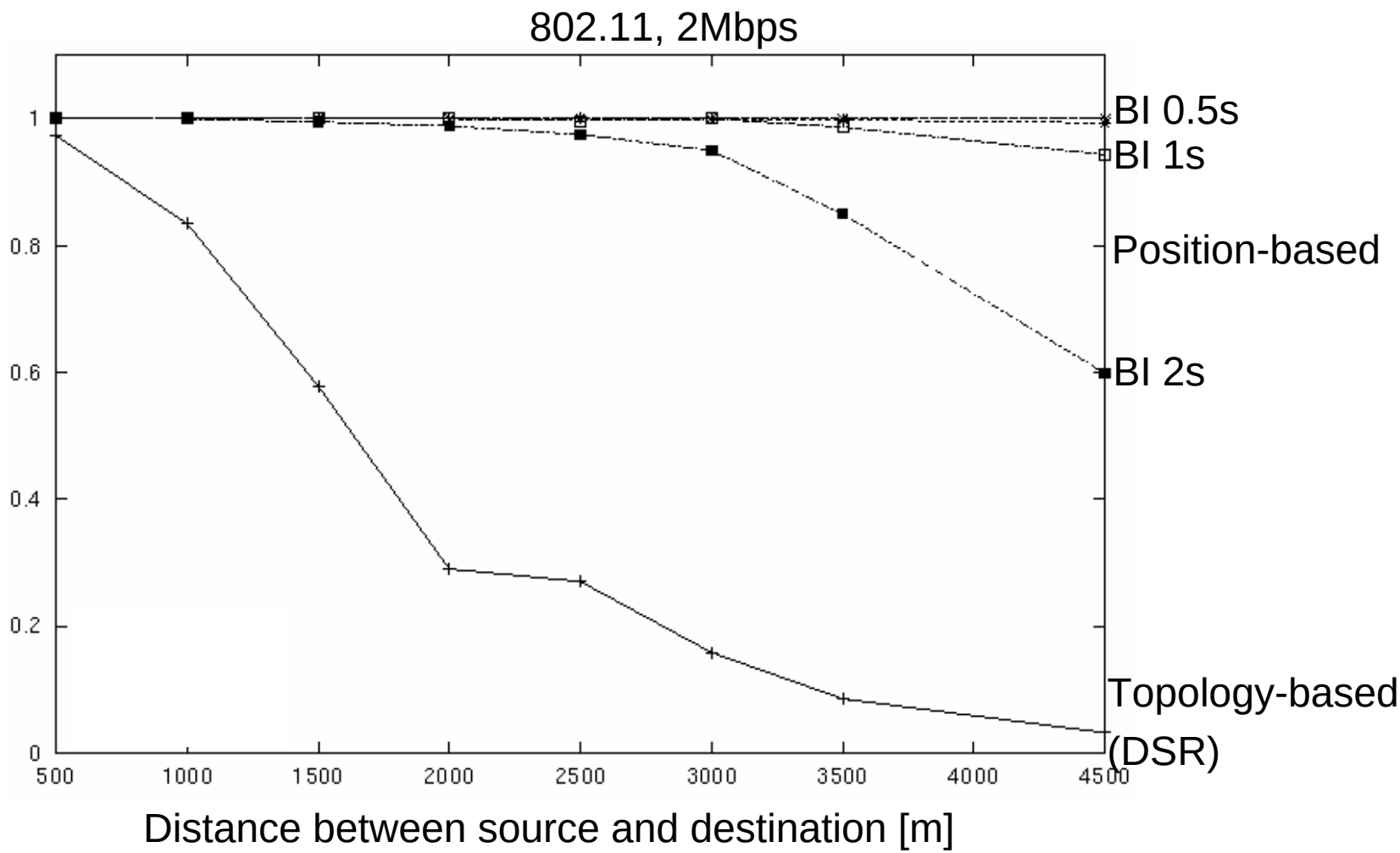


Case study: inter-vehicle communications

Simulation study on top of realistic vehicle movement patterns



Case study: packet delivery rate (highway)

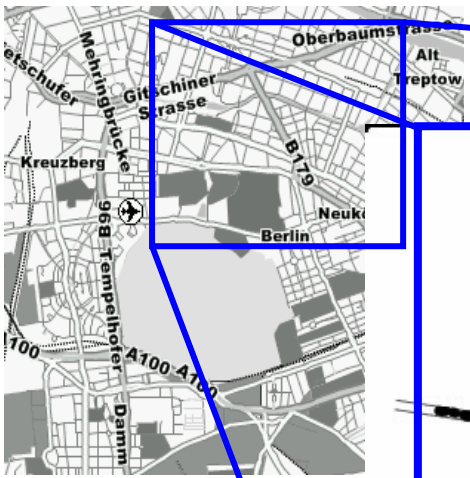


Case study: costs (highway)

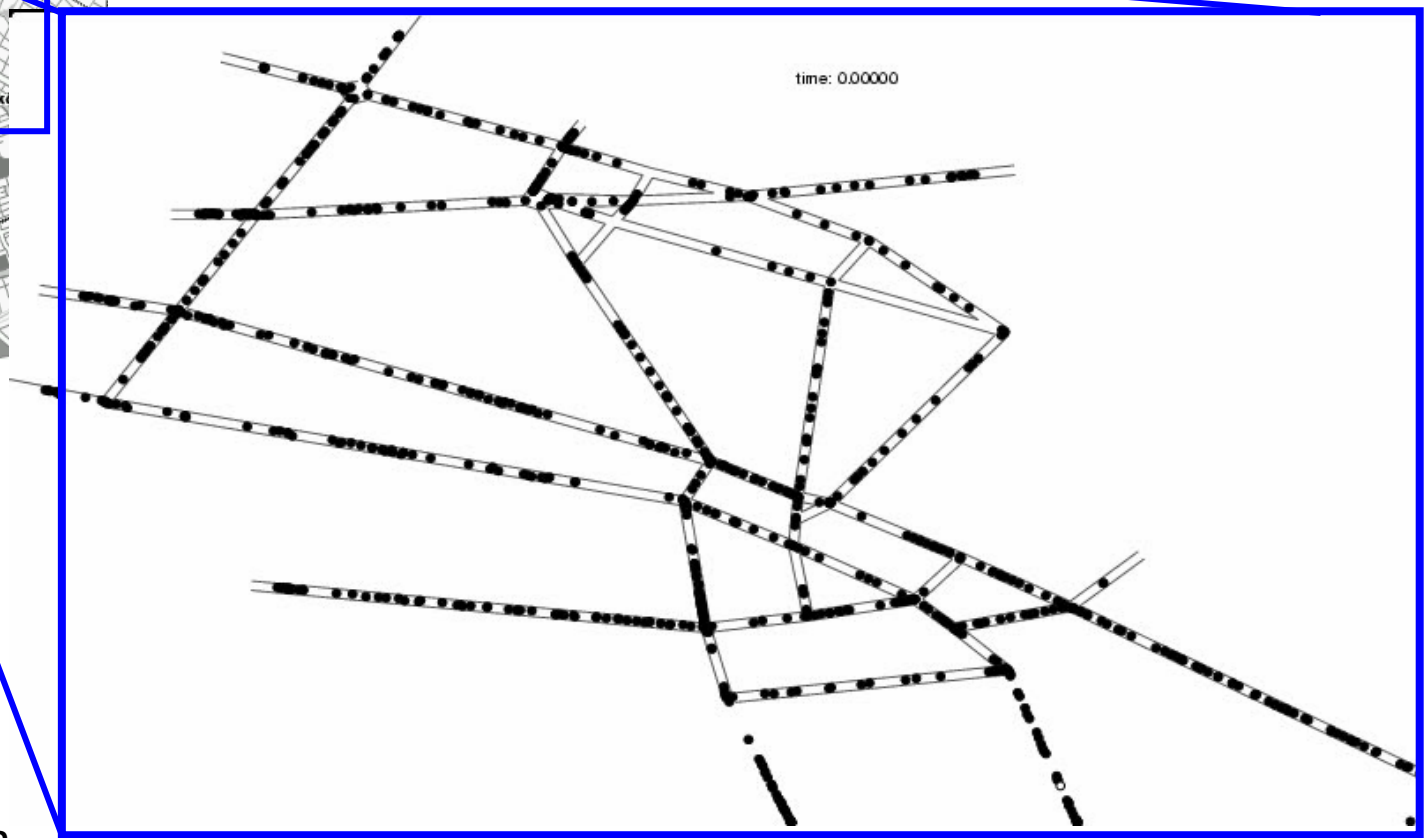
- Bandwidth:
  - DSR: significanly higher overhead compared to position-based routing
  - Since ‘source route’ is specified in each header

- Number of ‘one-hop transmissions’
  - for distances of 1500m and higher: position-based routing more efficient than DSR
  - for lower distances: ‘beaconing’ overhead (not required for DSR)

Case study: city scenario



[Hermann, DCAG]



6250m x 3450m

28 junctions

67 streets

32,29km total length

955 vehicles

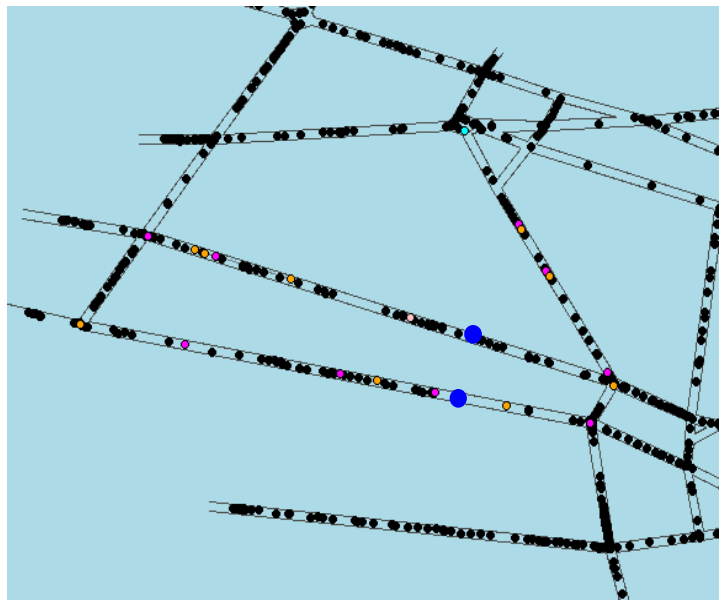
Case study: challenges of city scenarios

Radio propagation modeling:

- simple model implemented in NS-2 to account for ‘radio obstacles’
- Weakens semantics of positional information

Problems of ‘Perimeter-Mode’

- wrong direction?
- distributed planarization: connectivity ‘damaged’ by radio obstacles.
- too many hops.



Case study: routing in city scenarios

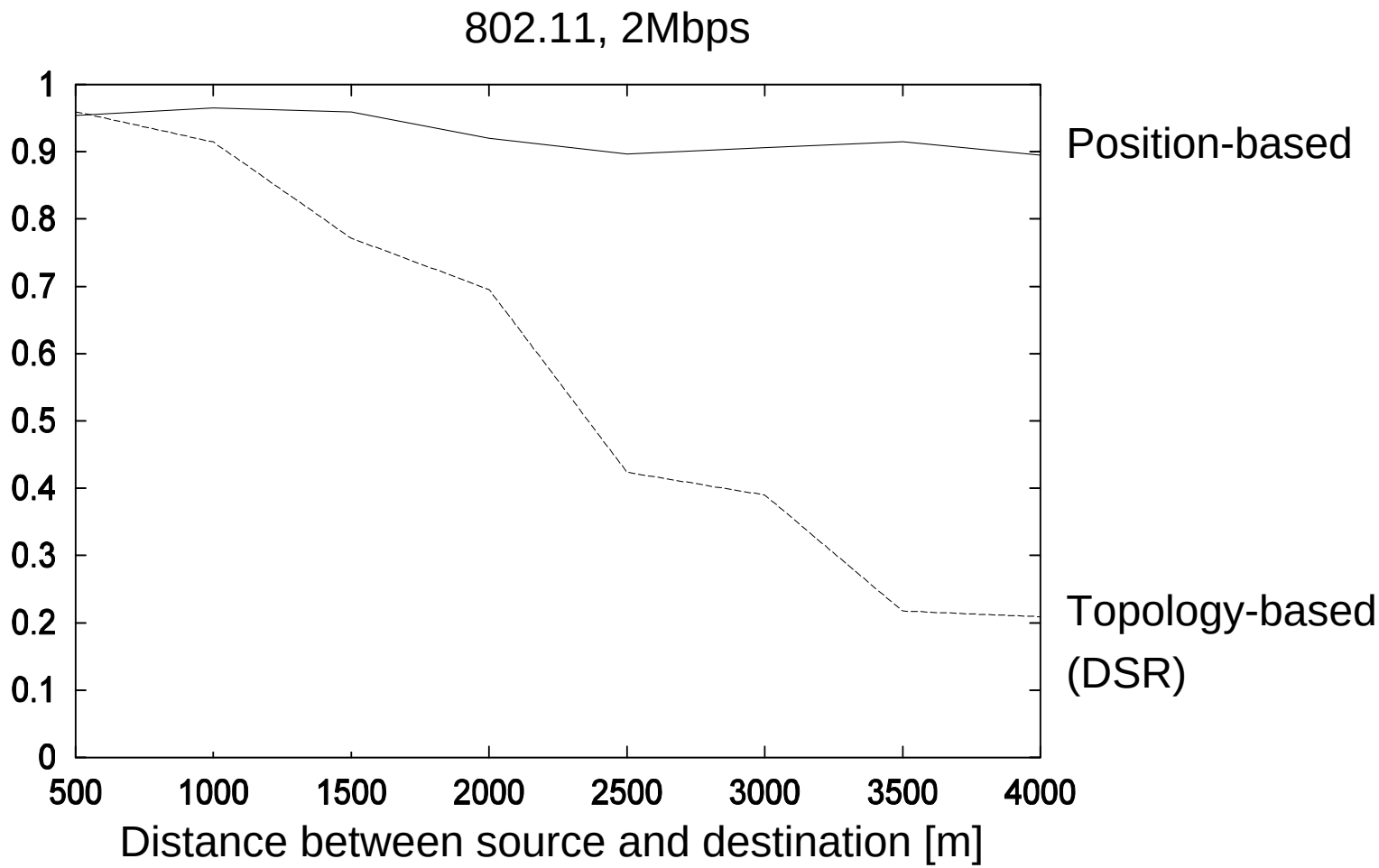
Geographic ‘Source Routing’ (GSR)

- Assumption: each vehicle has access to digital map of city
- Compute shortest path on ‘street graph’ to a communication partner.
- Sequence of junctions can be put into the packet header.
  - Combines advantages of topology-based and position-based routing.

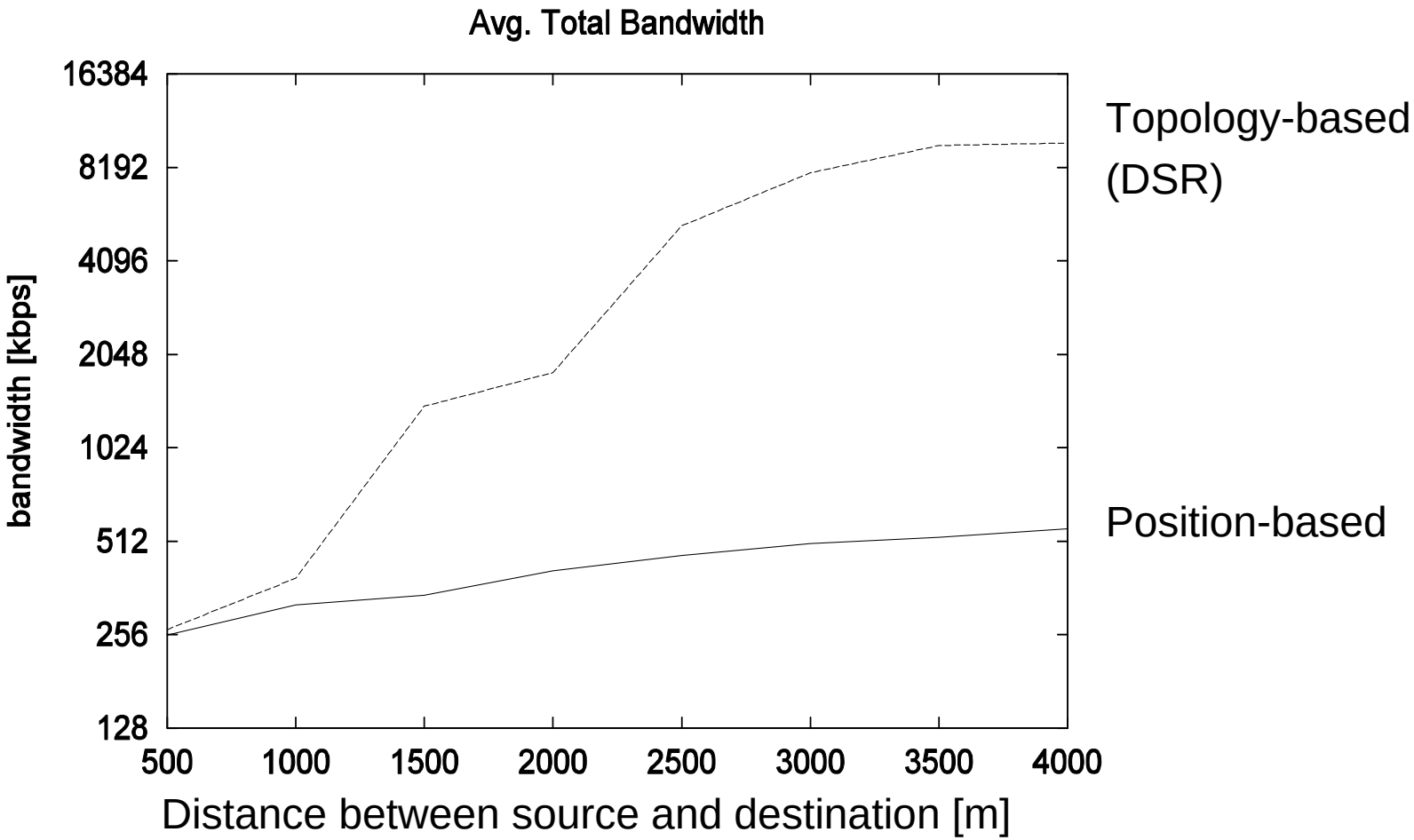
Not required!

Could also be computed by each node separately.

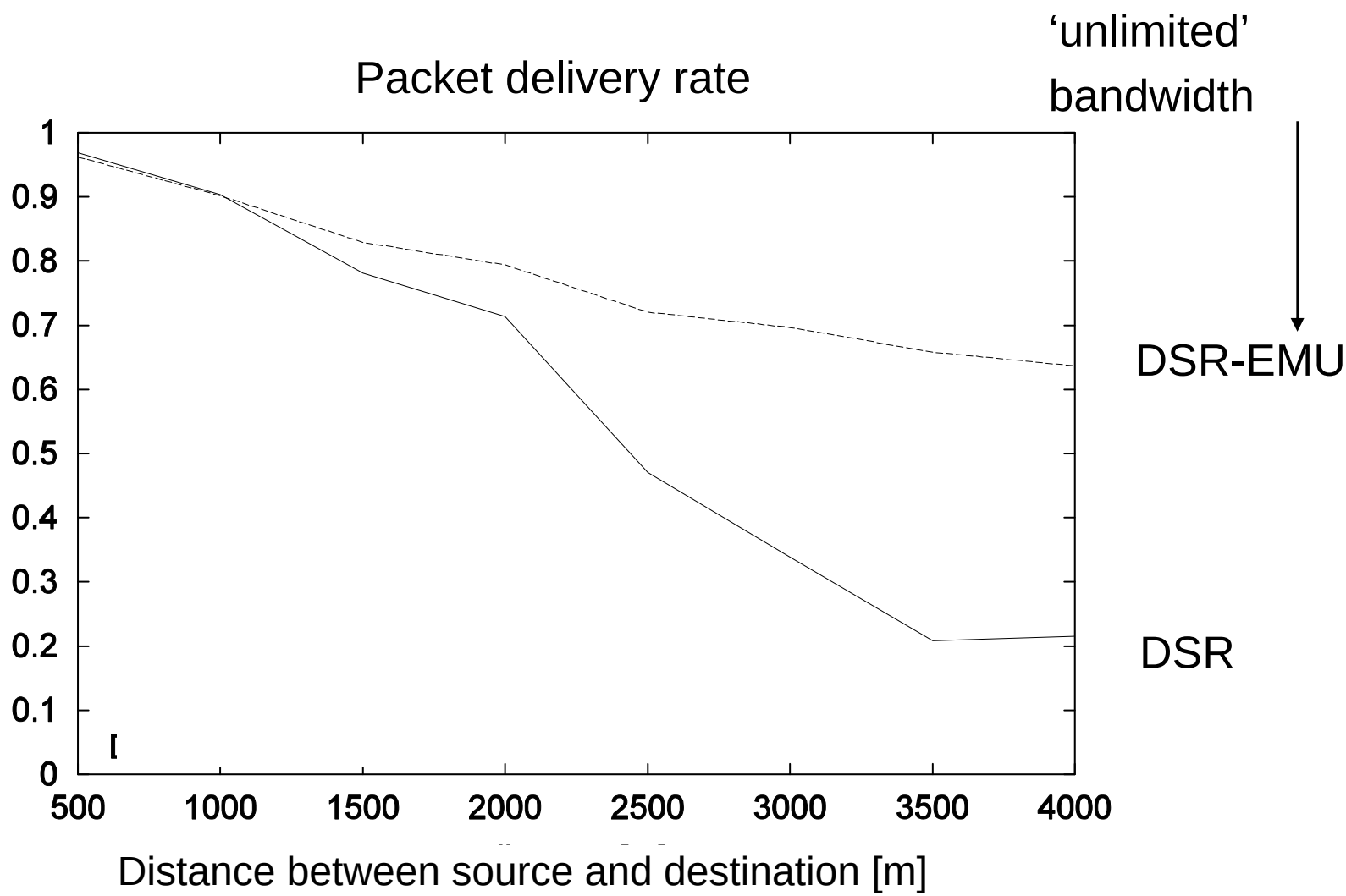
Case study: packet delivery rate (city scenario)



Case study: bandwidth costs (city scenario)



Case study: DSR



History / Future

- 1972: DARPA: PRNet – Packet Radio Network
- 1978: first GPS satellite in space
- 1984: H. Takagi, L. Kleinrock, *Optimal transmission ranges for randomly distributed packet radio terminals*, IEEE Trans. on Communications, March 1984
  - MFR: first position-based‘greedy forwarding’ für ‘ad hoc’
- 1994: 24 GPS satellites in space (completed)
- A lot of papers in the late 90’s
  - GPS available and relatively inexpensive
- 2000: Terminodes Project (now: NCCR-MICS) started in Switzerland.

- 2008: Galileo
- Position-based routing for inter-vehicle communication
- Position-based routing for sensor networks

Some open issues

- Position-based multicast
- Load balancing, fairness
- What is the ‚optimal' location service – given some communication patterns?
- Routing in 2D scenarios with radio obstacles
- Security, confidentiality of routing information

References

General:

- [MWH01] M. Mauve, J. Widmer, H. Hartenstein, A survey on position-based routing in mobile ad hoc networks, IEEE Network, Nov/Dec 2001.
- [GS02] S. Giordano, I. Stojmenovic, Position-based ad hoc routes in ad hoc networks, in: M. Illyas (ed.), The Handbook of Ad Hoc Wireless Networks, CRC Press, 2002.

Positioning w/o GPS:

- [CHH01] S. Capkun, M. Hamdi, J.-P. Hubaux, GPS-free positioning in mobile ad hoc networks, HICSS 2001.
- [IS03] R. Iyengar and B. Sikdar, Scalable and Distributed GPS Free Positioning for Sensor Network, IEEE ICC 2003.

Geocast:

- [NI97] J. Navas, T. Imielinski, GeoCast – geographic addressing and routing, ACM Mobicom, Budapest, 1997.

References

Location services:

- [KFHM02] M. Käsemann, H. Füßler, H. Hartenstein, M. Mauve, A reactive location service for mobile ad hoc networks, Technical Report TR-14-2002, Dept. Computer Science, University of Mannheim, Nov. 2002.
- [GH99] S. Giordano, M. Hamdi, Mobility Management: The Virtual Home Region, Technical Report SSC/1999/037, EPFL-ICA, 1999.
- [LJCKM00] J. Li, J. Jannotti, D. De Couto, D. Karger, R. Morris, A scalable location service for geographic ad hoc routing, ACM Mobicom, Boston, 2000.
- [BCSW98] S. Basagni, I. Chlamtac, V. R. Syrotiuk, B. A. Woodward, A distance routing effect algorithm for mobility (DREAM), ACM Mobicom, Dallas, 1998.

Forwarding strategies:

- [TK84] H. Takagi, L. Kleinrock, *Optimal transmission ranges for randomly distributed packet radio terminals*, IEEE Trans. on Communications, March 1984.
- [F87] G. Finn, *Routing and addressing problems in large metropolitan-scale Internetworks*, ISI Research Report ISU/RR-87-180, March 1987.

References

- [HL86] T.-C. Hou, V. Li, Transmission range control in multihop packet radio networks, IEEE Trans. Communications, Jan. 1986.
- [KSU99] E. Kranakis, H. Singh, J. Urrutia, Compass routing on geometric networks, Proc. 11th Canadian Conf. Computational Geometry, Vancouver, Aug. 1999.
- Recovery strategies:
- [BMSU99] P. Bose, P. Morin, I. Stojmenovic, J. Urrutia, Routing with guaranteed delivery in ad hoc wireless networks, Proc. 3rd ACM Wksp. Discrete Algorithms and Methods for Mobile Comp. and Commun., 1999.
- [KK00] B. Karp, H. Kung, Greedy perimeter stateless routing for wireless networks, ACM Mobicom, Boston, 2000.

Algorithm-theoretical results:

- [BM99] P. Bose and P. Morin, Online routing in triangulations. In *Proceedings of the Tenth International Symposium on Algorithms and Computation (ISAAC'99)*, volume 1741 of *LNCS*, pages 113-122. Springer-Verlag, 1999.

References

- [KWZ02] F. Kuhn, R. Wattenhofer, A. Zollinger, Asymptotically optimal geometric mobile ad-hoc routing, ACM DIAM M, Atlanta, Sept. 2002.

Inter-vehicle communications:

- FleetNet Projekt: www.fleetnet.de
- M. Mauve, H. Hartenstein, H. Füßler, J. Widmer, W. Effelsberg, Positionsbasiertes Routing für die Kommunikation zwischen Fahrzeugen, it + ti 44 (5), S. 278--286, Oktober 2002.
- H. Füßler, M. Mauve, H. Hartenstein, M. Käsemann, D. Vollmer, Location-Based Routing for Vehicular Ad-Hoc Networks, Poster bei der ACM MobiCom '02, Atlanta, 2002; Abstract wird erscheinen in: ACM MC2R.
- C. Lochert, H. Hartenstein, J. Tian, H. Füßler, D. Hermann, M. Mauve, A routing strategy for vehicular ad hoc networks in city environments, akzeptiert für IEEE Intelligent Vehicles Symposium 2003.

Information Diffusion in Sensor Networks

Hannes Hartenstein, NEC Europe Network Labs

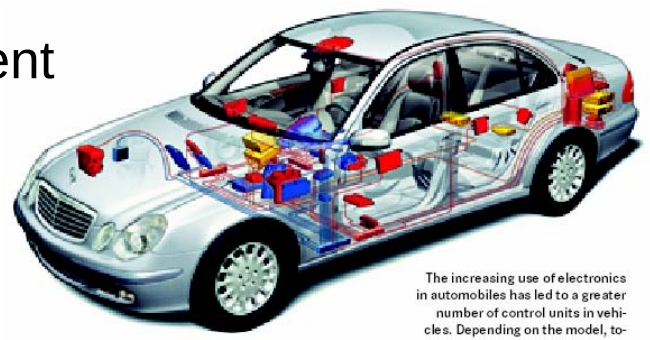
Berkeley Motes

Hitachi's mu chip
- not yet a sensor ...

Weather station

Building management

(C) Siemens



(C) DaimlerChrysler Media Services

Sensor network structures

Static, but self-configuring or self-organizing sensor networks

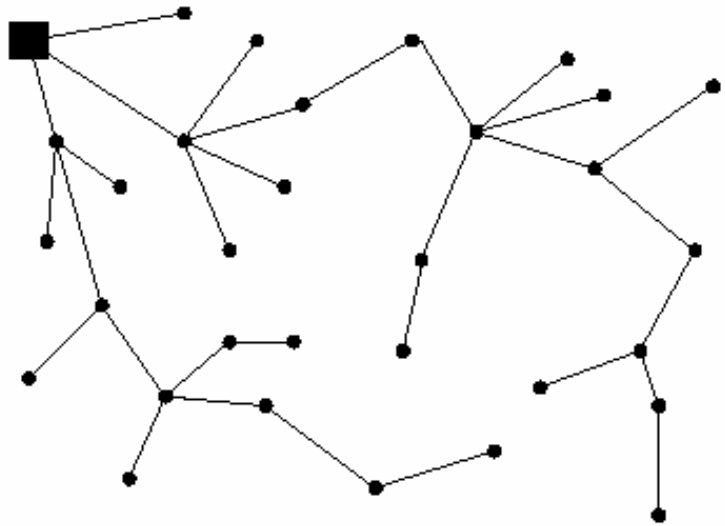


Fig. 4. A representative topology constructed using TinyOS beaconing with a single base station.

From: Karlof/Wagner

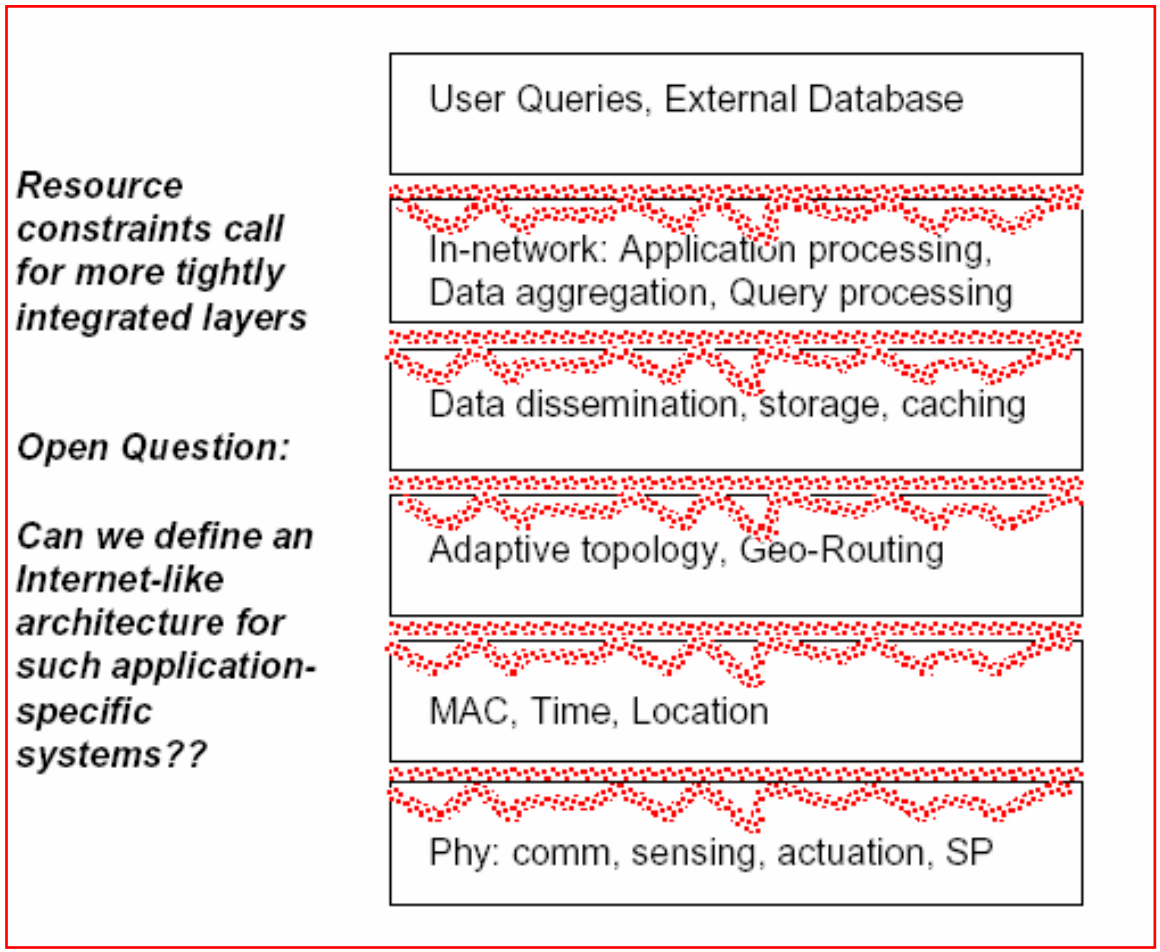
Mobile self-configuring or self-organizing sensor networks

Sensor networks: an interdisciplinary Field

- Look, e.g., at NSF's Sensor and Sensor Networks program 03-512:
- Topical areas:
  - Designs, materials and concepts for new sensors and sensing systems
  - Arrayed sensor networks and networking
  - Interpretation, decision and action-based on sensor-data

Sensor networks: communication model

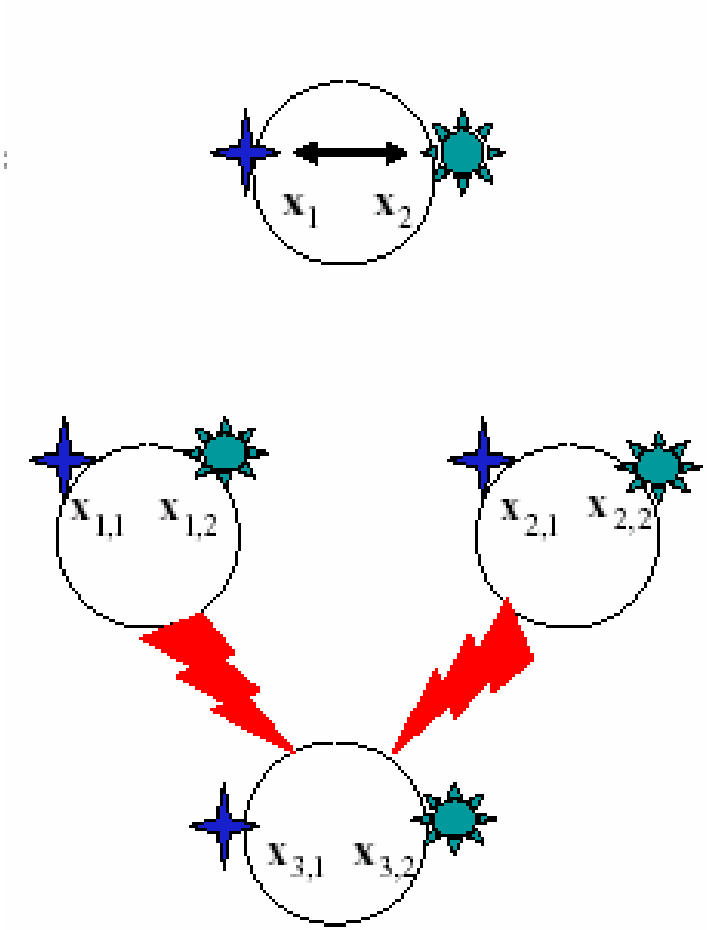
- Machine-to-Machine, or Machine-to-Man
- Application-specific



From: Mobicom Tutorial 2002

Collaborative (distributed) signal processing

- Vertically/horizontally
  - intra-node collaboration: combining multiple sensing modalities
  - inter-node collaboration: combining measurements of different nodes, particularly to increase ‘confidence’ in measurements.



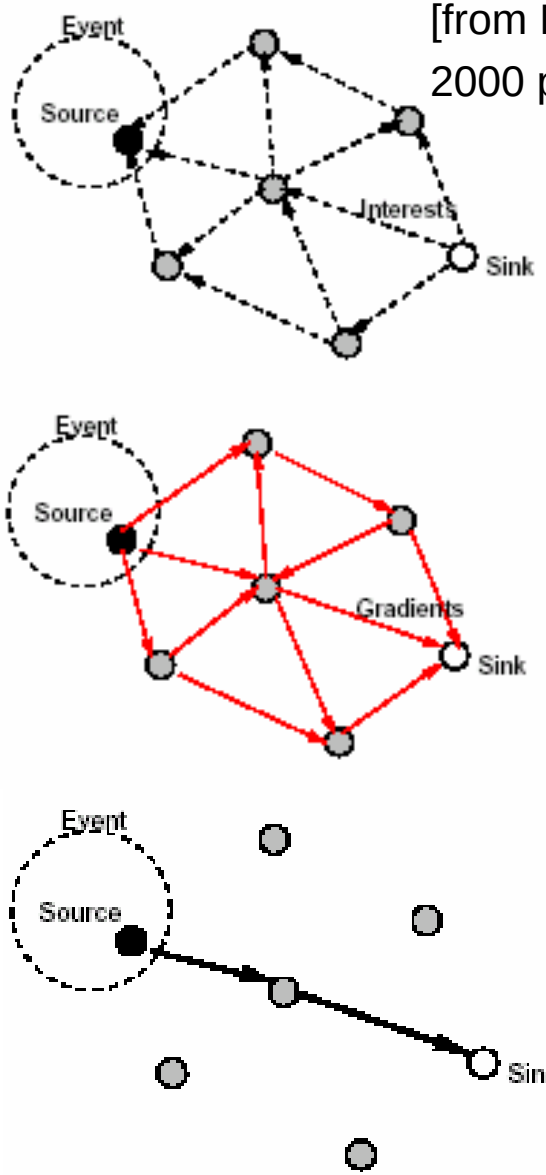
From: Mobicom 2002 Tutorial

Directed diffusion: basics

- Seminal paper by Intanagonwiwat, Govindan, Estrin, Mobicom 2000.

- Basic idea:
  - Diffuse ‘interest’, i.e., monitoring task, in the network, thereby setting up reverse paths to the node requesting the task and some soft state
  - Diffuse responses but optimize path with gradient-based feedback.
  - Supports in-network data aggregation and processing

[from Mobicom 2000 paper]



Directed diffusion: naming

```
type      = four-legged animal
interval  = 20ms
duration  = 10s
rect      = [-100, 100, 200, 400]
```

Interest

```
type       = four-legged animal
instance   = elephant
location   = [125,220]
intensity  = 0.6
confidence= 0.85
timestamp  = 01:20:40
```

Response

No source-destination addresses!

Directed diffusion: gradients

- Every node maintains an ‘interest cache’ (soft state).
  - Cache entry: `interest : timestamp : gradient(s)`
    - Gradient: `r-neighbor : data rate : duration`
- ‘Sink’ broadcasts interest periodically to all one-hop neighbors.
- After receiving an interest, a node may decide to re-send the interest to some neighbors.
  - Re-broadcast; leads to flooding.
  - Geographic routing.
  - Based on cached data.

- ‘Data rate’ can be tuned to first find nodes that actually can responed to an interest with moderate network load. Upon success, the data rate is increased but only for ‘suitable’ paths/nodes.

Directed diffusion: data propagation/reinforcement

- Sensor node in the interest's area sends data to all r-neighbors of this interest.
- Nodes receiving data
  - check with their interest cache
  - check with their data cache
  - re-send data again, maybe with 'downconversion'.
- Sink might reinforce a specific neighbor that appears to be 'optimal' w.r.t. some metrics.

Conclusions

Specific features of ‘Directed Diffusion’ and Sensor Networking:

- Data-centric dissemination
- Reinforcement-based adaptation to the emperically best path
- In-network data aggregation and caching.

References

- C. Inatagonwiwat, R. Govindan, D. Estrin, *Directed Diffusion: a scalable and robust communication paradigm for sensor networks*, ACM Mobicom 2000.
- Mobicom 2002 Tutorial T5 “Wireless Sensor Networks” by D. Estrin, M. Srivastava, A. Sayeed, see also http://nesl.ee.ucla.edu/tutorials/mobicom02/
- C. Karlof, D. Wagner, *Secure routing in wireless sensor networks: attacks and countermeasures*, Elsevier's AdHoc Networks Journal, Special Issue on Sensor Network Applications and Protocols, Volume 1, Issues 2-3, pages 293-315 (September 2003)

Medium Access and Mobile Ad Hoc Networks

Martin Mauve, University of Düsseldorf

Medium Access Control

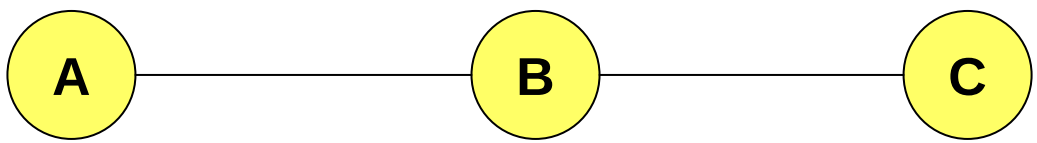
- So far:
  - nodes can communicate if in transmission range
- Reality is more complex:
  - Wireless channel is a shared medium
  - Need access control mechanism to avoid interference
- MAC protocol design has been an active area of research for many years [CGL00a]
- In this tutorial: IEEE802.11 [IEEE97a] (and its problems) for ad-hoc networks

IEEE 802.11 Wireless MAC

- Many ad-hoc network implementations use IEEE 802.11
- Reason: availability (no necessarily because it is well suited!)
- Distributed and centralized MAC components
  - Distributed Coordination Function (DCF)
  - Point Coordination Function (PCF)
- DCF often used for multi-hop ad hoc networking

Hidden Terminal Problem

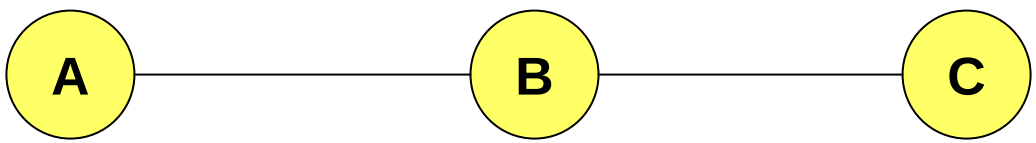
- Nodes should only transmit if the channel is free
  - carrier sensing
- Problem in wireless networks:
  - Node B can communicate with A and C both
  - A and C cannot hear each other
  - When A transmits to B, C cannot detect the transmission using the *carrier sense* mechanism
  - If C transmits, collision will occur at node B



- Hidden Terminal Problem [TK75a]

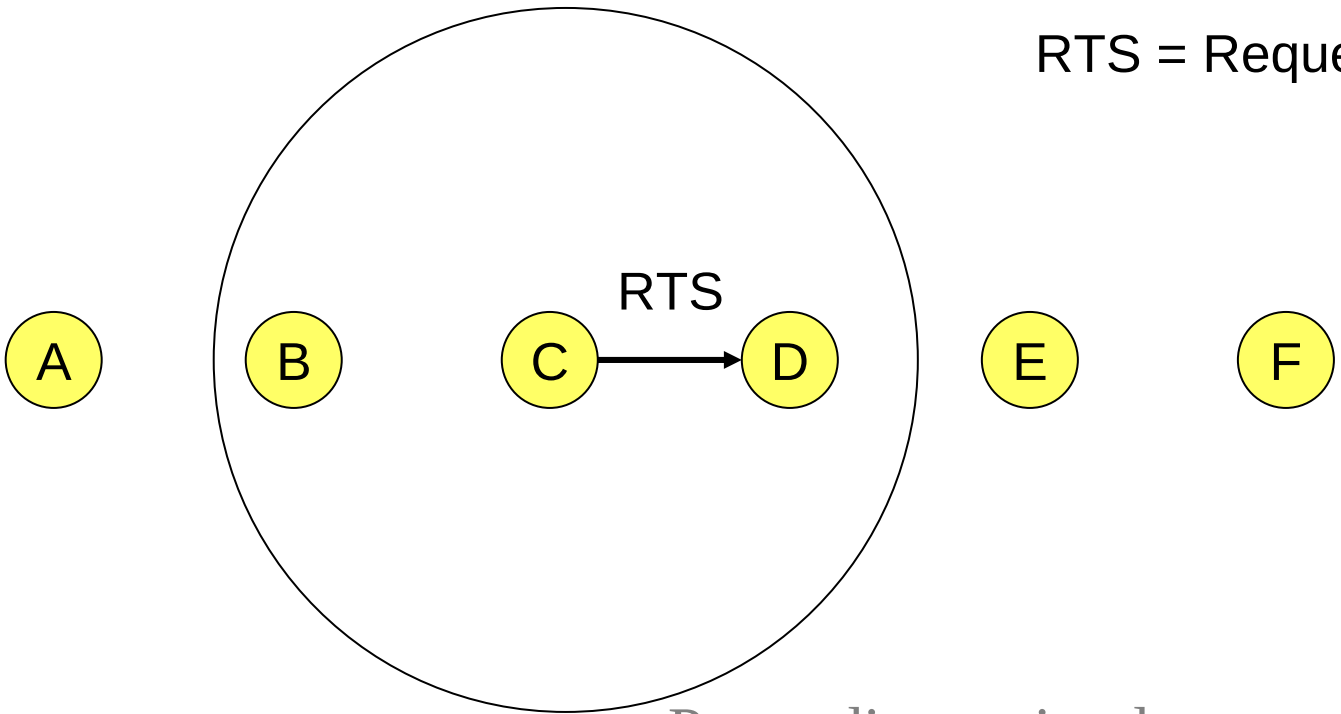
MACA Solution for Hidden Terminal Problem

- When node A wants to send a packet to node B, node A first sends a *Request-to-Send (RTS)* to B
- On receiving RTS, node B responds by sending *Clear-to-Send (CTS)*, provided node B is able to receive the packet
- When a node (such as C) overhears a CTS, it keeps quiet for the duration of the transfer
  - Transfer duration is included in both RTS and CTS

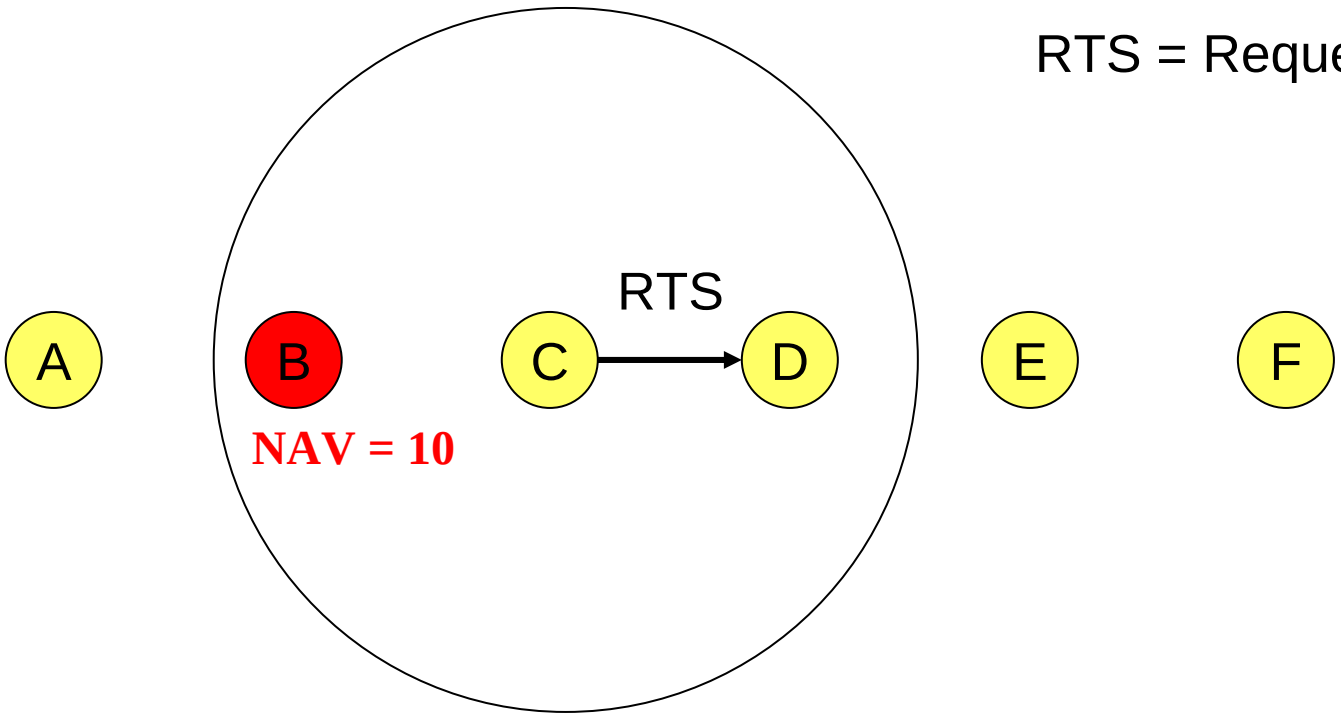


- This is called Multiple Access with Collision Avoidance (MACA) or virtual carrier sensing [Karn90a]

RTS/CTS Example

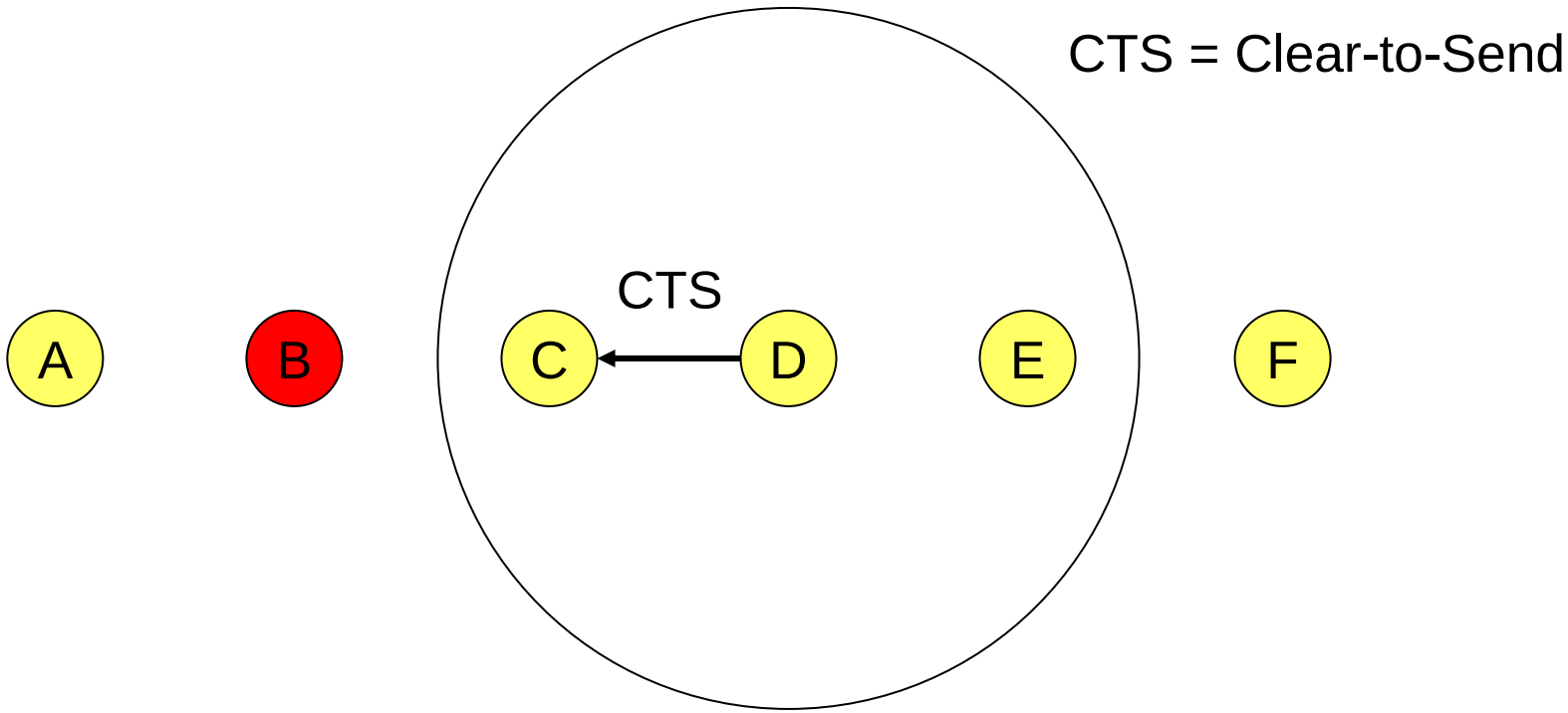


RTS/CTS Example

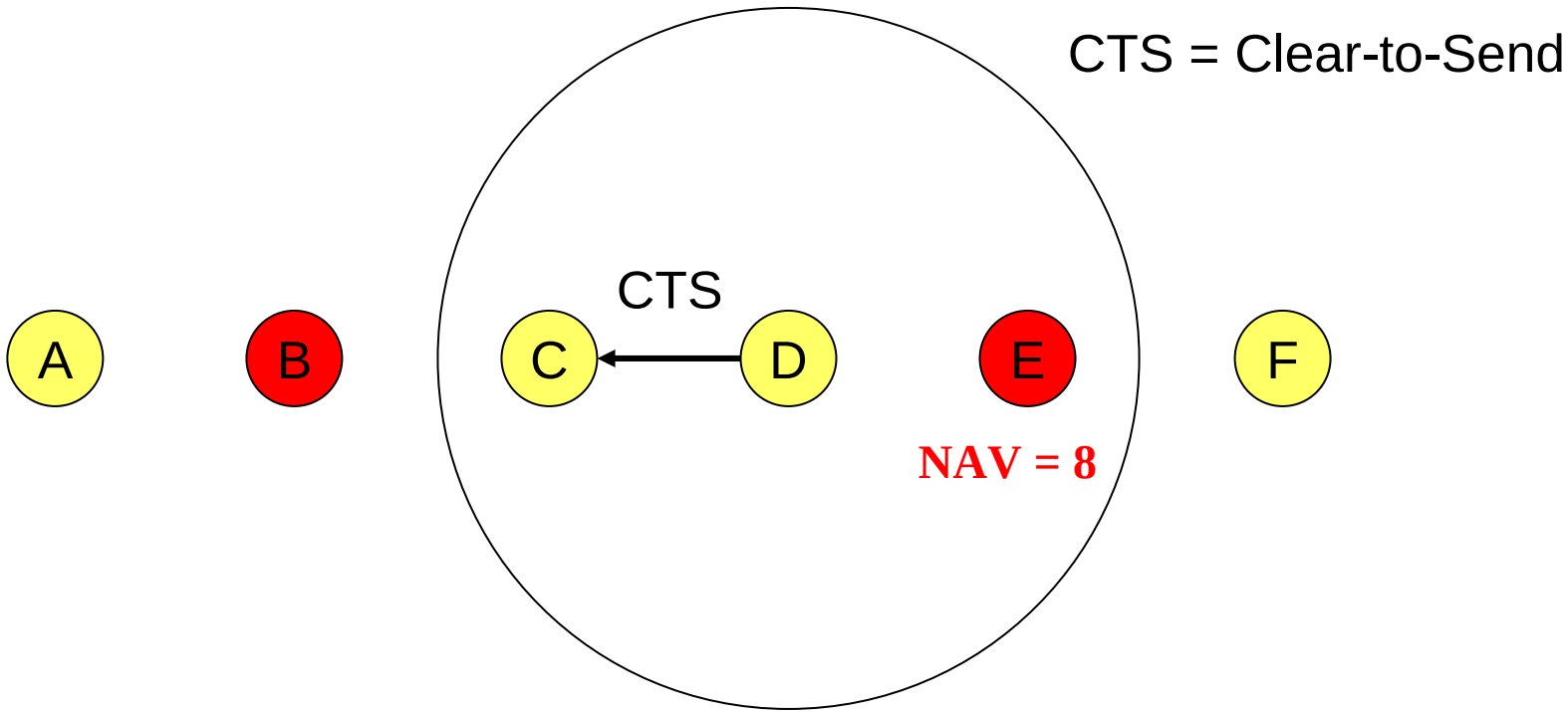


NAV (network allocation vector) = remaining duration to keep quiet

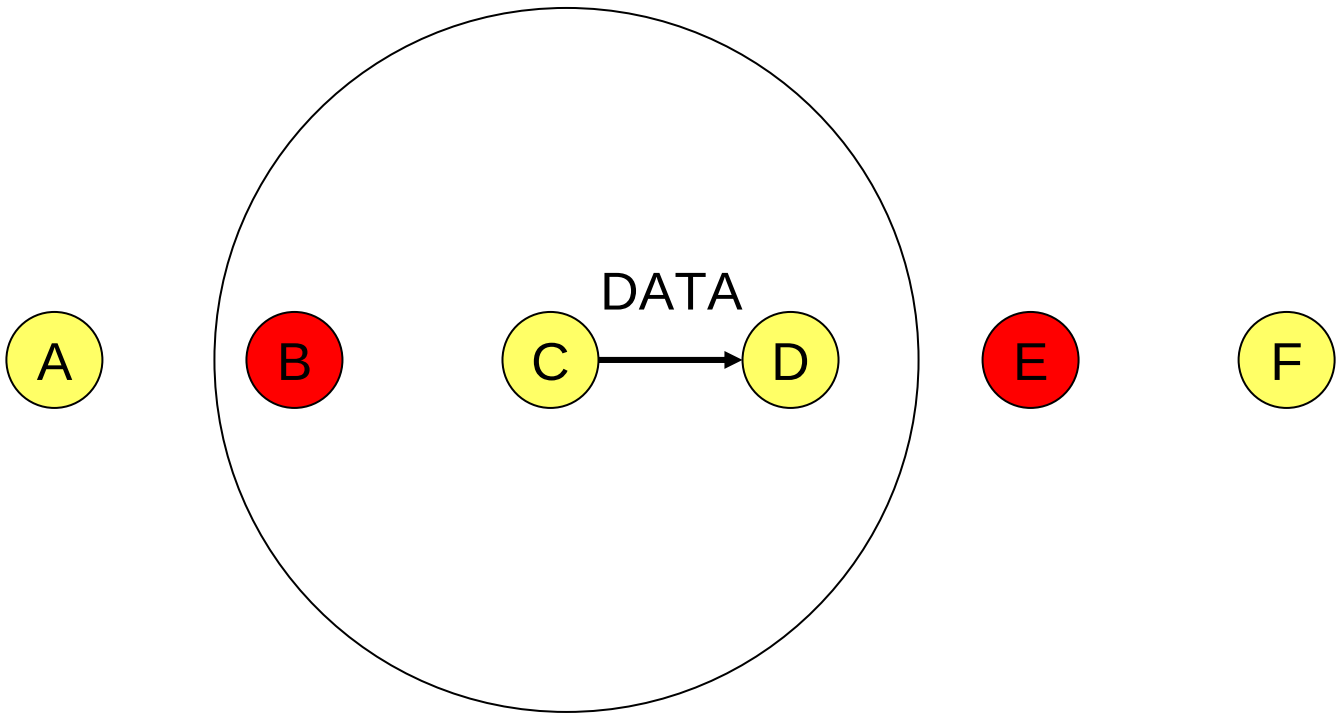
RTS/CTS Example



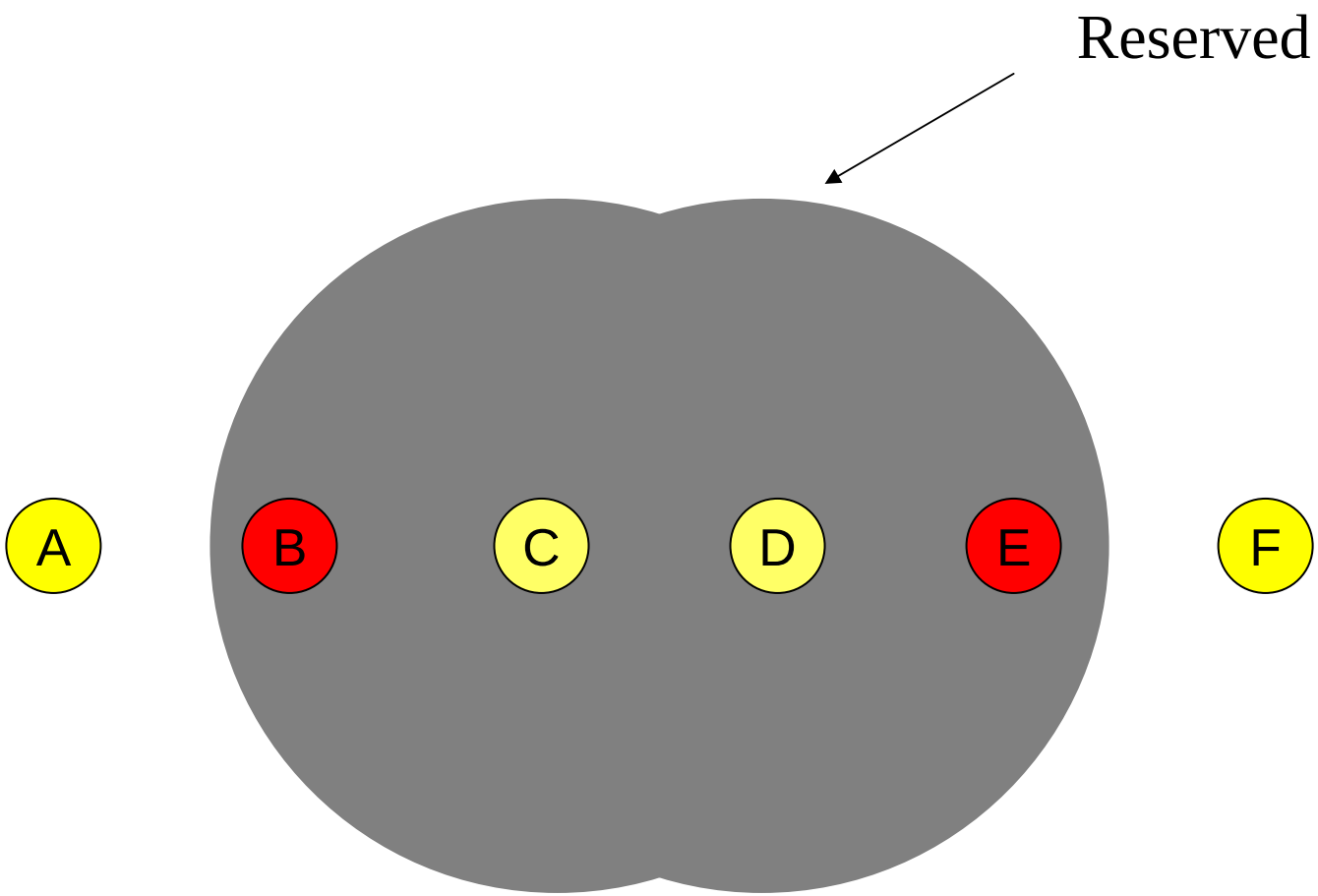
RTS/CTS Example



RTS/CTS Example



RTS/CTS Example



RTS/CTS in multi-hop Ad-Hoc Networks?

- Implicit assumption: nodes do not move (fast)
- Otherwise:
  - nodes may move into reserved area (and transmit)
  - nodes may leave reserved area (and still have to wait)
  - receiver may move and cause both problems

- Implicit assumption: RTS/CTS occupy only a small fraction of the available bandwidth
- May not be true for multi-hop ad-hoc networks:
  - linear decrease of per-node capacity with route length
  - remaining capacity per node will be very low
  - RTS/CTS may cause massive congestion

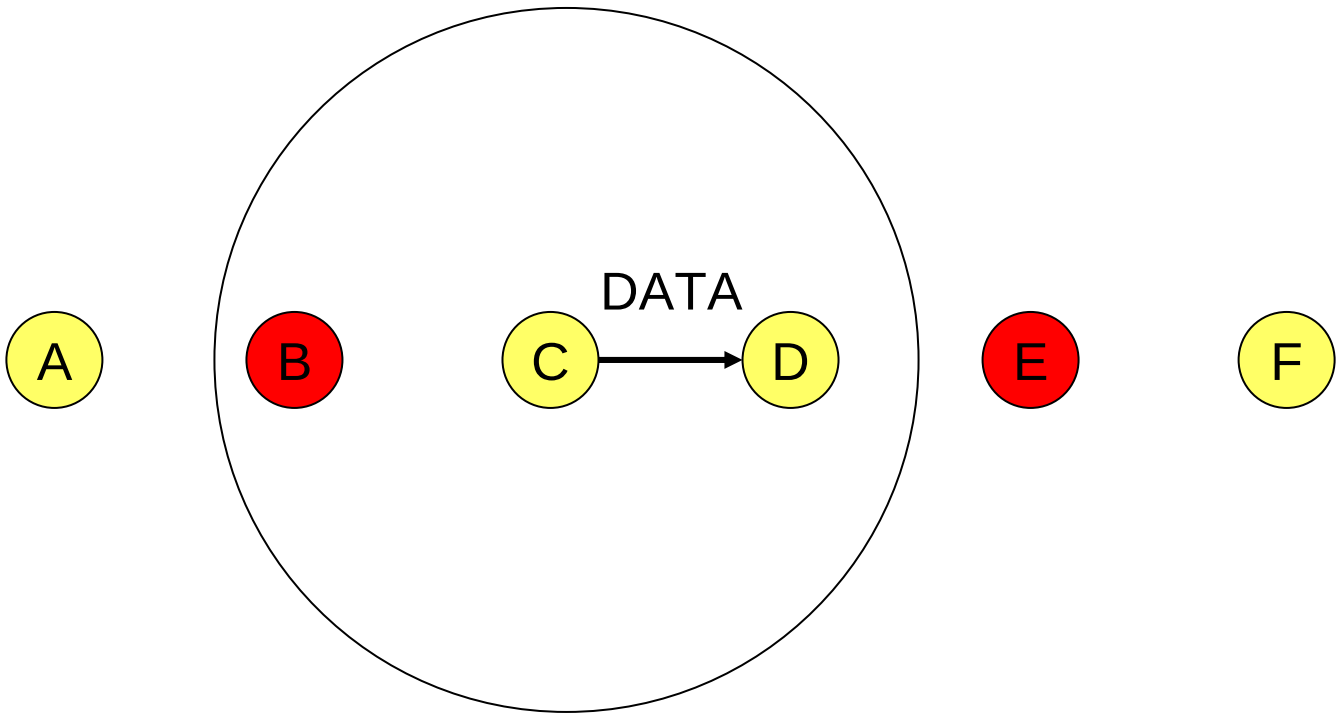
- Consequence:
  - RTC/CTS often turned off for highly mobile multi-hop ad-hoc networks

Reliability

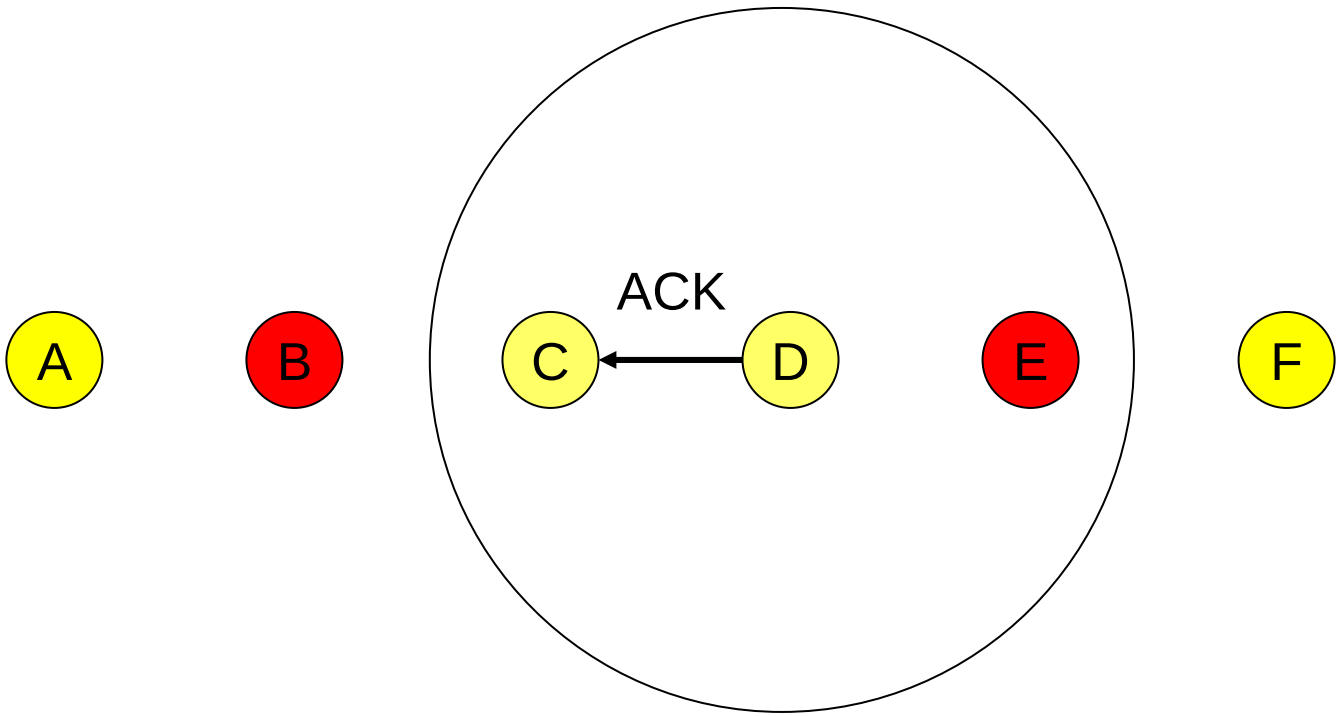
- Wireless links are prone to errors
  - either because of interference
  - or because of collisions
    (collision detection does not work for half-duplex radios)
- High packet loss rate detrimental to transport-layer performance
- Mechanisms needed to increase reliability:
  - Forward error correction (FEC) - include redundancy in the packet
  - Automatic repeat request (ARQ) - use ACKs and retransmissions

ARQ Example

- Successful data reception acknowledged using ACK.



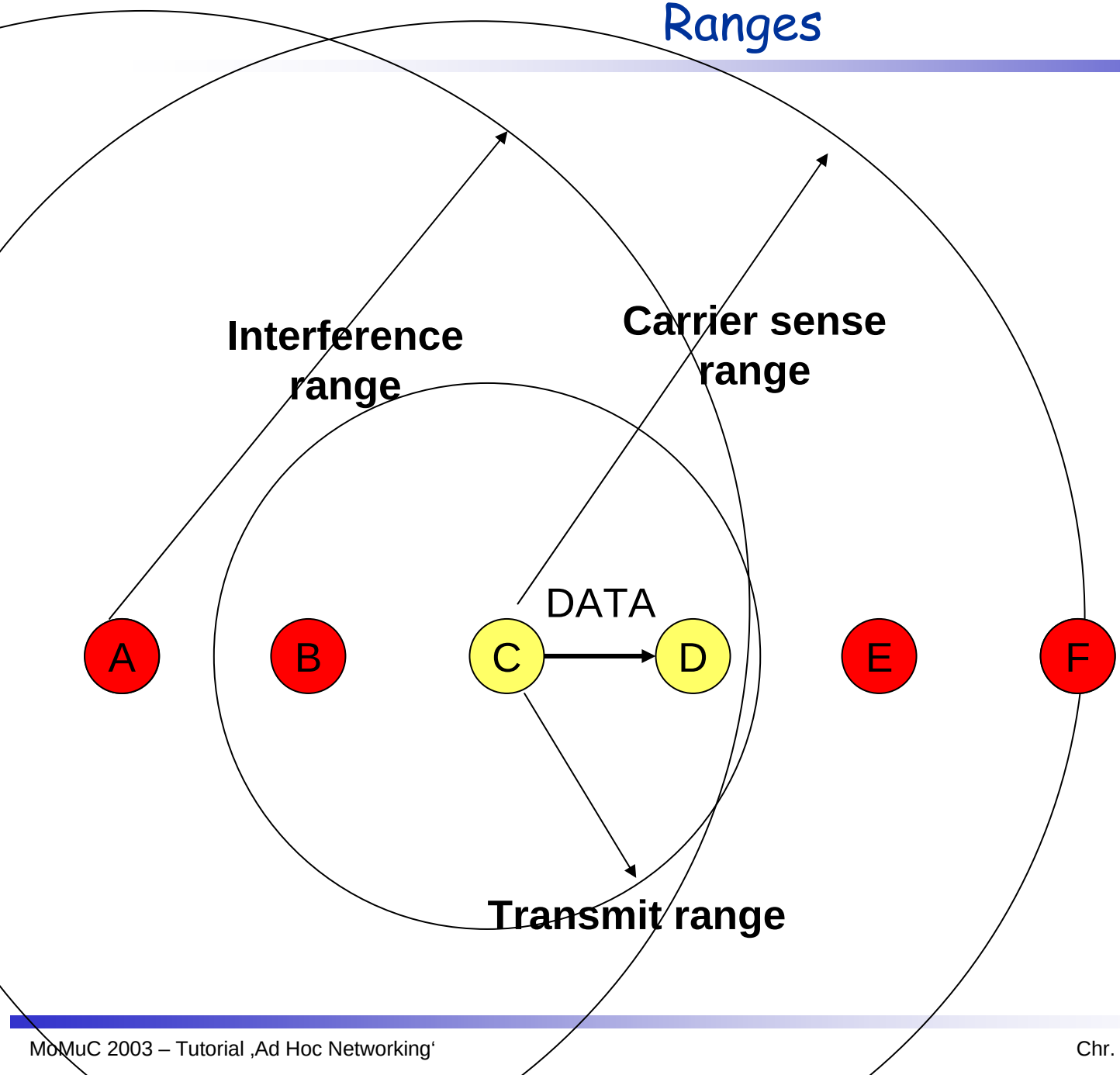
ARQ Example



ARQ for multi-hop Ad-Hoc Networks?

- Implicit assumption:
  - packet loss is caused by interference or collisions
  - retransmission seems to be appropriate
- What happens if packet loss occurs due to a node leaving the transmission range?
  - multiple retransmissions before the sender gives up
  - massive increase in network congestion
- Unlikely?
  - No – route discover strategies favor shortest (i.e., minimal hop) paths
- Note: broadcasts (used for route discovery) are not protected by ARQ

Ranges


Interference range
Carrier sense range
DATA
A
B
C
D
E
F
Transmit range

Problems with Ranges for multi-hop Ad-Hoc Networks

- Due to the large interference range:
  - dramatically reduced capacity
- Ranges depend on transmission rate
  - lower rate = less vulnerable to interference = higher range
- Broadcasts use a lower rate than unicast in IEEE 802.11 (to make the transmission more reliable)
- AODV and DSR use:
  - broadcast for route discovery:
  - unicast for data delivery
- Consequence:
  - routes (found via broadcast) may not be usable for data traffic
  - called Grey Zones [LNT02a]

Conclusion

- IEEE 802.11 is and will be used for multi-hop ad-hoc networks
  - inter-vehicle communication
  - as access network
- It is certainly not optimal – focus is on single hop networks
- Many pitfalls when „blindly“ using existing MAC mechanisms
- Need for an integrated routing/MAC approach
- Actually building a new MAC is hard and expensive
  - so far mostly paper and simulator work

References

- [CGL00a] A. Chandra, V. Gummalla, and J. Limb. Wireless medium access control protocols, IEEE Communication Surveys, Vol. 3, No. 2, 2000.
- [CYVR02a] R. Choudhury, X. Yang, N. Vaidya, and R. Ramanathan. Using directional antennas for medium access control in ad hoc networks, MobiCom'02, pp. 59-70, 2002.
- [IEEE97a] IEEE Computer Society. 802.11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, June 1997.
- [LNT02a] H. Lundgren, E. Nordström, and C. Tschudin. Coping with communication grey zones in IEEE 802.11b based ad hoc networks, Proceedings of WoWMoM, September 2002.
- [TK75a] F. Tobagi, and L. Kleinrock, Packet switching in radio channels: Part II – the hidden terminal problem in carrier sense multiple-access modes and the busy-tone solution, IEEE Transactions on Communications, Vol. 23, No. 12, pp. 1417-1433, 1975.
- [TMBR02] M. Takai, J. Martin, R. Bagrodia, and A. Ren. Directional virtual carrier sensing for directional antennas in mobiel ad hoc networks. MobiHoc'02, pp. 183 – 193, 2002.

Security in Mobile Ad Hoc Networks

Hannes Hartenstein, NEC Europe Network Labs

with big thanks to
Dirk Westhoff, NEC NL-E

Structure

- Introduction: Security needs and threats (general)
- Ad hoc specific security challenges
- Routing exploits
- Examples of secure routing protocols
- Trust, key management
- Fairness & Cooperation
- Intrusion detection + example (SRP)
- Conclusions

Introduction (coarse-grained, general)

"Security"

Security

Features/needs:

- subject/object authenticity
- data integrity
- confidentiality
- non-repudiation, accountability

Privacy/anonymity

Features/needs:

- confidentiality, sort of ...
- no unauthorized dissemination of personal data
- location, address, service privacy

Dependability

Features/needs:

- availability
- ...

'Network security' seen as customer-provider relationship:

- End user perspective: wants secure end-to-end communication
- Operator perspective: has to provide secure network organization as basis for offering a 'secure communication service'.

Attack types & Building blocks of countermeasures

- Passive attacks
  - get ‘content’
  - profiling

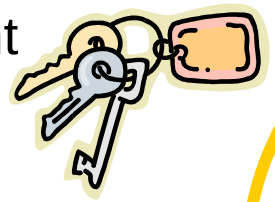
- Active attacks
  - fabricating or ‘stealing’ of packets
  - modification of packets
  - DoS attacks

- Counter measures can be based on
  - cryptography
  - monitoring

Differences in securing 'classical' and ad hoc networks

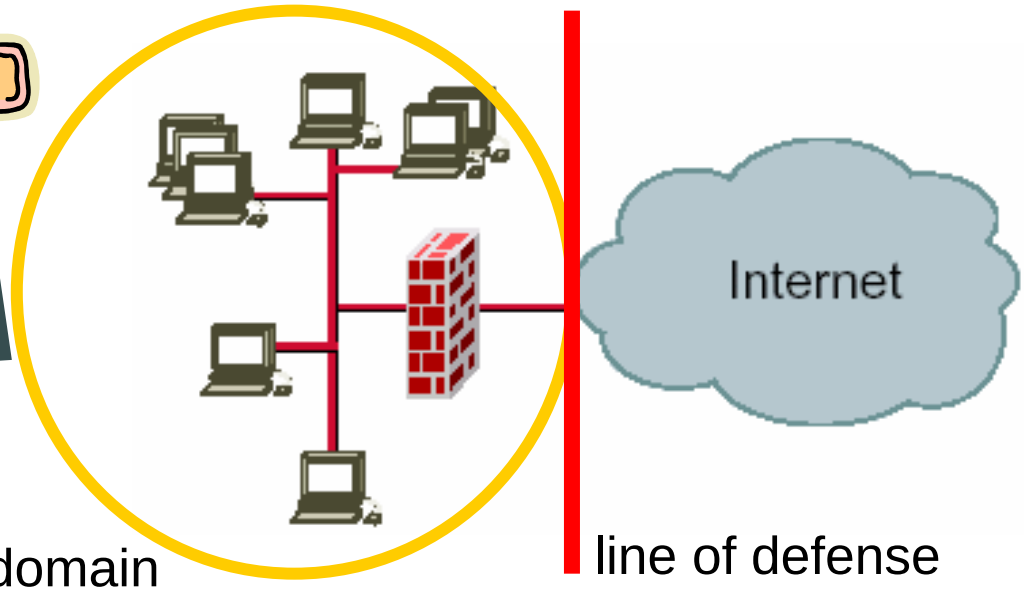
key management

infrastructure



intrusion

detection



single administrative domain

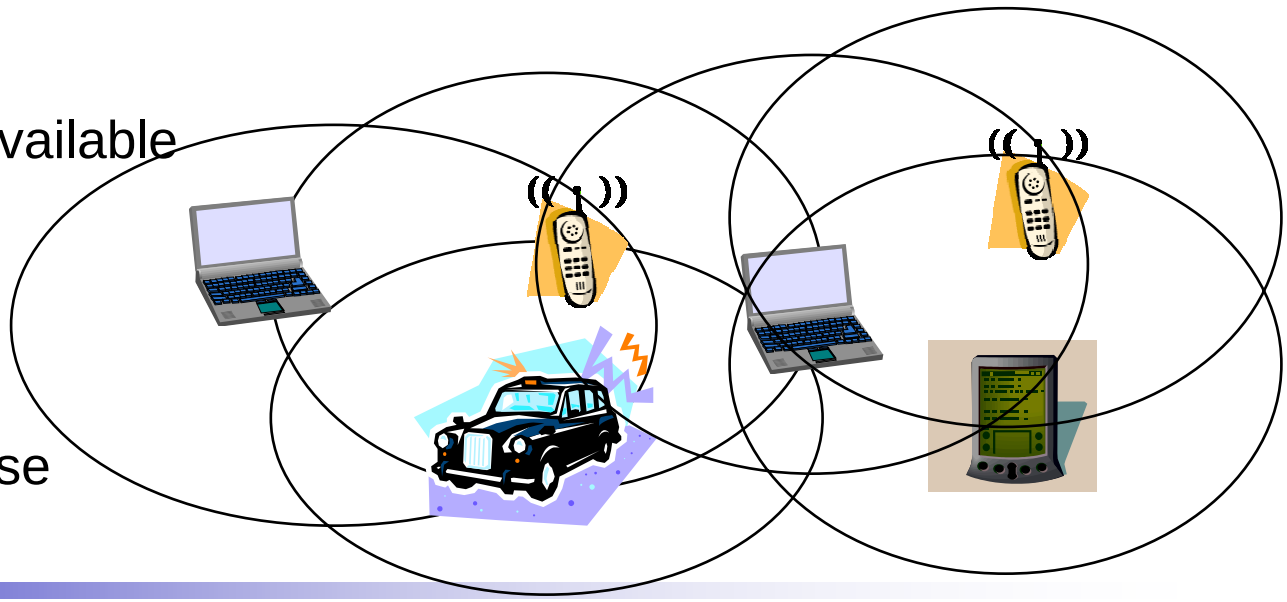
line of defense

PKI: (transiently) unavailable

only local monitoring

multiple domains

no clear line of defense



What are 'ad hoc specific' attack types?

Equipment Battery	No obvious 'line of defence'; side channel attacks 'Sleep deprivation torture' [Stajano2002]
Radio	Jamming
DLC	Attacks on MAC, MAC address
Routing	No infrastructure support; no clear line of defense
Cooperation	Based on principle of mutual assistance. Simple 'attack': drop packet.
Transport	Congestion control
Application	Attacks on key distribution and trust management; attacks on 'content' when content is used for forwarding decisions, data aggregation

Fairness and reliability

Routing exploits I: modification

- Modify header fields of packets in transit.

- A routing protocol enables nodes to learn the network's global topology through local information of other nodes.
- When the information gained is incorrect, wrong decisions or actions are taken, thus, proper functioning of routing is damaged.

Examples:

- AODV: modify SN or HopCount fields to irritate routing logic.
- DSR: modify source route for denial-of-service attack.
- Geographic routing: in location reply, modify current actual position.

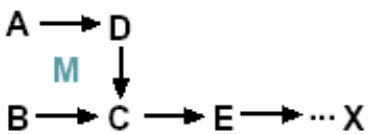
Routing exploits II: impersonation

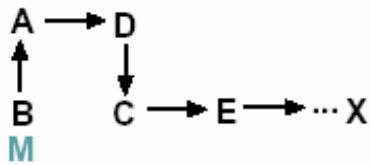
- “Spoofing”
- ... modification of address ...

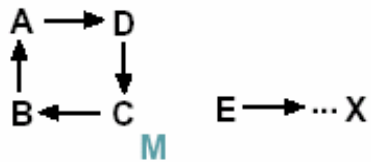
- Enables provision of misleading information on ‘impersonated’ node.

Examples:

- AODV/DSR: forming loops.







[Sanzgiri02]

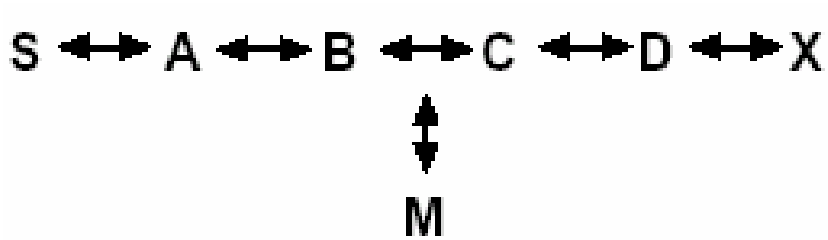
- Geographic routing: providing incorrect geographic position of a node.

Routing exploits III: fabrication

- ... of packets like route/location reply, error messages, beacon messages.
- Injects invalid information on which the protocol will react.

Examples:

- AODV/DSR: Fabricated route error messages as denial-of-service attack

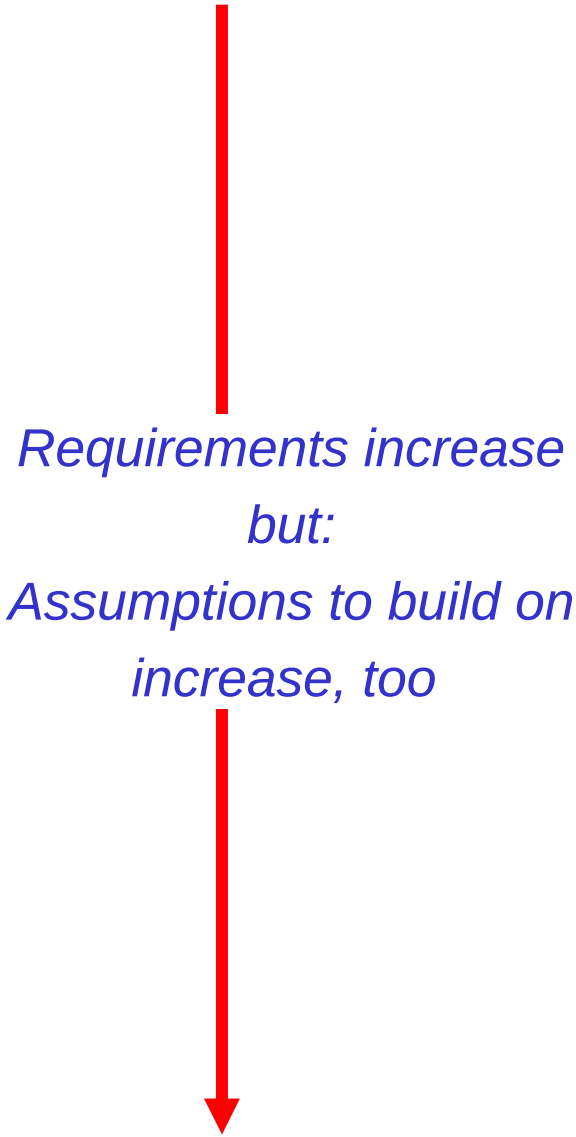


[Sanzgiri02]

- Geographic routing: Fabricated location replies or beacons.

Security goals w.r.t. ad hoc routing

- *Open* environment:
  - Route signaling cannot be spoofed
  - Fabricated routing messages cannot be injected into the network
  - Routing messages cannot be altered in transit, except according to the normal functionality of the routing protocol
  - Routing loops cannot be formed through malicious action
  - Routes cannot be redirected from the shortest path by malicious action
- *Managed open* environment
  - + Unauthorized nodes should be excluded from route computation and discovery.
- *Managed hostile* environment
  - + The network topology must not be exposed neither to adversaries nor to authorized nodes by the routing messages.



Example solution for secure routing 1: ARAN

Authenticated Routing for Ad hoc Networks (ARAN)

... securing AODV ...

Assumptions: *Managed Open Environment*

- Trusted certificate server T; its public key is known to all nodes.
- Each node has own certificate signed by T.

Procedure:

- ***Signed*** route discovery packet (RDP) propagates to sought destination.
- Destination sends back ***signed*** route reply (REP).
- At each hop:
  - validation of original signature
  - validation of last hop signature
  - when last hop is not source/destination: ***replace last hop signature by own signature***

ARAN: basic procedure

[RDP, IP(X), cert(A), N(A), t**] K(A-)**

Route Discovery Packet

Address of sought destination

A's certificate

Nonce

timestamp

everything signed with A's private key

Send out by source node A

[[RDP, IP(X), cert(A), N(A), t**] K(A-)] K(B-), cert(B)**

Send out by intermediate node B

[[RDP, IP(X), cert(A), N(A), t**] K(A-)] K(C-), cert(C)**

Send out by intermediate node C

ARAN: checklist

- Unauthorized participation: managed by trusted authority.
- Spoofed route signaling: everything is signed.
- Fabricated routing messages: Hm ... but at least ‘non-repudiation’ or ‘isolation’.
- Alteration of routing message: fields of RDP, REP packets remain unchanged.
- Replay attacks: nonce + timestamp.

- Certificates add significant overhead w.r.t. byte load
  - Example: X.509 certificate is usually several hundred bytes long with 700 bytes a typical value (ANSI DER).
  - ‘Compressed format’ with only mandatory fields is important.
- Route setup o.k., but then ...?

Example solution for secure routing 2: S-AODV

Secure AODV [Zapata2001]

- Similar to ARAN but
- Assumes all node know all certificates (so there is no need to include them in the S-AODV protocol)
- Allows route replies from intermediate nodes.
- Uses ‘Lamport hash chains’ [Lamport1981] to authenticate the hop count field:

F is a one-way hash function

x -> F(x) easy; F(x) -> x infeasible

Seed				*Top hash*
x	$F^2(x)$	$F^3(x)$	...	$F^n(x)$
Source	*Intermediate*	*Intermediate*	...	

Key & trust management

- Symmetric vs asymmetric keys
  - Symmetric keys: key distribution problem
  - Asymmetric keys (public-private key pairs): certificate overhead

- Challenge in ad hoc networks: no support of infrastructure w.r.t. trust assumptions and contexts
  - transiently disconnected operation
  - pure ad hoc network-based operation

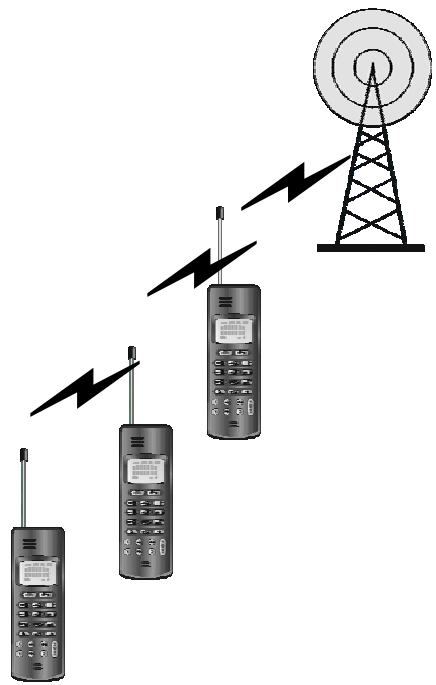
Examples Scenarios/Solutions:

- Key agreement in a local group (Asokan, Ginzboorg 2000)
  - based on ‘encrypted key exchange’; transforms weak secret into strong one.
- Distributed CA (Zhou, Haas 1999)
  - based on threshold cryptography; only a min of *t* server can sign a certificate
- Self-organized public key management (Capkun, Buttyan, Hubaux 2003)
  - inspired by PGP and its web of trust.

Fairness & cooperation

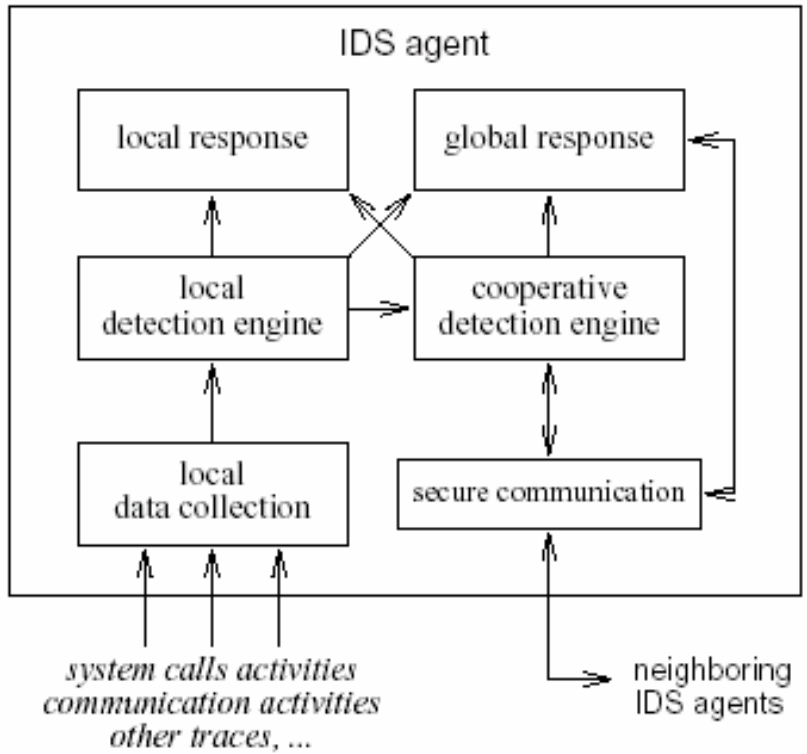
- Detection-based methods
  - Idea: observe a neighboring node's behavior. If it does not behave 'correctly' or fair, put it on the black list and tell the others.
  - Meta-problem: defamation.
  - See, e.g., work by S. Buchegger / J.-Y. LeBoudec and by K. Paul / D. Westhoff.

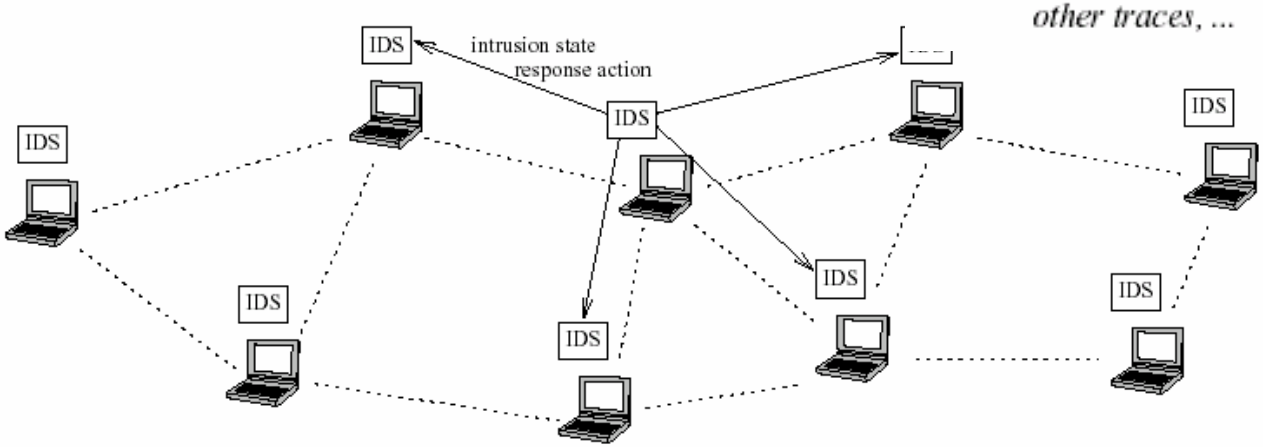
- Motivation-based methods
  - Idea: introduce 'virtual' money and/or accounting scheme.
  - Works for multi-hop access with AAA infrastructure of an network operator
  - See, e.g., work by N. Ben Salem / J.-P. Hubaux, B. Lamparter / D. Westhoff (SCP), . Zhong, Y. R. Yang, J. Chen (SPRITE)



Intrusion detection

- ... preventive methods do not solve all the problems; detective methods needed as well.
- Zhang/Lee 2000:
  - No ‘concentration points’, thus, needs to be fully distributed and cooperative.
  - Algorithms must be made to work on partial/localized information.
  - Multi-layer integrated intrusion detection required.





Source:
Zhang, Lee

SRP & NLP

- *Secure Routing Protocol:* a protocol for ‘secure’ route discovery, i.e., to learn correct connectivity information [Papadimitratos, Haas, Samar; work-in progress, 2002]

- Neighbor Lookup Protocol: Part of *Secure Routing Protocol* Shows some elements of intrusion detection, e.g., to detect spoofing:
  - Checks MAC address – IP address binding of `overheard’ nodes. A node is not allowed to use several IP addresses. Assumption is: MAC addresses are hardwired ... (!?)
  - Detects whether two neighbor use same IP address.
  - Detects whether a neighbor uses same MAC address.

  - NLP also measures the rates at which control packets are received (per MAC address).

Conclusions

- Ad hoc security mechanisms have to built on cryptography and local monitoring as ‘security primitives’.
- Multiple domains, no clear line of defense, stand-alone operation, no global view make ad hoc security a serious challenge.
- Simple attack: do not participate ...
- Routing and cooperation: many ‘partial’ solutions exist

  ... but there is no ‘partial security’ ...
- There might be fundamental limits on what degree of ‘security’ is achievable ...

References I

- See bibliography by Feng Zhu: http://www.ccs.neu.edu/home/zhufeng/security_manet.html
- Stajano, F., *Security for Ubiquitous Computing*, Wiley, 2002.
- Sanzgiri, K., Dahill, B., Levine, B. N., Shields, C., Belding-Royer, E. M., *A secure routing protocol for ad hoc networks*, Proc. Int'l Conf. Network Protocols (ICNP), Nov. 2002.
- Guerrero Zapata, M., *Secure ad hoc on-demand distance vector (SAODV) routing,* draft-guerrero-manet-saodv-00.txt, work-in-progress, October 2001
- Lamport, L., *Password authentication with insecure communication*, Communications of the ACM, Nov. 1981.
- Papadimitratos, P., Haas, Z. J., Samar, P., *The secure routing protocol for ad hoc networks,* draft-papadimitratos-secure-routing-protocol-00.txt, work-in-progress, December 2002
- Papadimitratos, P., Haas, Z. J., *Secure Routing for Mobile Ad Hoc Networks*, Proc. SCS CNDS 2002, January 2002.
- Zhang, Y., Lee, W., *Intrusion detection in wireless ad-hoc networks, Proc. ACM Mobicom 2000.*
- Asokan, N., Ginzboorg, P., *Key agreement in ad-hoc networks*, Computer Communications, 23, 1627-1637, 2000.

References II

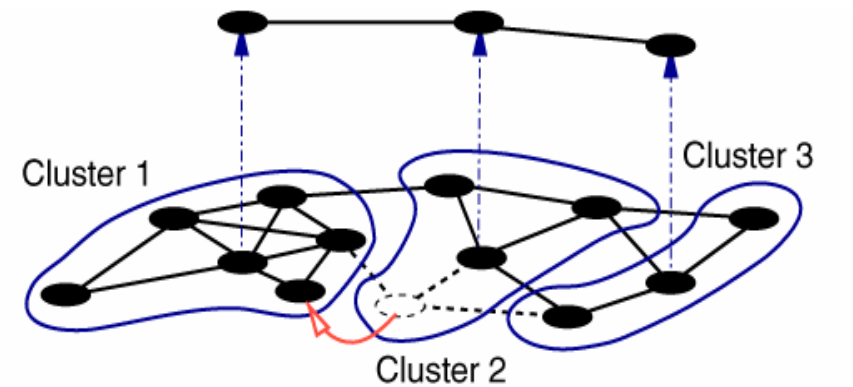
- Zhou, L., Haas, Z., *Securing ad hoc networks*, IEEE Network Magazine, Nov/Dec 1999.
- Capkun, S., Buttyan, L., Hubaux, J.-P., *Self-organizing public-key management for mobile ad hoc networks*, IEEE Trans. on Mobile Computing, vol. 2, no. 1. , January-March 2003.
- S. Buchegger, J. Y. Le Boudec, *Performance Analysis of the CONFIDANT Protocol (Cooperation Of Nodes - Fairness In Dynamic Ad-hoc NeTworks),* Proceedings of MobiHoc 2002, Lausanne, June 2002
- K. Paul, D. Westhoff, "Context Aware Detection of Selfish Nodes in DSR based Ad-hoc Networks", Proceedings of IEEE GLOBECOM `02, Taipei, Taiwan, November 2002.
- N. Ben Salem, L. Buttyán, J. P. Hubaux, and M. Jakobsson, *A Charging and Rewarding Scheme for Packet Forwarding in Multi-hop Cellular Networks*, *Fourth ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc),* Annapolis, Maryland, USA. June 1-3, 2003
- S. Zhong, Y. R. Yang, J. Chen, "Sprite: A Simple, Cheat-Proof, Credit-Based System for Mobile Ad-hoc Networks", Proceedings of IEEE INFOCOM `03, San Francisco, USA, March 2003.
- B. Lamparter, K. Paul, D. Westhoff, "Charging Support for Ad Hoc Stub Networks", Elsevier Journal of Computer Communication, Vol. 26, Issue 13, August 2003, pp. 1504-1514.

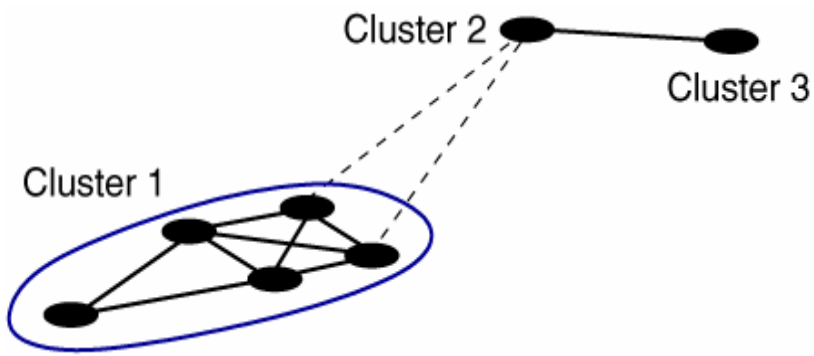
Distributed Clustering

Christian Bettstetter, TU München

Clustering

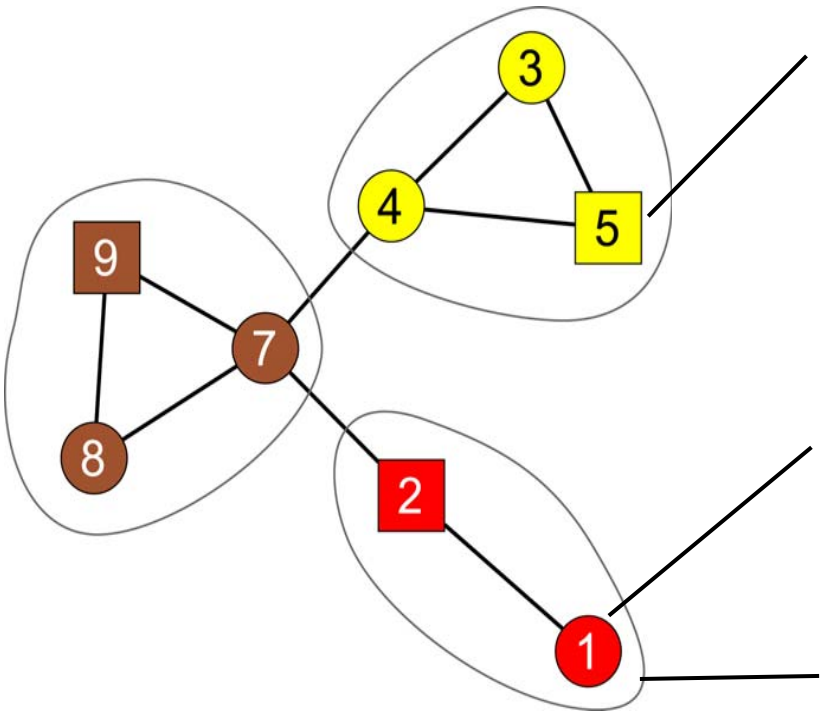
- Creates hierarchy
- Useful for:
  - Hierarchical routing
  - Address assignment
  - Radio resource allocation
- In ad hoc networks:
  - Distributed algorithm
  - Online algorithms
  - Adaptive to mobility





Makes dynamic networks look less dynamic.

DMAC algorithm (Basagni)



Clusterhead <weight>

- Has largest weight in its neighborhood
- Two clusterheads can not be neighbors

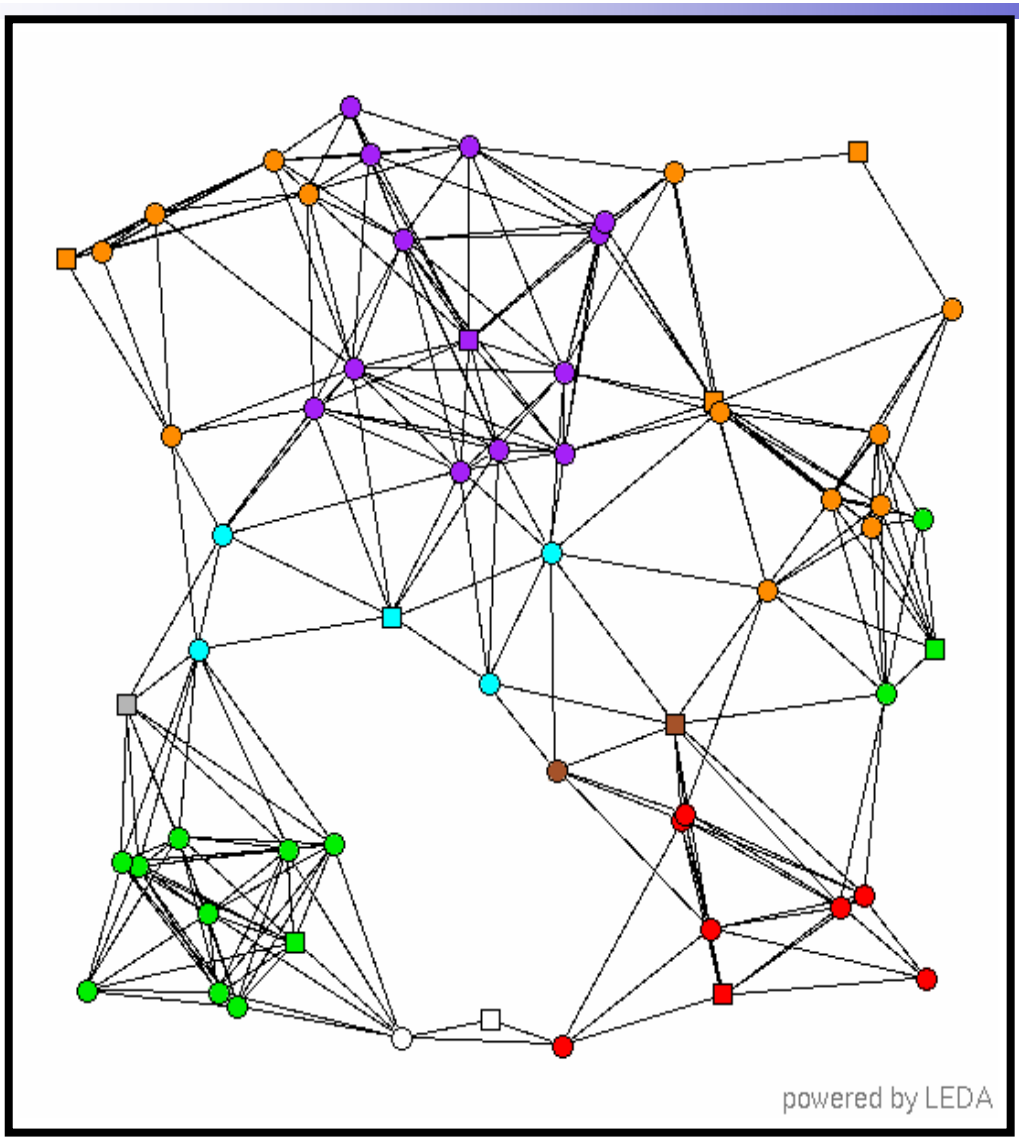
Ordinary node <weight>

- Joins the neighboring clusterhead with the largest weight.

Cluster

- two hop size

Example of Visualization

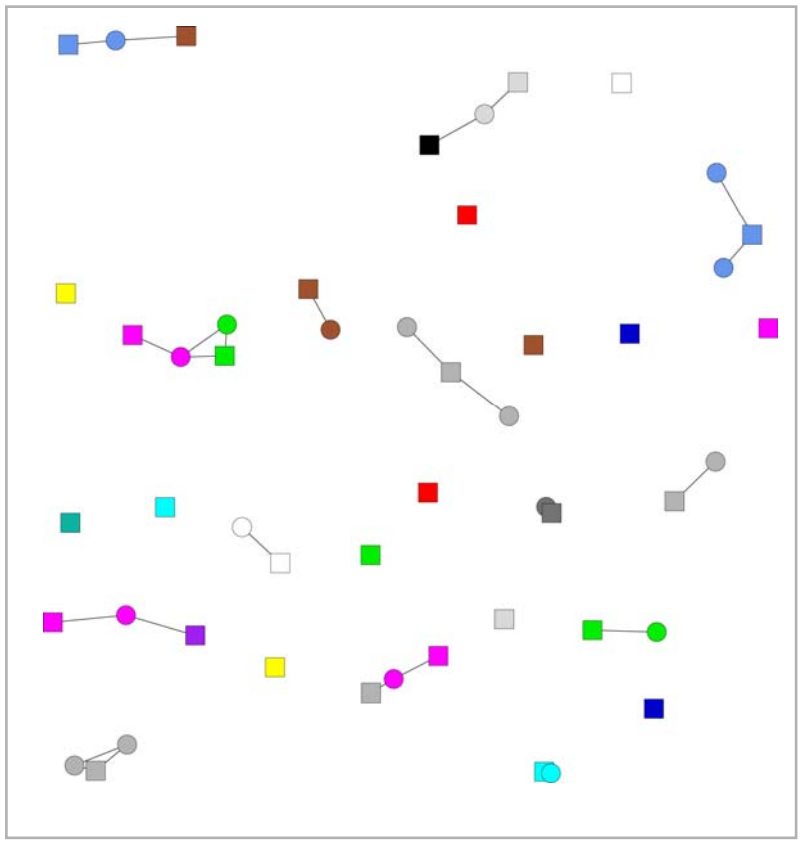


What is a „good" clustering algorithm?

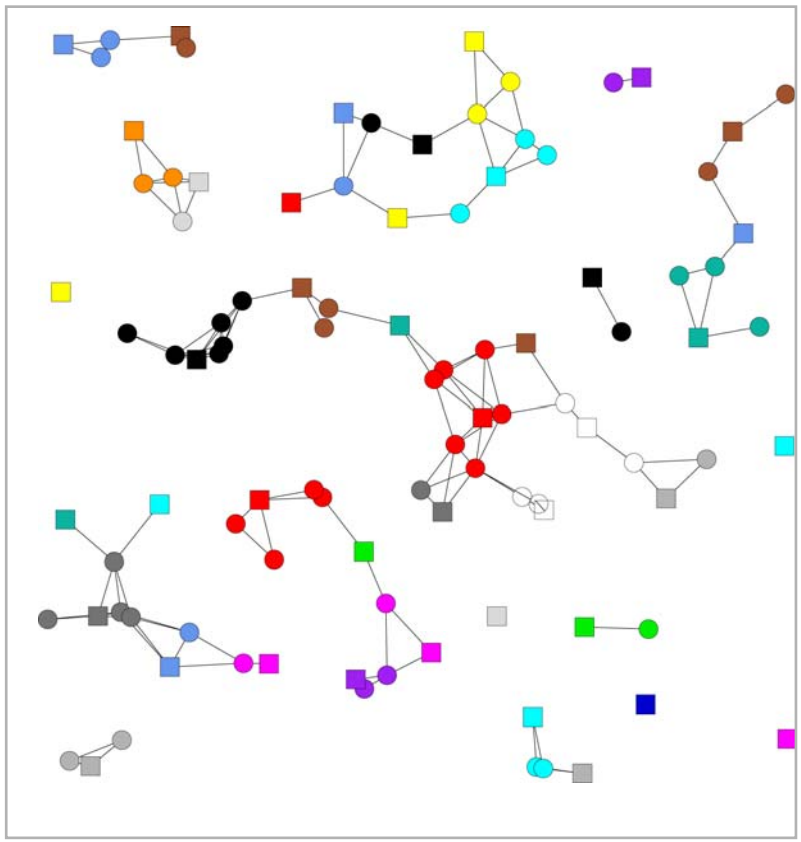
- Load on clusterheads (traffic and processing): bottlenecks?
- Message complexity: Number of messages after a change in the topology until a valid cluster structure is re-achieved.
- Convergence time complexity: Number of time steps after a change in the topology until a valid cluster structure is re-achieved.

- Routing table size and routing optimality (hierarchy)
- Decision speed (required neighbor knowledge)
- Level of adaptability (which parameters are adaptive?)
- Asynchronous operation
- Cluster stability

DMAC Cluster Density



(a) *n=50* nodes, range r_0=*0.1a*
gives here 32 clusters

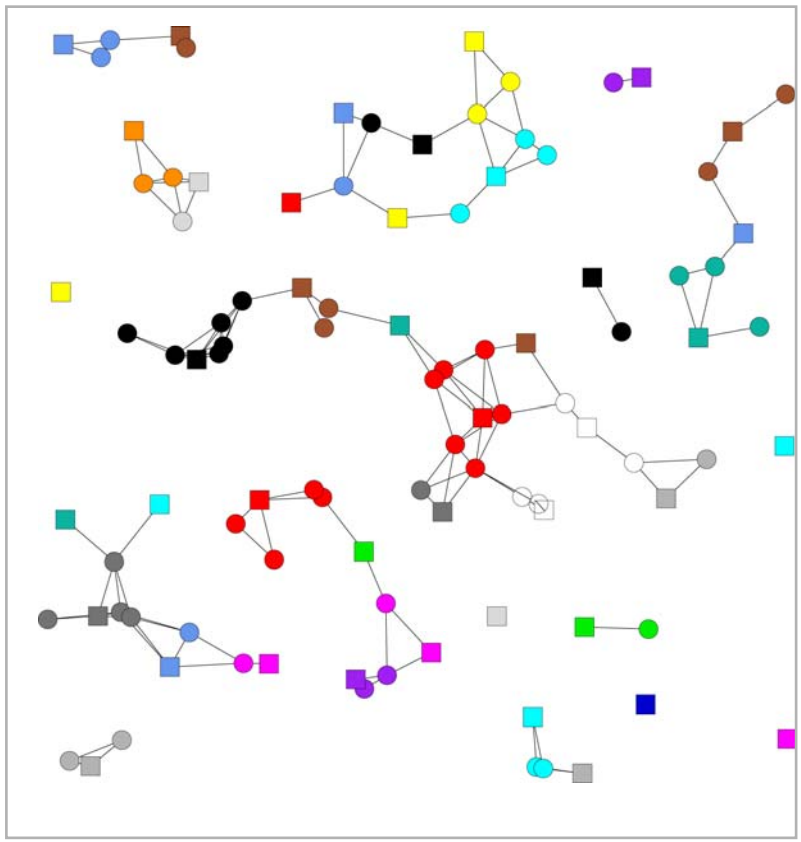


(b) *n=100* nodes, range r_0=*0.1a*
gives here 42 clusters

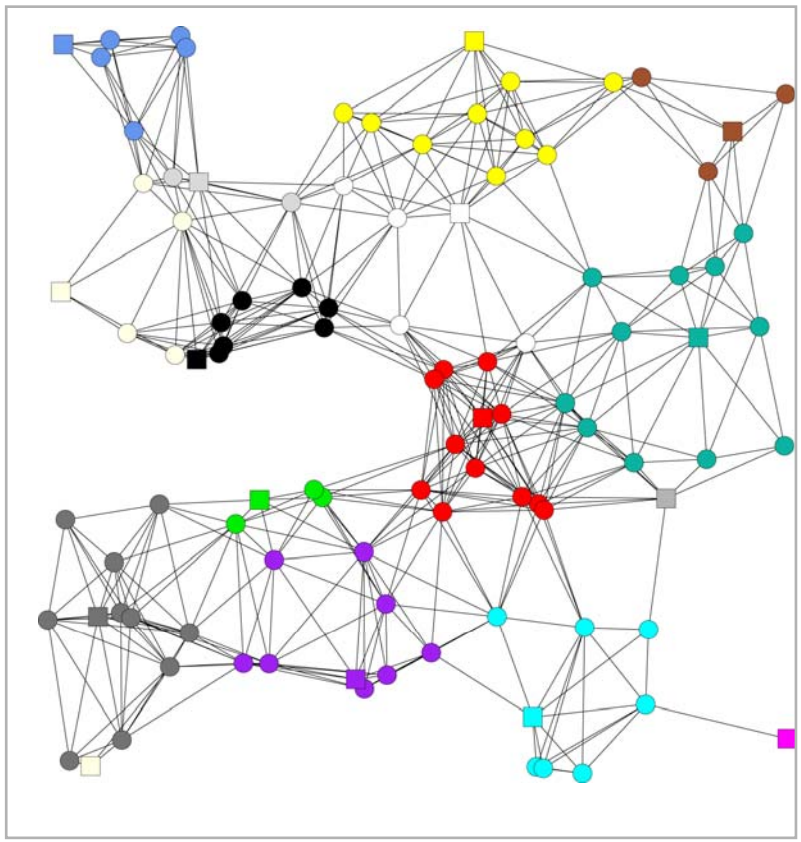
Uniformly distributed nodes on *a* x *a* square

from C. Bettstetter PhD thesis

DMAC Cluster Density



(b) *n=100* nodes, range r_0=*0.1a*
gives here 42 clusters

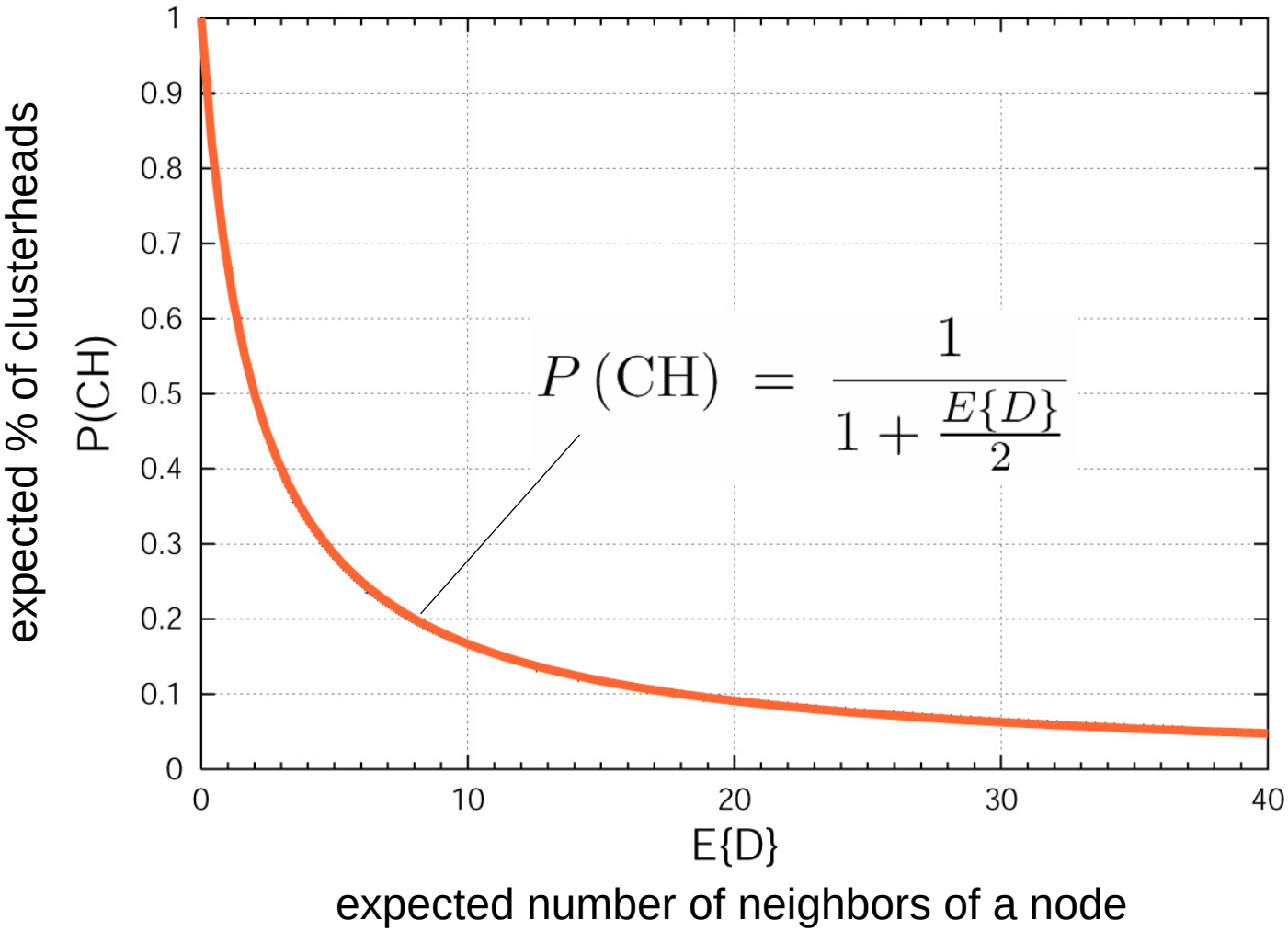


(c) *n=100* nodes, range r_0=*0.2a*
gives here 16 clusters

Uniformly distributed nodes on *a* x *a* square

from C. Bettstetter PhD thesis

DMAC Cluster Density



(uniformly distributed nodes)

from C. Bettstetter PhD thesis

Dynamic behavior of clustering

- **Design Goal 1: Minimize message and time complexity!**
- **Design Goal 2: Clusterheads should be especially stable!**

  Role change may trigger many other events with high complexity. Role change may even cause re-clustering chain reaction
- **Design Goal 3: Keep changes local!**

  Reactions to changes based only on local knowledge. Changes should only affect the neighborhood of the node

Clustering Algorithms

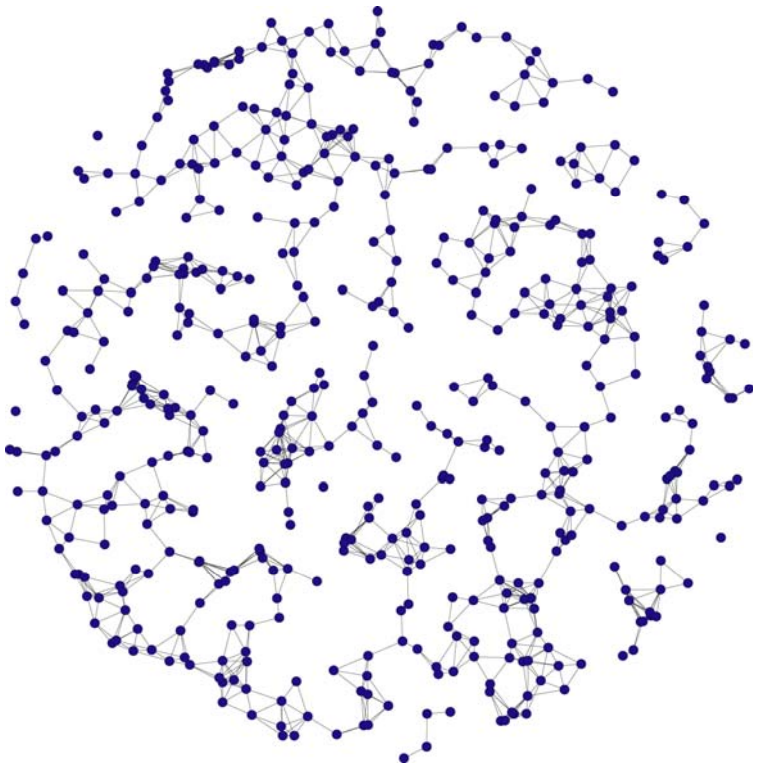
- **Ramanathan, Streenstrup:** Allow to control cluster size
- **Das, Bharghavan**: Minimum dominating set
- **Alzoubi, Wan, Frieder**: Minimum dominating set
- **McDonald, Znati**: Framework for adaptability to mobility
- and many others....

Connectivity in Ad Hoc Networks

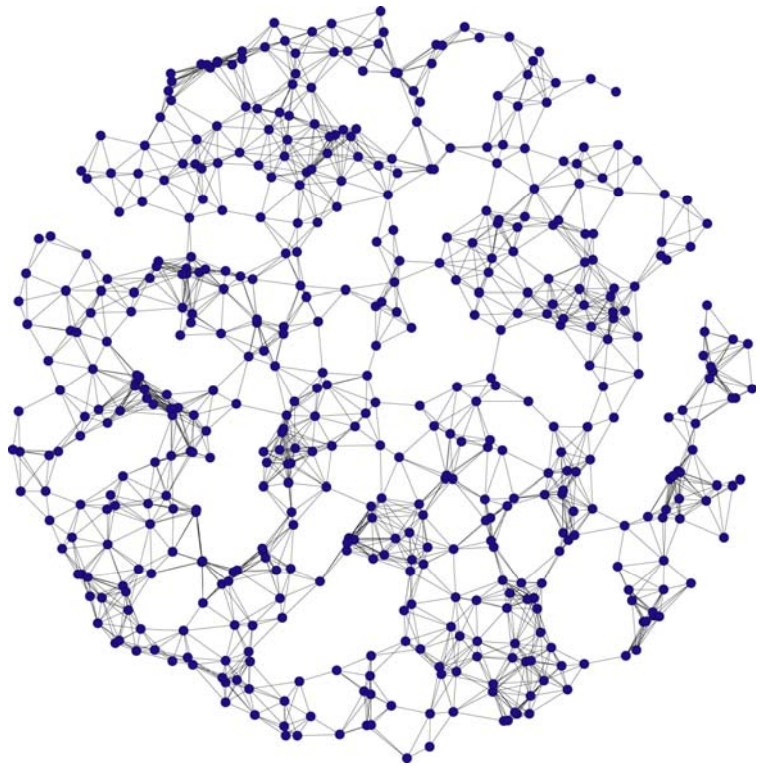
Christian Bettstetter, TU München

Motivation and Definition

The ad hoc network should be **connected**.



(a) disconnected network



(b) connected network

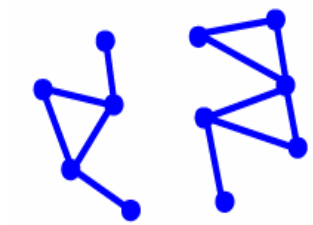
Problem Statement

- *n* randomly uniformly distributed nodes on area of size *A*
- Each node has a radio transmission range r_0

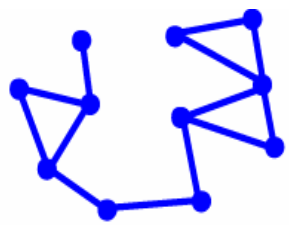
Which (r_0 , *n*) pairs achieve an almost surely connected network on given area *A*?

Practical application of results

- System design of sensor networks: How many sensors of given type (capable of transmitting r_0) are needed in given environment?
- Simulation of mobile ad hoc networks

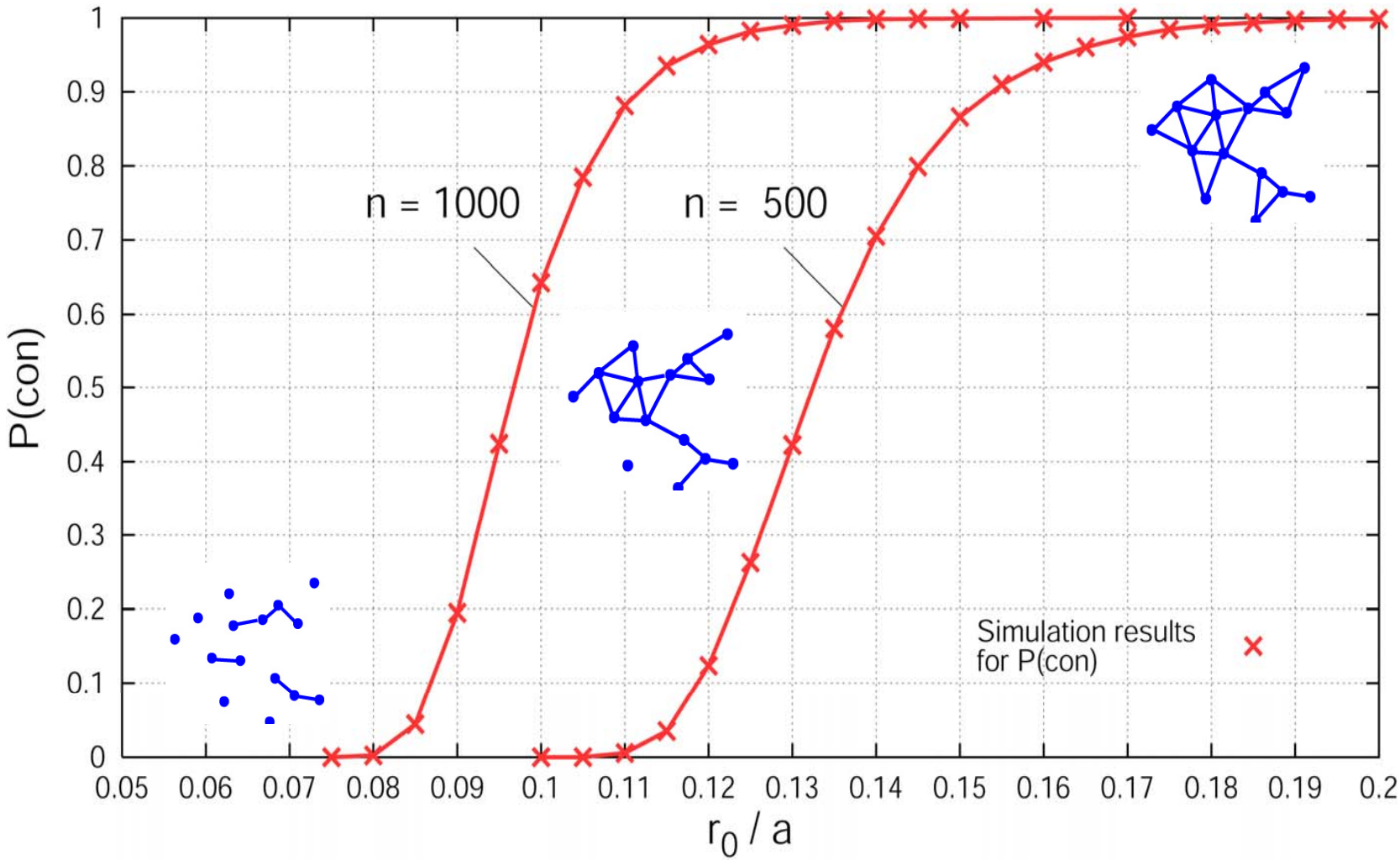


a) Unconnected graph



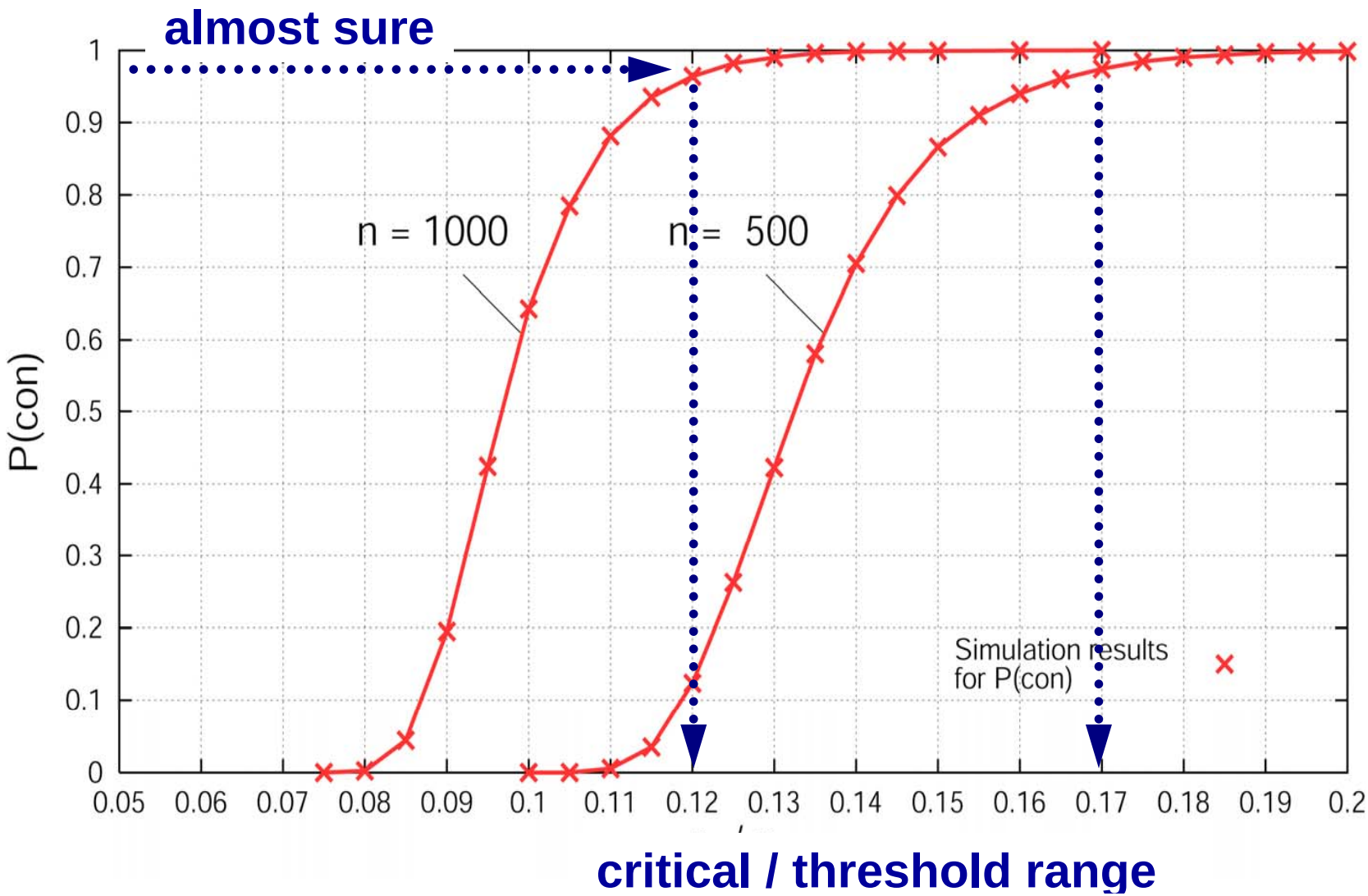
b) Connected graph

Connectivity



Disk of radius *a*

Connectivity

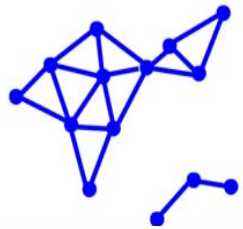


Question: Can we calculate these values ?

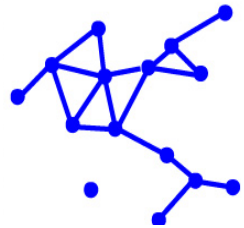
Relation between isolated nodes and connectivity

- Having **no isolated node** is a necessary but not sufficient condition for **connectivity**.

It follows: $P(\text{con}) \leq P(\text{no iso node})$



Two partitions



Isolated node

- In other words, for given number of nodes *n* and desired *p*:

$$\underbrace{r_0\big(P(\text{con}) = p, n\big)}_{\text{critical range for connectivity}} \geq \underbrace{r_0\big(P(\text{no iso node}) = p, n\big)}_{\text{critical range for no isolated node}} .$$

Calculation of P(no iso node) on bounded system area

- Expected number of neighbors of a node at given location

$$\mu_0(\mathbf{x})$$

- Probability that this node is isolated:

$$P(\text{node iso} \mid \mathbf{x}) = e^{-\mu_0(\mathbf{x})}$$

- Probability that a randomly chosen node is isolated:

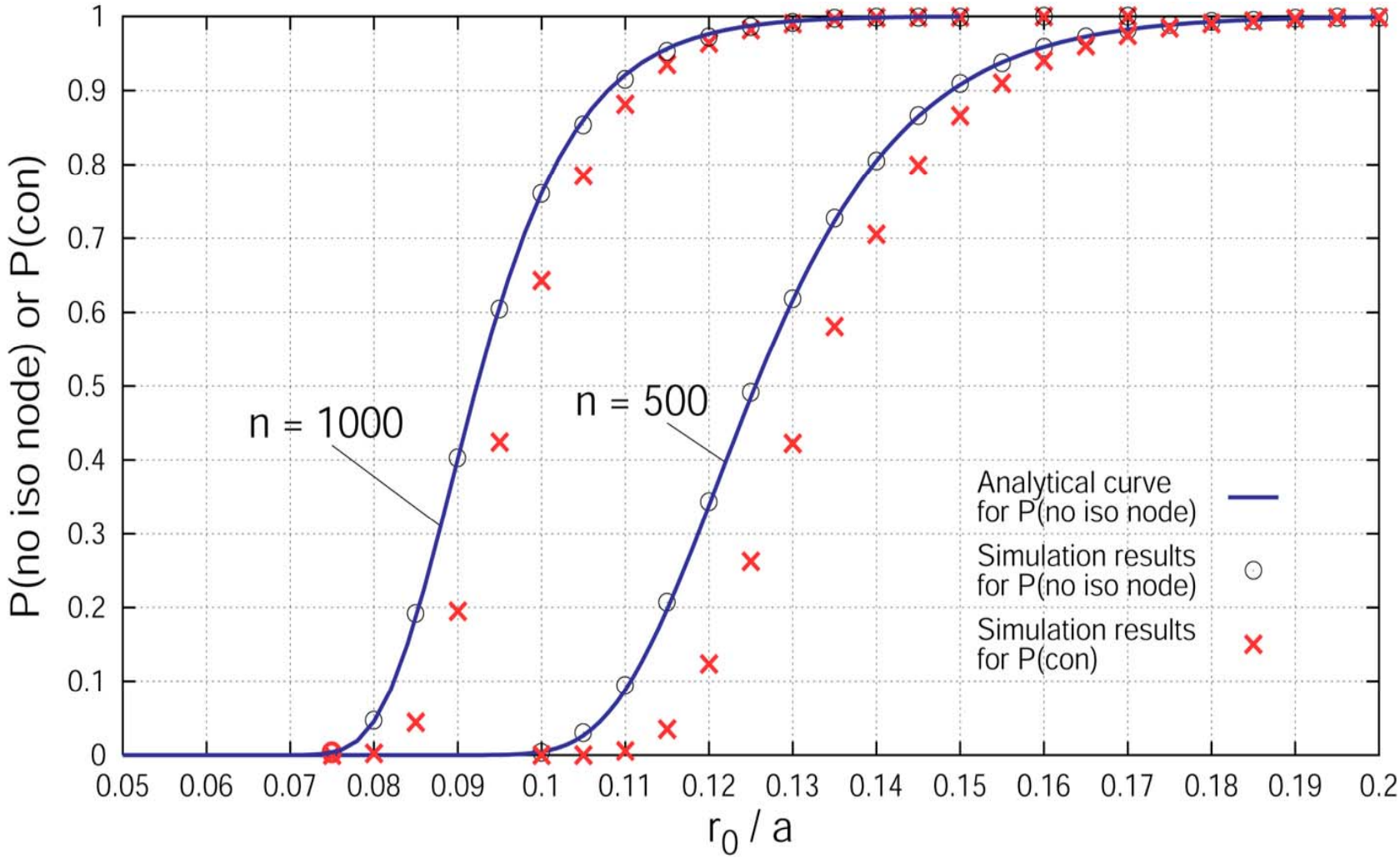
$$P(\text{node iso}) = \iint P(\text{node iso} \mid \mathbf{x}) \underbrace{f_{\mathbf{X}}}_{\text{Pdf of spatial node distribution}} dA$$

- Probability that none of *n* nodes is isolated:

$$P(\text{no iso node}) = \exp\left(-n\, P(\text{node iso})\right)$$

Question: How tight is this bound ?

Relation between isolated nodes and connectivity



How tight is the bound ?

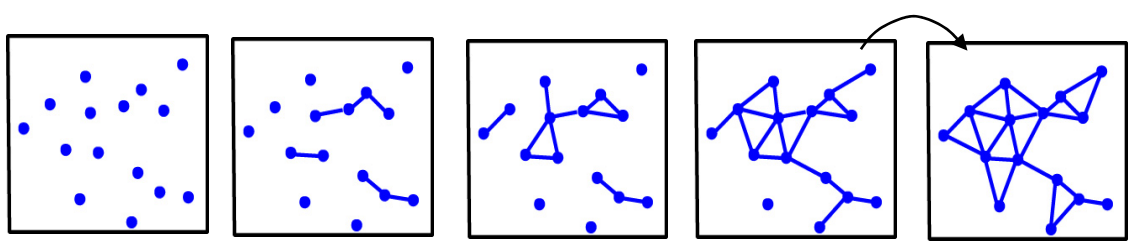
In own words:

$$\underbrace{r_0\big(P(\text{con}) = p, n\big)}_{\text{critical range for connectivity}} = \underbrace{r_0\big(P(\text{no iso node}) = p, n\big)}_{\text{critical range for no isolated node}} + \epsilon\,, \quad \epsilon \geq 0$$

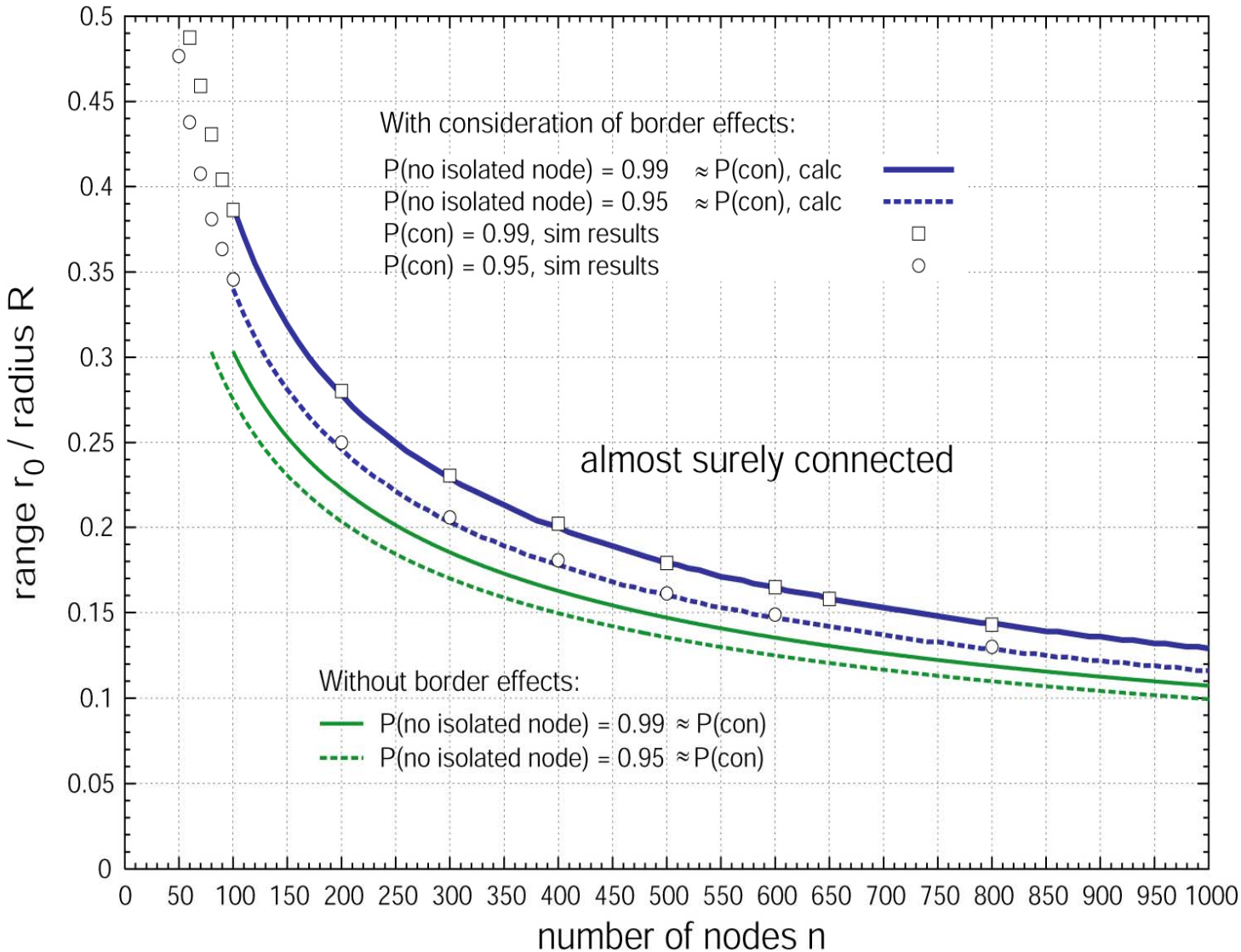
$$\epsilon \to 0 \text{ as } p \to 1$$

In practice: Critical (r_0, n)-pairs for P(no iso node) = 99% are very tight bounds for P(con) = 99%. (see *Bettstetter Mobihoc02*)

Mathematical background: Penrose's theorem on the connectivity of geometric random graphs (1997, 1999)



Critical (r_0, n) pairs for almost sure connectivity



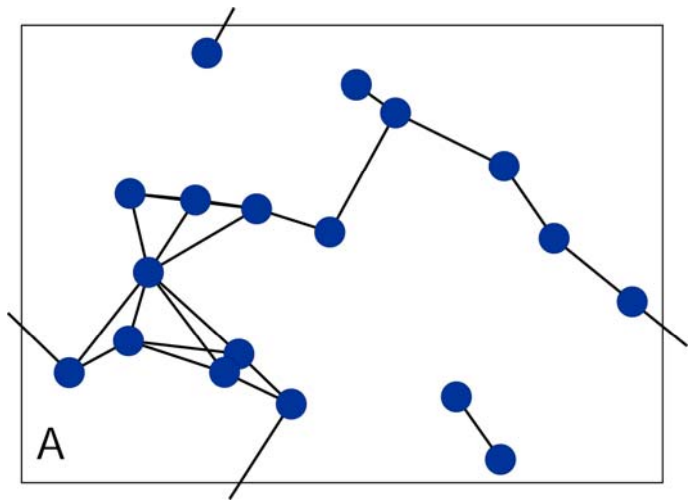
(*Bettstetter MWCN 2002*)

Disk of radius *R*

Connectivity without border effects

- Critical range to achieve network with no isolated node:

$$r_0^{ni}(p,n) = \sqrt{\frac{A}{n\pi}\left(\ln n - \ln\ln\frac{1}{p}\right)}$$

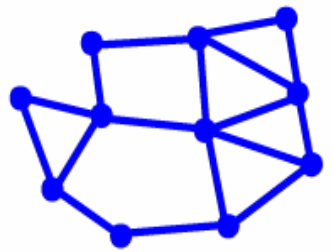


- $p = 1 \Rightarrow -\ln\ln\frac{1}{p} = +\infty$
- $n \to \infty \Rightarrow \frac{\ln n}{n} \longrightarrow 0$
- Serves as a lower bound for critical range for connectivity on bounded area

- Results by Gupta and Kumar (1998)

Further Issues

- *k*-connectivity to improve network resilience
- More realistic channel model
- Path probability between two nodes
- ...



2-connected graph

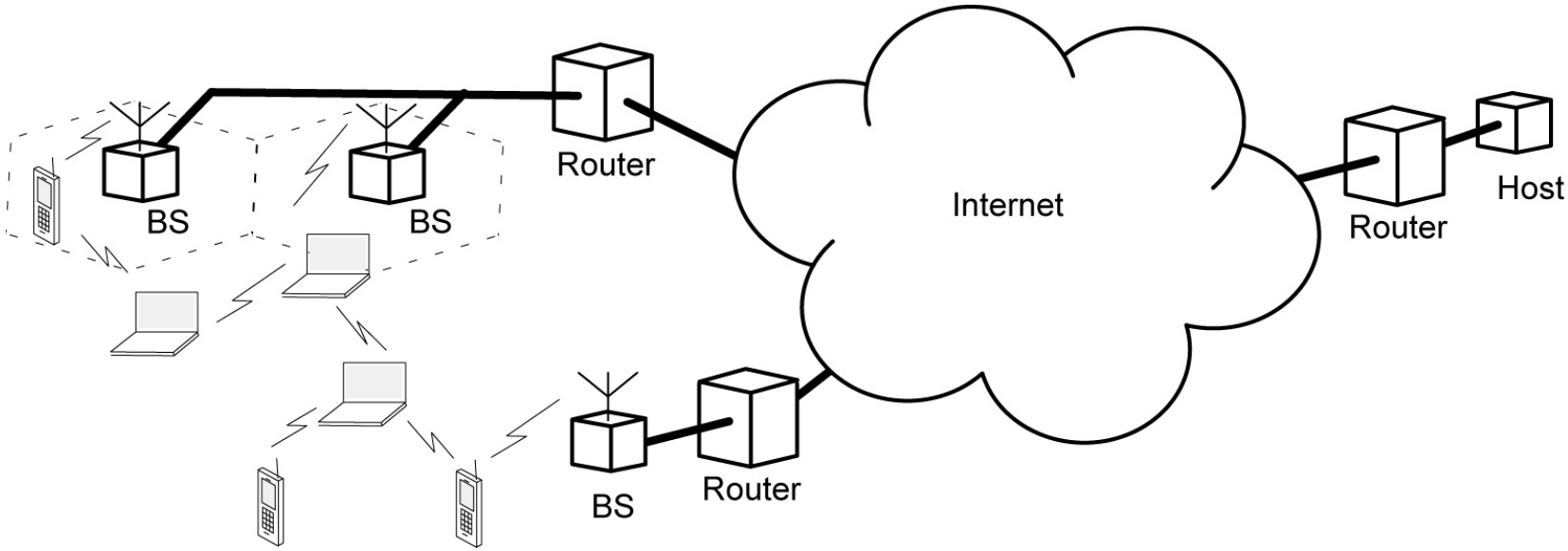
Some Literature

- **Cheng and Robertazzi**, “Critical connectivity phenomena in multihop radio networks,” *IEEE Trans. Com.,* July 1989
- **Piret**, “Cn the connectivity of radio networks,“ *IEEE Trans. Inf. Theory*, Sept 1991.
- **Gupta and Kumar**, “Critical power for asymptotic connectivity in wireless networks,“ in *Stoch. Analysis, Control, Optimization, and Appl*, Birkhäuser, 1998.
- **Santi, Blough, and Vainstein**, “A probabilistic analysis for the radio range assignment problem in ad hoc networks,“ in *Proc. ACM MobiHoc*, Long Beach, Oct. 2001.
- **Bettstetter**, “On the minimum node degree and connectivity of a wireless multihop network,” In *Proc. ACM MobiHoc*, Lausanne, Switzerland, June 2002
- **Dousse, Thiran, and Hasler**, “Connectivity in adhoc and hybrid networks,“ in *Proc. IEEE Infocom*, New York, June 2002.
- **Santi, Blough,** “The critical transmitting range for connectivity in sparse wireless ad hoc networks”, *IEEE Trans. Mobile Comp.,* March 2003
- **Bettstetter and Hartmann**, “Connectivity of wireless multihop networks in a shadow fading environment,” in *Proc. ACM MSWiM,* San Diego, Sept 2003.

Interconnection of Ad Hoc Networks to the Internet

Christian Bettstetter, TU München

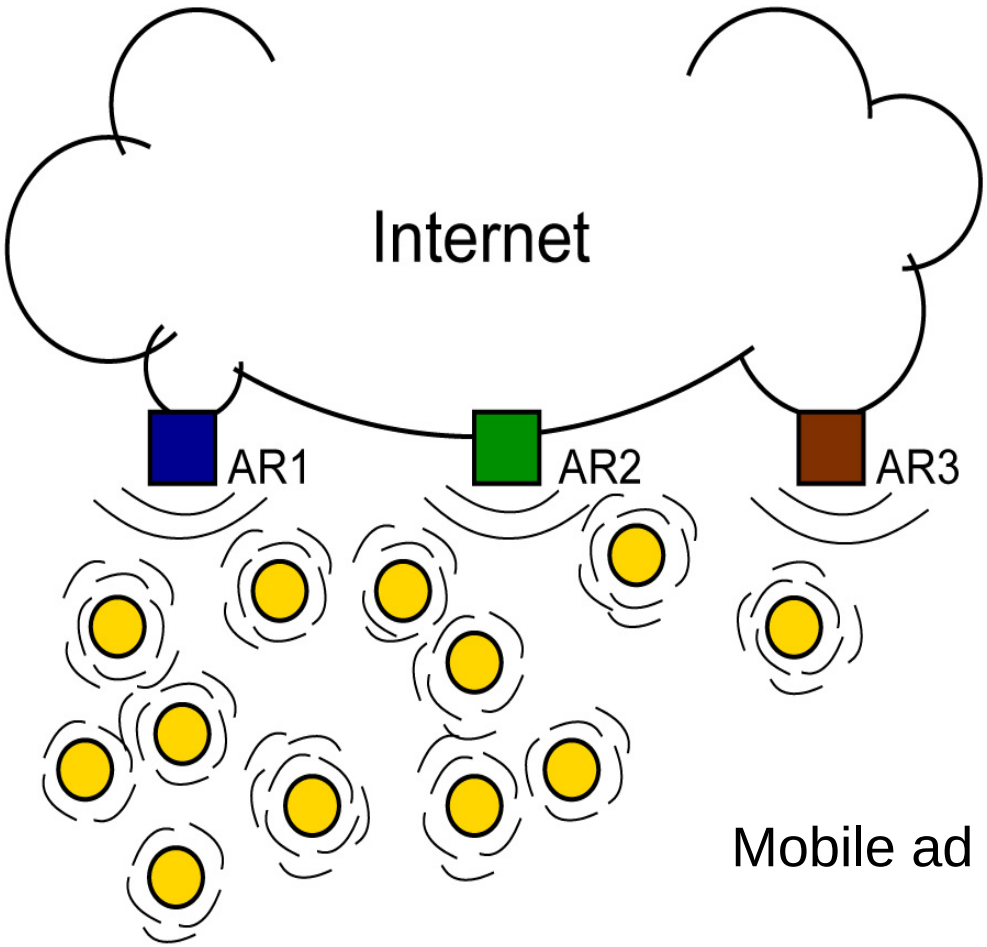
Interconnection of Ad Hoc Networks to the Internet



- **Gateway discovery and selection**: How does a node in the ad hoc network detect the existence of nearby base stations and access routers? Which base stations will a node choose?
- **Address autoconfiguration**: How does a node configure a globally valid IP address?
- **Heterogeneous routing**: How does a node send/receive packets to/from the Internet?

from C. Bettstetter PhD thesis

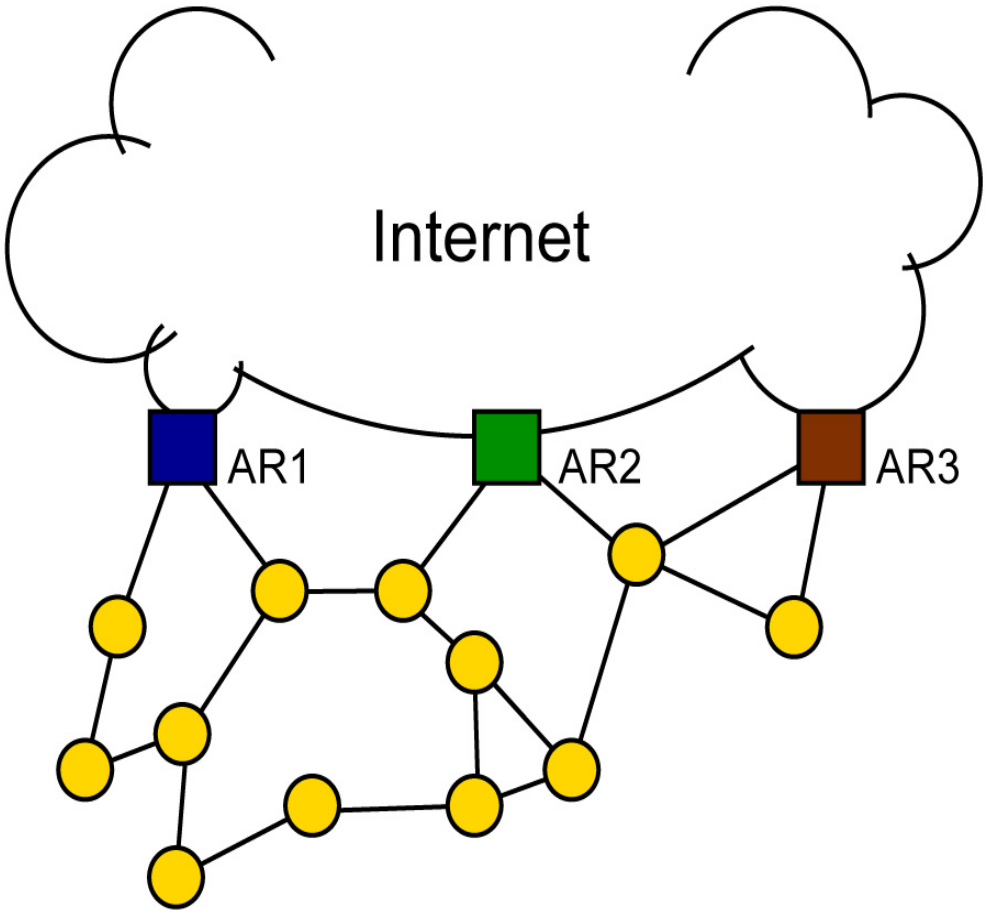
Interconnection of Ad Hoc Networks to the Internet



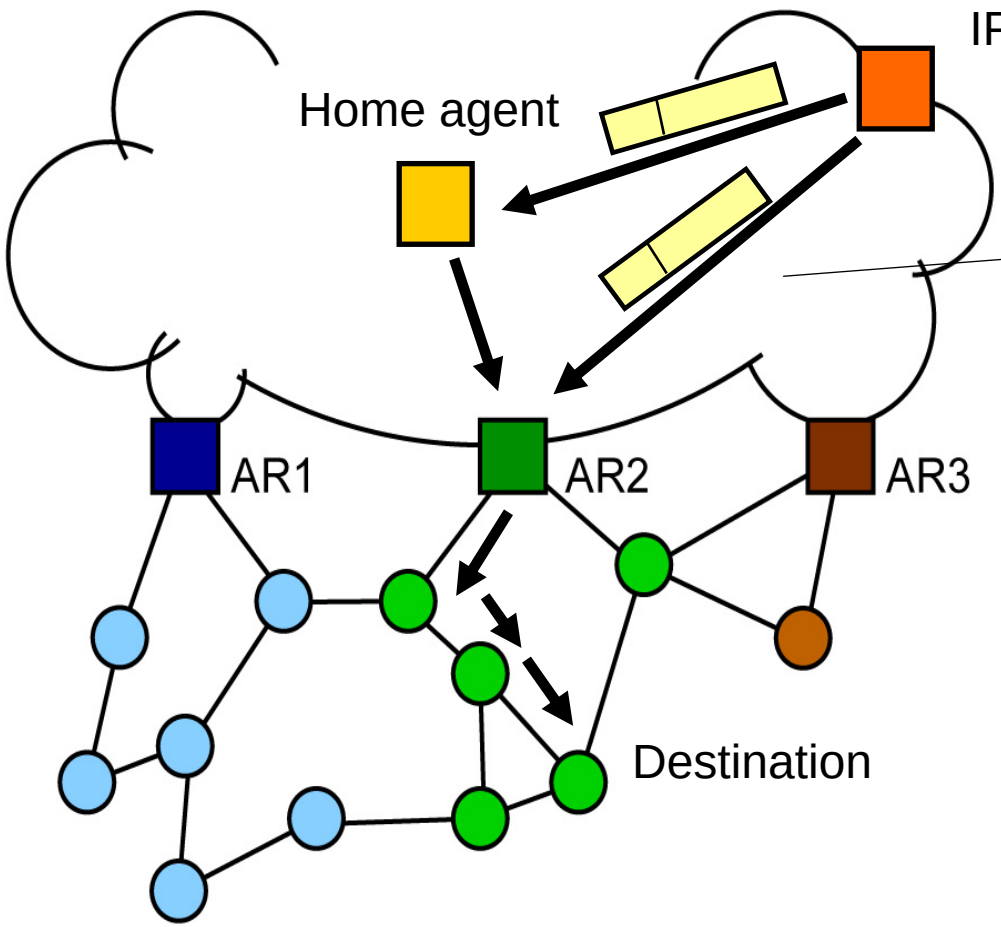
Access routers

Mobile ad hoc nodes

Interconnection of Ad Hoc Networks to the Internet



Routing: Internet -> ad hoc node



Node needs globally valid *care-of IP address* with subnet prefix of AR

IP address:

subnet prefix	host

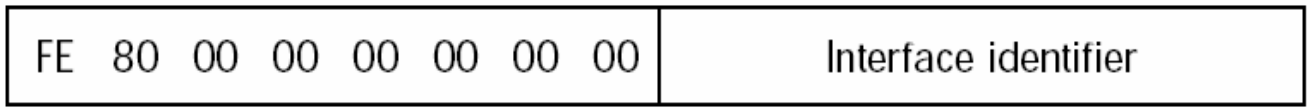
Ad hoc routing protocols
(e.g., AODV, DSR)

How does an ad hoc node obtain its care-of IP address?

IPv6 Stateless Autoconfiguration

- In fixed IPv6 networks with neighbor discovery (NDP):

initial address of node: link-local address



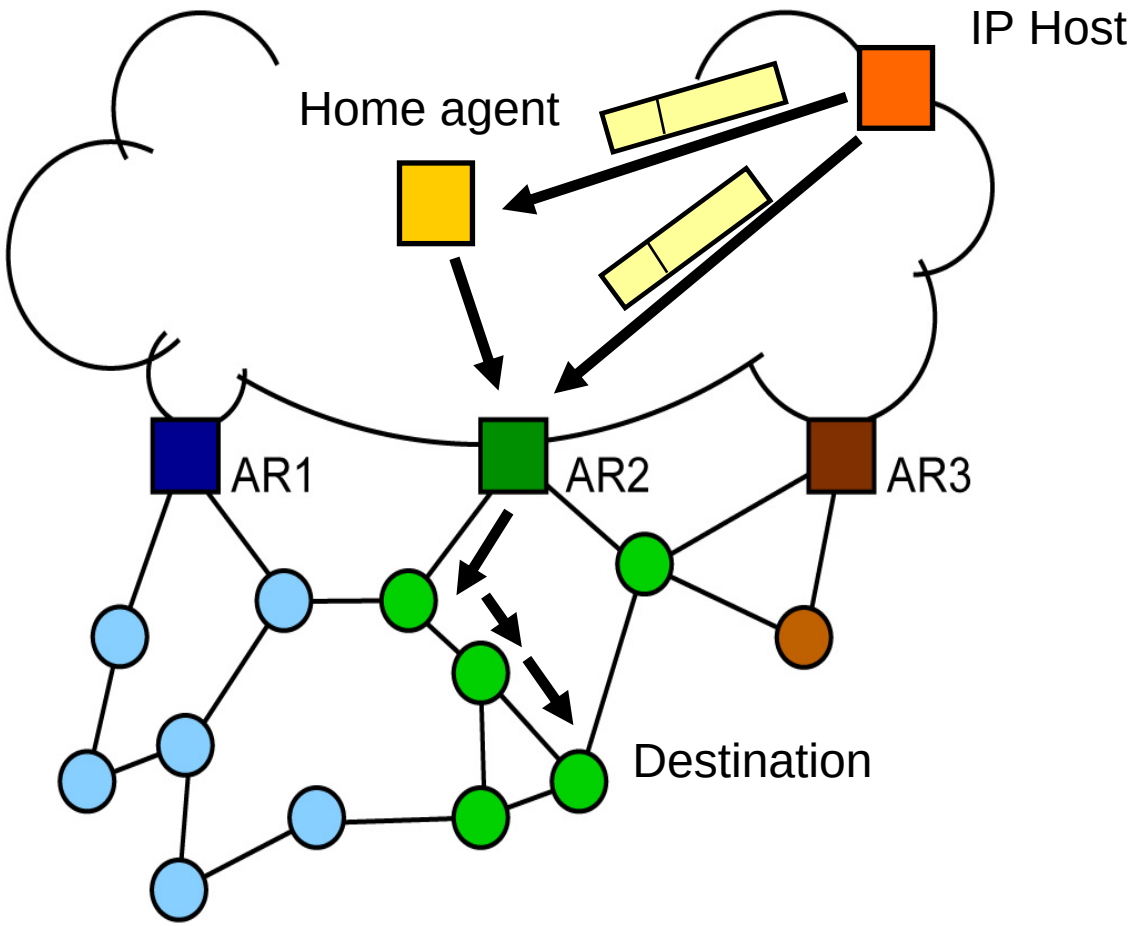
link-local prefix | interface ID

- With this temporary address it contacts AR to get subnet prefix
- Problem: *Link-local prefix* not appropriate in multihop environm.
- Solution: Definition of *MANET-local prefix* (only valid in ad hoc network)

Duplicate Address Detection

- We cannot guarantee the uniqueness of addresses because of the mobile scenario.

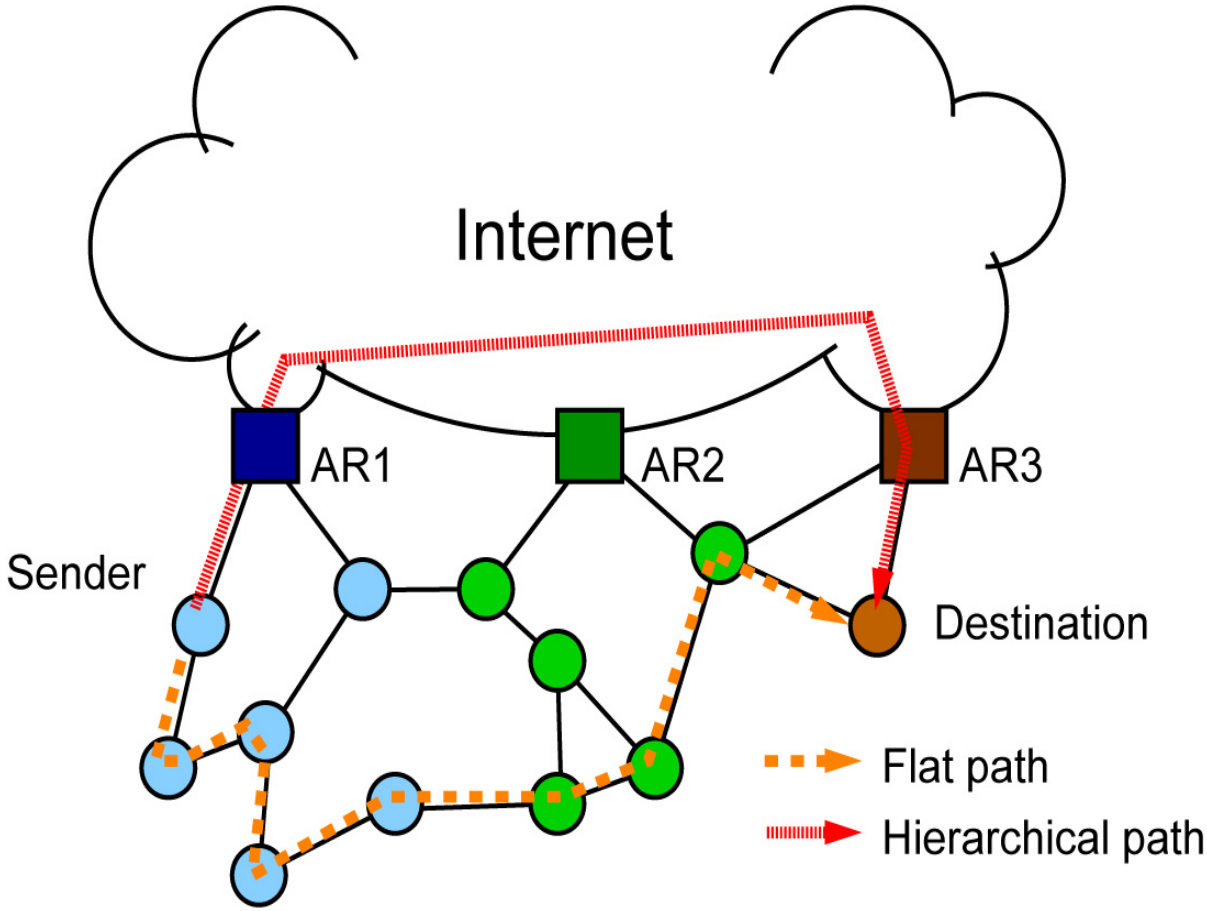
Routing: Internet -> ad hoc node



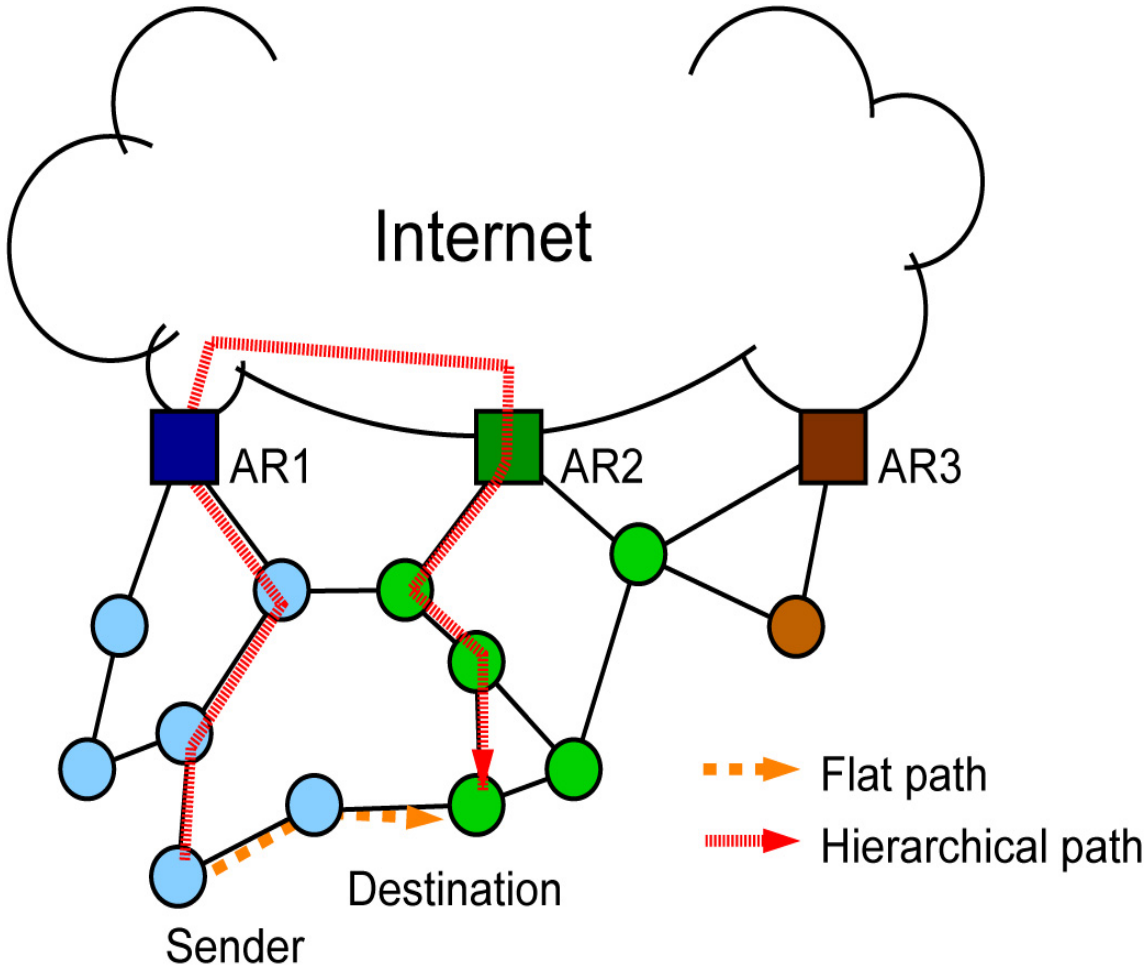
Multiple Addresses

- **Home IP address**
  - prefix of home network; globally routable
  - for identification
- **Care-of IP address**
  - location-dependent; prefix of current AR; globally routable
  - for routing from Internet to corresponding (AR)
  - for hierarchical routing ad hoc node <-> ad hoc node
- **MANET-local address**
  - reserved MANET prefix
  - for autoconfiguration of care-of address
  - for flat routing ad hoc node <-> ad hoc node

Routing: Ad Hoc Node -> Ad Hoc Node



Routing: Ad Hoc Node -> Ad Hoc Node



Summary

- Good advances in solving the interconnection of ad hoc networks to fixed IP networks:
  - Address autoconfiguration
  - Hybrid routing
- But still open issues:
  - Path selection
  - Gateway selection
  - ..

Some Literature

- **Broch, Maltz, Johnson**: “Supporting Hierarchy and Heterogeneous Interfaces in Multi-Hop Wireless Ad Hoc Networks,” *ISPAN*, 1999.
- **Jönsson, Alriksson, Larsson, Johansson, and Maguire**: “MIPMANET: Mobile IP for mobile ad hoc networks,” in *Proc. ACM MobiHoc*, 2000.
- **Sun, Belding-Royer, Perkins**: “Internet Connectivity for Ad hoc Mobile Networks,” *Intern. J. of Wireless Information Networks*, 9(2), April 2002.
- **Xi and Bettstetter**: “Wireless Multi-Hop Internet Access: Gateway Discovery, Routing, and Addressing,” In *Proc. Intern. Conf. on 3G Wireless and Beyond (3Gwireless'02)*, May 2002.
- **Andreadis**: “Providing Internet Access to Mobile Ad Hoc Networks”, *London Communications Symposium*, Sept 2002.
- **Wakikawa, Malinen, Perkins, Nilsson, Tuominen**: Global connectivity for IPv6 Mobile Ad Hoc Networks” (draft-wakikawa-manet-globalv6-02.txt), Nov 2002
- **Ratanchandani and Kravets**: “A Hybrid Approach to Internet Connectivity for Mobile Ad Hoc Networks”, *IEEE WCNC*, Mar 2003.

Summary and Future Research

Christian Bettstetter, TU München

Outline of the Remainder of the Tutorial

- Principles and Applications
- Routing
- Information diffusion in sensor networks
- Medium access control (MAC)
- Security
- Clustering
- Connectivity
- Interworking with fixed IP networks
- Future research directions

Future Research

- Cross-layer topics: Reliability, fairness, ...
- Directional Antennas
- Information-theoretical topics
- Interconnection to fixed IP networks
- Vehicular networks
- ...