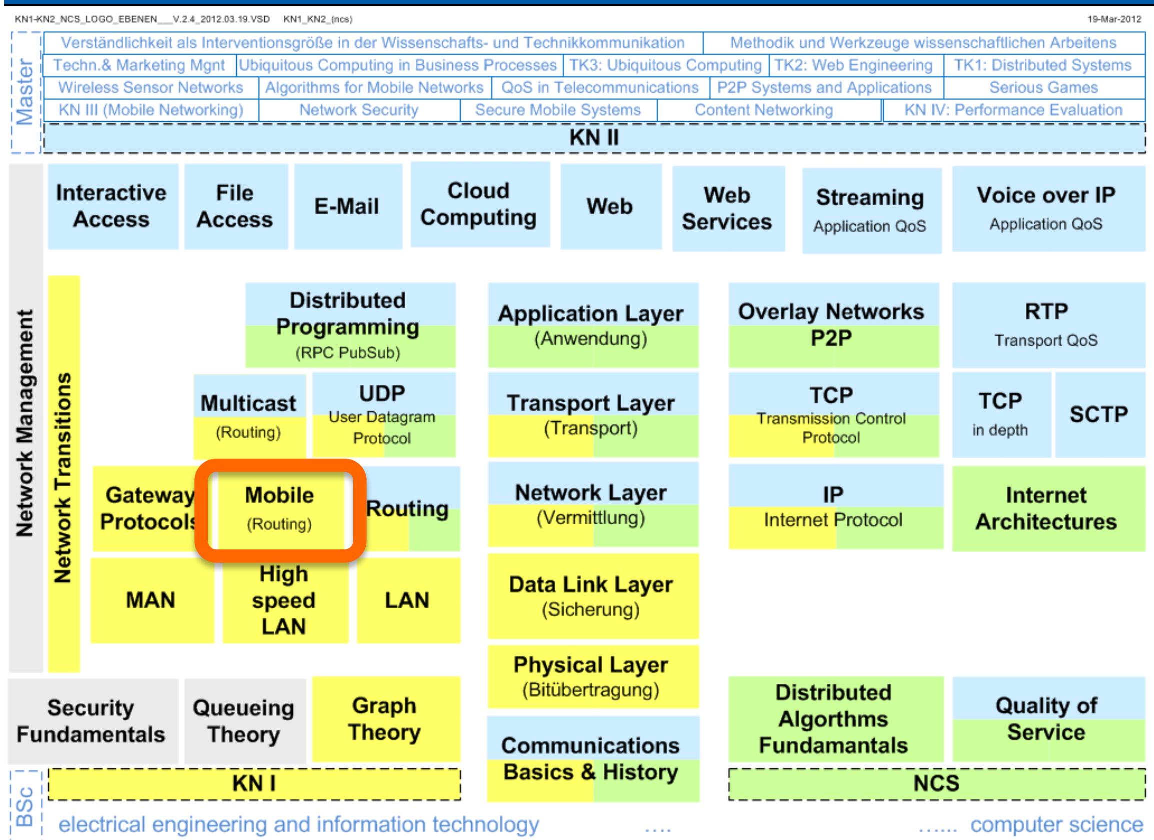
# Communication Networks I

## Mobile Routing





Prof. Dr.-Ing. **Ralf Steinmetz**

KOM - Multimedia Communications Lab

# Overview

# 1 Basic Challenges in Mobile Networking

## Interesting problems spanning multiple layers

- Security, QoS, Scalability, Heterogeneity, Adaptation, Dependability

## Application Layer

- Discovery of Services, where to place services, service awareness

## Transport Layer

- Esp. TCP-performance

## Network Layer

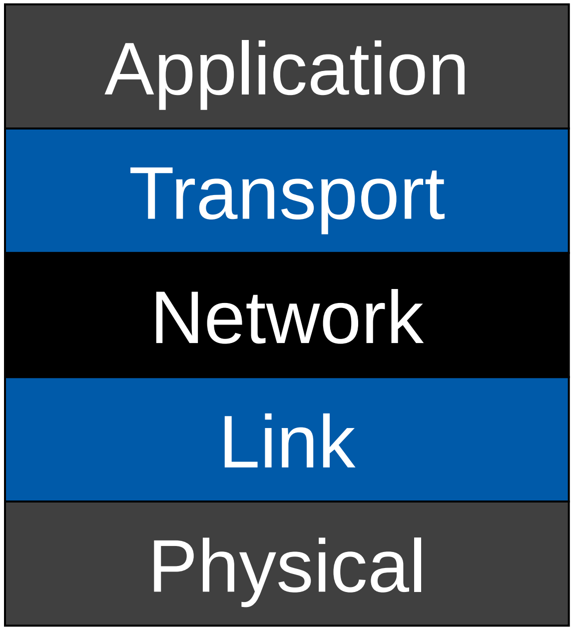
- Adaptation of routing protocols, multicast routing

## Link Layer

- Medium Access Control / Scheduling

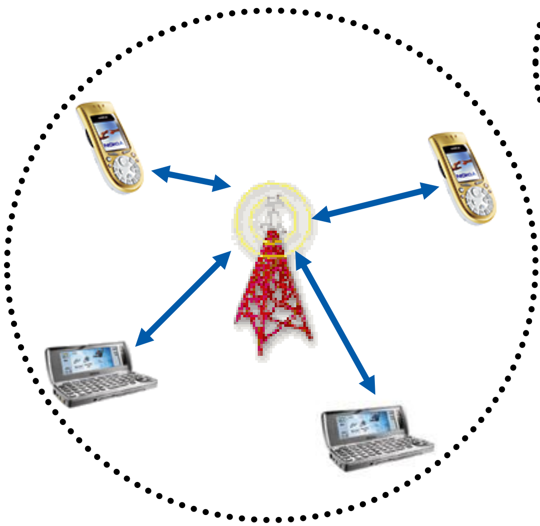
## Physical Layer

- Power Control
  (to maximize power-usage / to minimize interference)

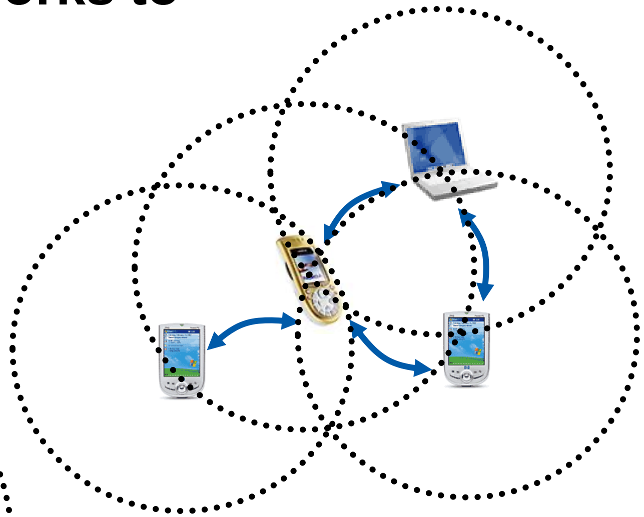


# Types of Mobile Networks

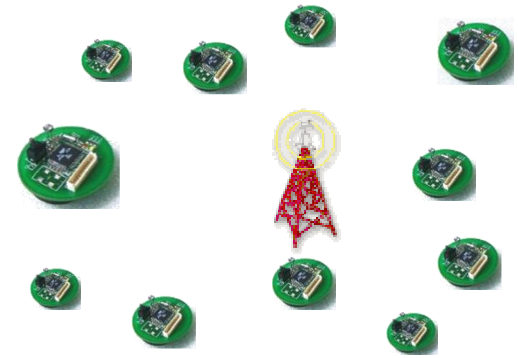
**Today, diverse networks to support mobility**



Cellular networks



Ad hoc networks

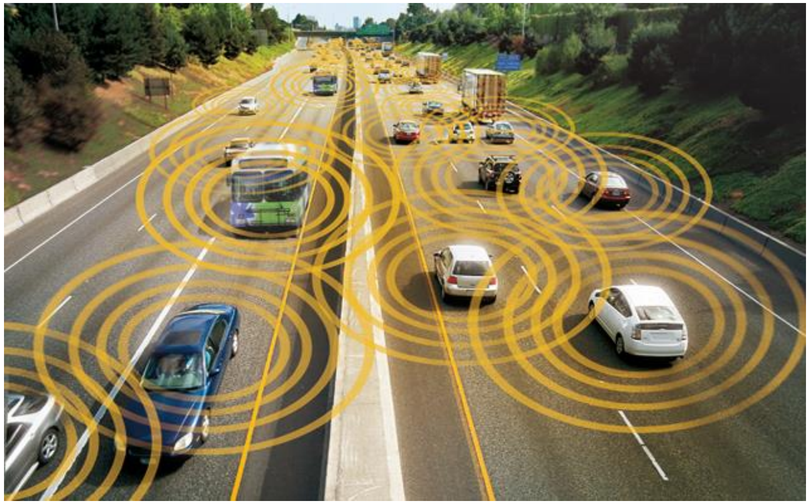


Sensor networks

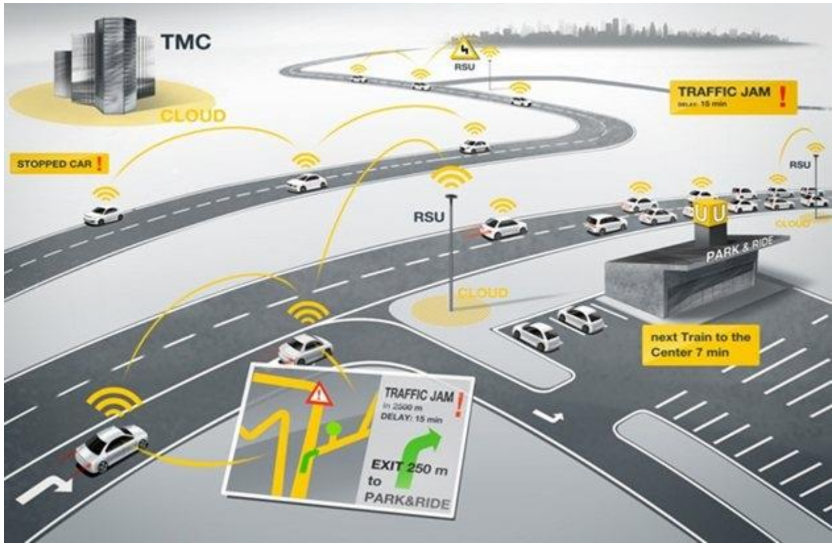
**Based on work with KN 3 – Mobile Networks (M. Hollick)**

**Fits well with lectures on mobile communications**

# Example: Car-to-car communication



Source: extremetech.com




Source: robohaat.com

## Two aspects of mobility

- User mobility:
  - users communicate (wireless) “anytime, anywhere, with anyone”
- Device portability:
  - devices can be connected anytime, anywhere to the network

| Wireless | vs. mobile | Examples |
| --- | --- | --- |
| ✗ | ✗ | **stationary computer** |
| ✗ | ✓ | **notebook in hotel** |
| ✓ | ✗ | **wireless LANs in historic buildings** |
| ✓ | ✓ | **Personal Digital Assistant** |

## Nomadic vs. mobile computing

## Integration of wireless networks with fixed networks

# Terminology

## "Ad hoc"

- Often improvised or impromptu; *„an ad hoc committee meeting"*

  *Wordnet*

- Formed or used for specific or immediate problems or needs; *„ad hoc solutions"*

- Fashioned from whatever is immediately available: improvised; *„large ad hoc parades and demonstrations"*

  *Encyclopædia Britannica*

## "Spontaneous"

- Arising from a momentary impulse

- Controlled and directed internally; *„self-acting"*

- Produced without being planted or without human labor; *„indigenous"*

- Developing without apparent external influence, force, cause, or treatment

  *Encyclopædia Britannica*

## (Mobile) Ad Hoc Communication Networks - MANET

- Historical successor of packet radio networks
- Self-organizing, mobile and wireless nodes
- Absence of infrastructure, multi-hop routing necessary
- Systems are both, terminals (end-systems) and routers (nodes)
- Constraints (dynamics, energy, bandwidth, link asymmetry)

# What is different?
# Characteristics of Ad Hoc Communications

TECHNISCHE UNIVERSITÄT DARMSTADT

## Variability

- Mobility characteristics
  - speed, predictability, uniformity, synthetic vs. empirical models , …
- Wireless characteristics
  - broadcast nature of the network, packet losses due to transmission errors, limited range, hidden and exposed terminals, partitioning
- Application / traffic characteristics and patterns
  - P2P, real time, unicast, multicast, geocast, CBR, VBR, self-similar, …
- System characteristics
  - distribution, absence of infrastructure, (unpredictable) high dynamics, (a)symmetry …

## Inherent heterogeneity

- Do nodes have identical capabilities, responsibilities, and constraints?
  - Transmission ranges and radios may differ, battery life may differ, processing capacity may differ,
    - asymmetric capabilities
  - Only some nodes may route packets, some nodes may act as leaders of nearby nodes, e.g. cluster head
    - asymmetric responsibilities

→ **Adaptation is crucial**

# 2 Challenges in Mobile Communications

Application

Transport

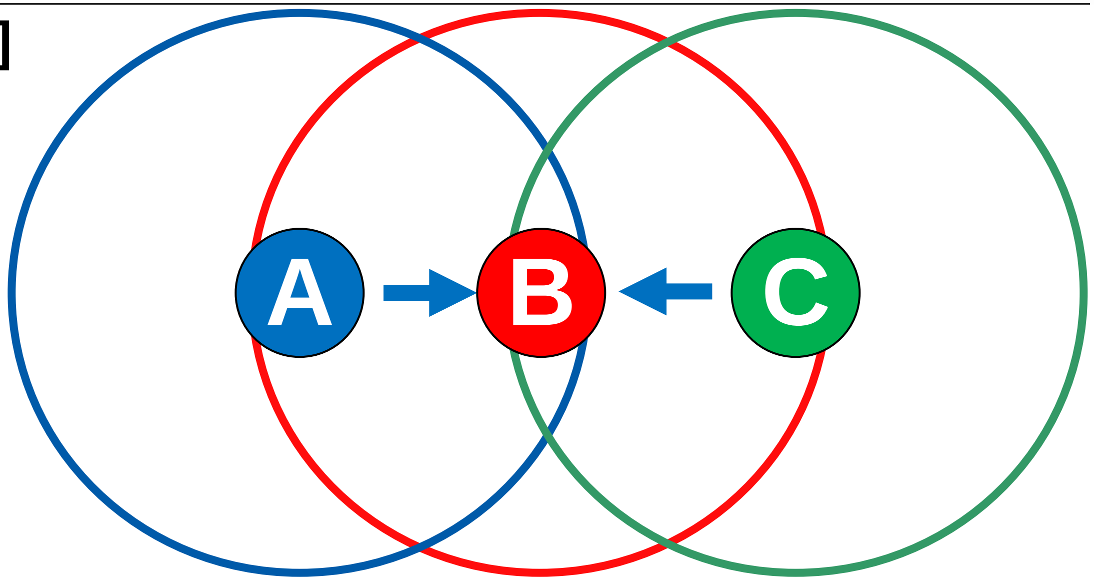
Network

Link

Physical

### Hidden terminals [Tobagi75]

- Nodes A and C cannot hear each other
- Transmissions by nodes A and C can collide at node B
- Nodes A and C are hidden from each other



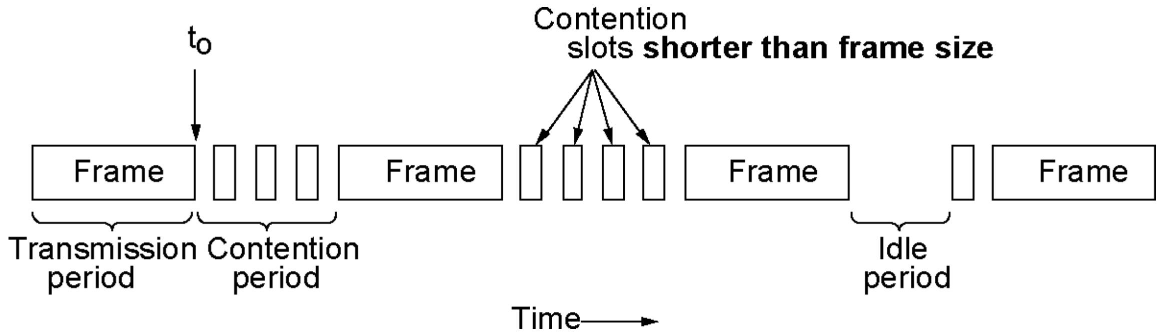

### E.g.

- A sends to B, C cannot receive A
- C senses a “free” medium (carrier sense fails), C sends to B
- Collision at B, A cannot detect the collision (collision detection fails)
- A is “hidden” for C and vice versa

### Problems

- More collisions, unreliability as a result
- Waste of resources
- CSMA/CD does not fit …

# CSMA CD in Troubles with Hidden Terminal Problem




## Carrier Sense Multiple Access with Collision Detection

- CSMA 1-persistent with CD

## Principle

- Sending station interrupts transmission as soon as it detects a collision
  - saves time and bandwidth
  - frequently used (802.3, Ethernet)
  - Algorithm: station has to realize DURING the sending of a frame if a collision occurred

## Extreme case

- Short frame, maximum distance to station

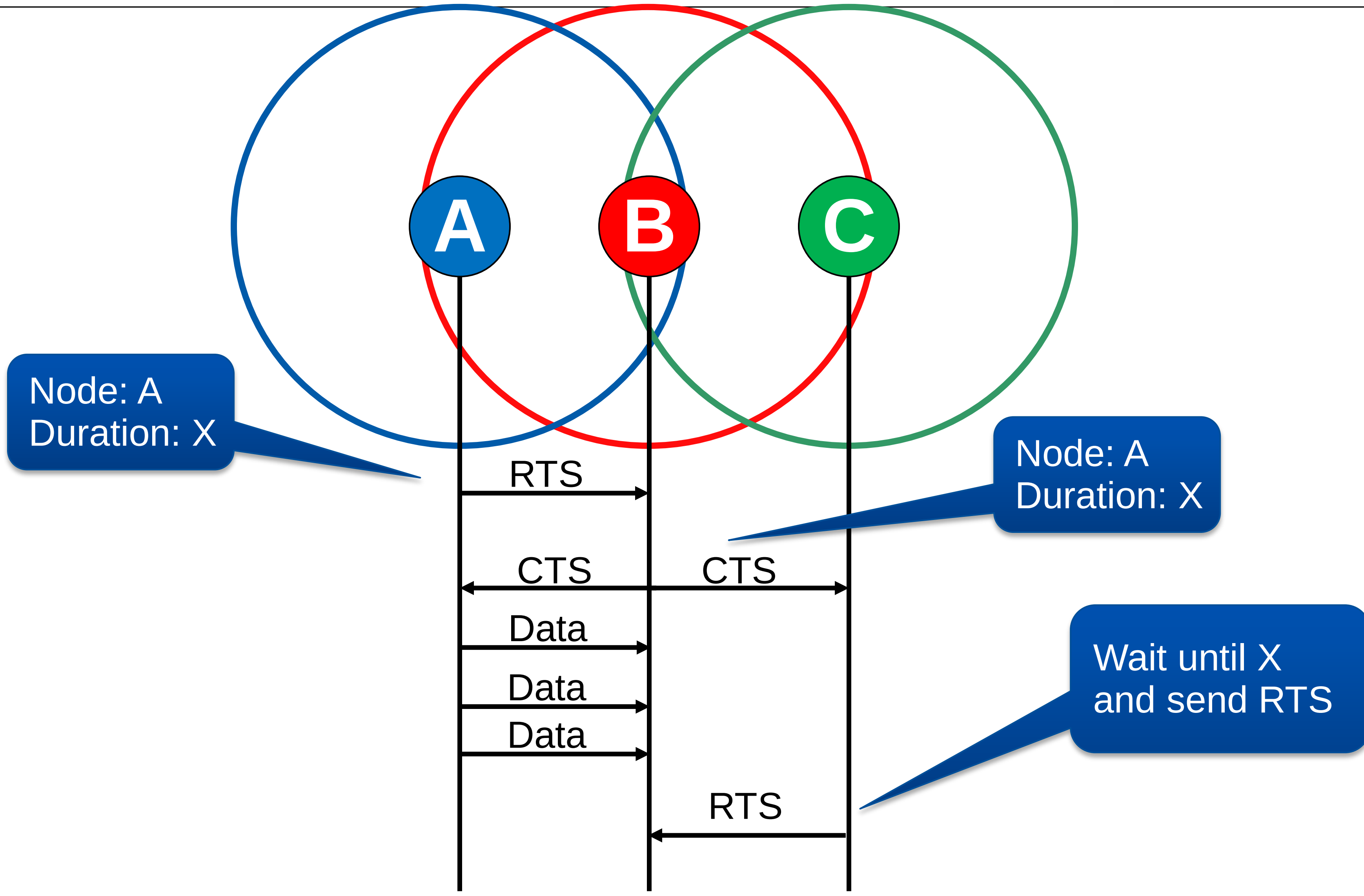
# Solution for Hidden Terminals Problem

## Busy Tone [Tobagi75, Haas98]

- A receiver transmits busy tone when receiving data
- All nodes hearing busy tone keep silent
- Avoids interference from hidden terminals
- Requires a separate channel for busy tone

## And: Reliability achieved by Acknowledgements (ACK)

# Solution for Hidden Terminals Problem CSMA/CA



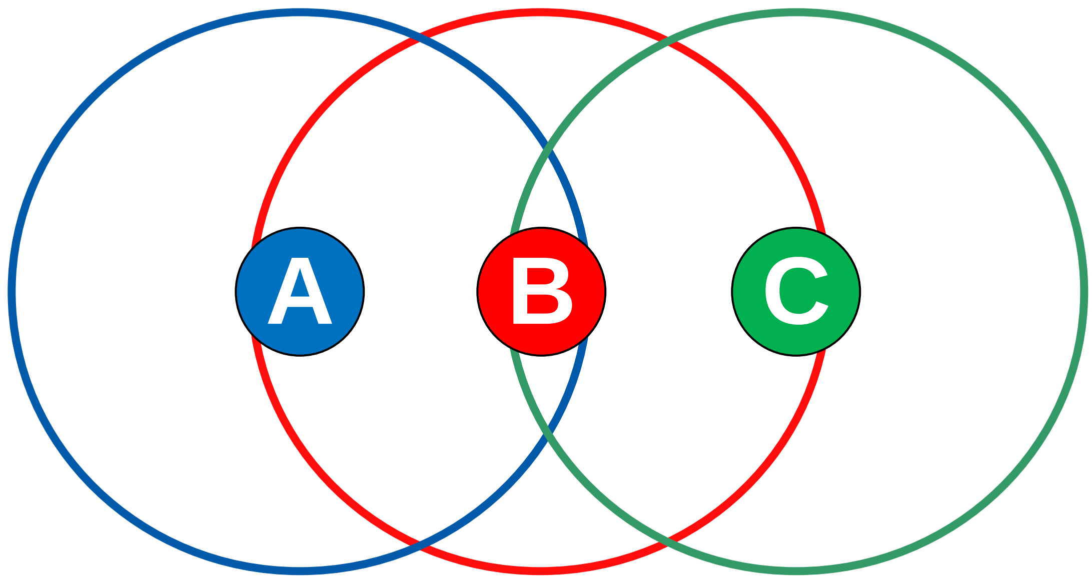
# Solution for Hidden Terminals Problem CSMA/CA

## Carrier Sense Multiple Access/Collision Avoidance CSMA/CA

## i.e. MACA

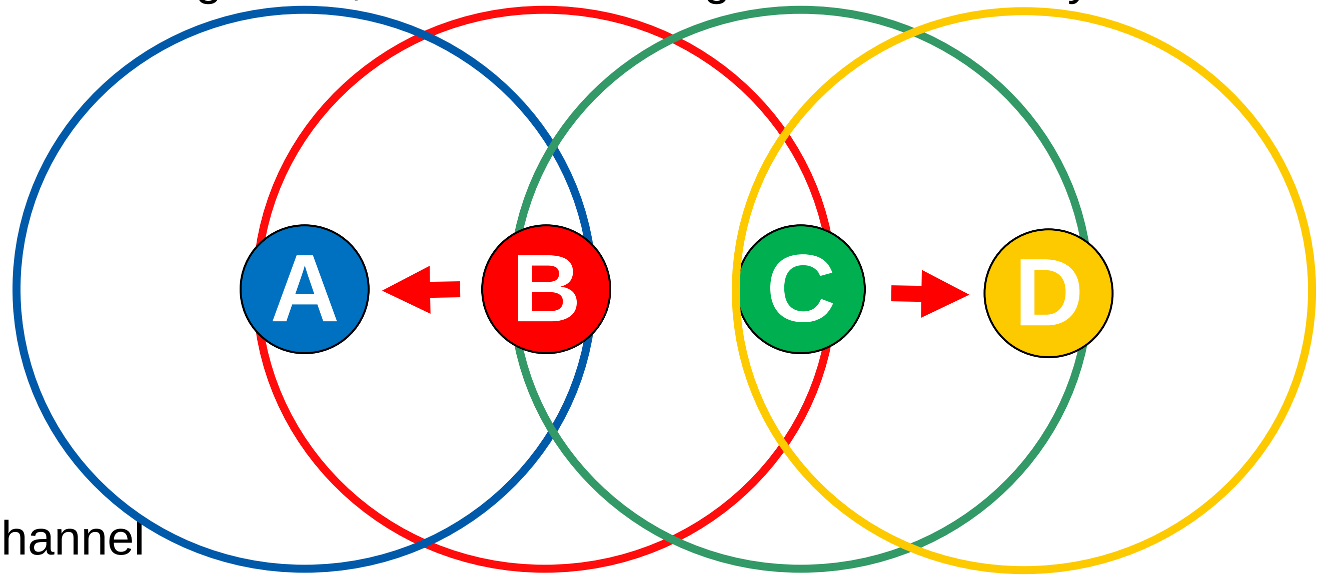
## Solution for Hidden Terminal Problem [Karn90]

- A first sends a Request-to-Send (RTS) to B
- On receiving RTS, B responds Clear-to-Send (CTS)
- Hidden node C overhears CTS and keeps quiet
  - Transfer duration is included in both RTS and CTS
- Exposed node overhears a RTS but not the CTS
  - C's transmission cannot interfere at B



## Exposed terminals

- B sends to A, C wants to send to another terminal (not A or B)
- C has to wait, signals a medium in use
- But A is outside the radio range of C, therefore waiting is not necessary
- C is "exposed" to B



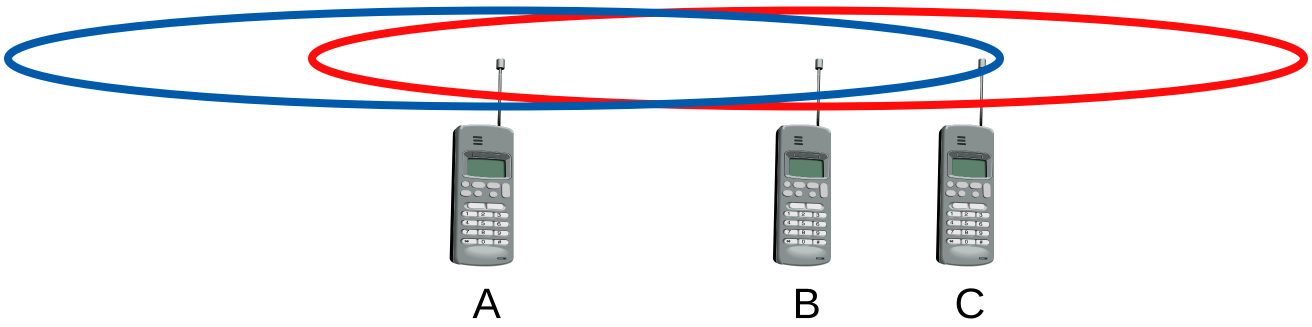

## Problems

- Underutilization of channel
- Lower effective throughput
- CSMA/CD does not fit

TECHNISCHE UNIVERSITÄT DARMSTADT

## Terminals A and B send, C receives

- Signal strength decreases proportionally to square of distance
- Signal of B therefore drowns out A’s signal
- C cannot receive A

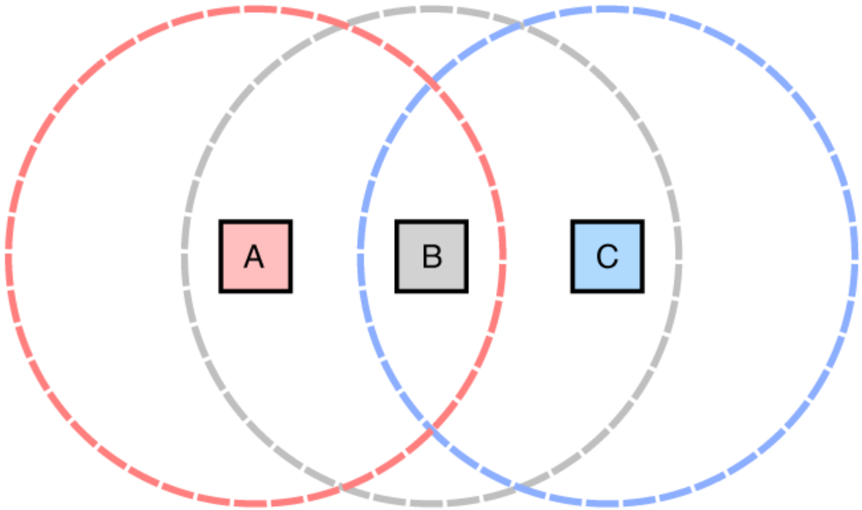


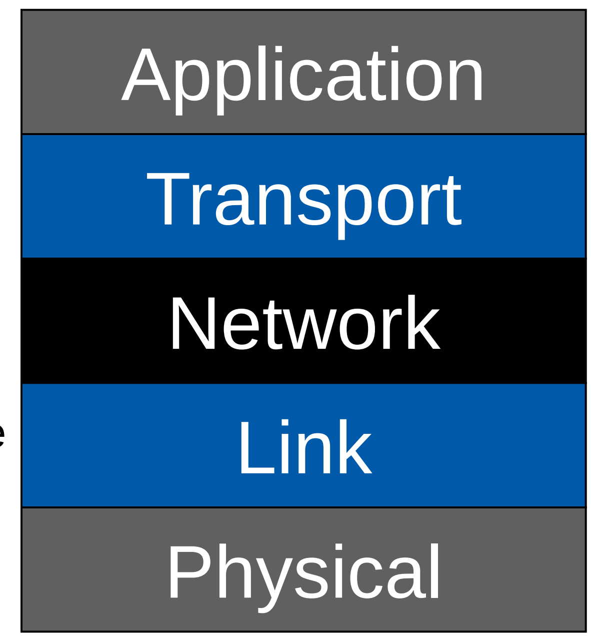

## If e.g. C is arbiter for sending rights

- B would drown out terminal A already on the physical layer

## Also severe problem for CDMA-networks –
## → precise power control needed

## Why specialized Ad Hoc Routing ?




- Some nodes may be out of range of others
- Must use other peer nodes as routers to forward packets
- Need to find new routes as nodes move or conditions change
  - (highly dynamic and unpredictable)
- Routing protocol captures and distributes state of network
- Routing strategy (algorithm) computes shortest paths

# Requirements for Ad Hoc Routing

## The routing protocol needs to

- Converge fast
- Minimize signaling overhead

## The routing strategy (algorithm) may include

- Shortest distance
- Minimum delay
- Minimum loss
- Minimum congestion (load-balancing)
- Minimal interference
- Maximum stability of routes or maximal signal strength
- Minimum energy (power aware routing)

## Standard Internet routing cannot fulfill these requirements

- Assumes infrastructure, assumes symmetrical conditions, assumes plenty of resources, to slow, misses metrics, …

# 3.1 Overview on Ad Hoc Routing Protocols

## Proactive protocols

- Routing information is computed and updated independent of whether there is any traffic between the nodes or not
- Traditional routing protocols are proactive
  - Link-state and
  - Distance-vector

## Reactive protocols

- Routes calculated / maintained when there is traffic and no route is known
- Routes are calculated only when needed, i.e.,
  - A does not compute route to B until A wants to send something to B
- When do we calculate the route?
  - For connection-oriented:
    - At connection setup
  - For connectionless:
    - On first packet

## Hybrid protocols

# Ad Hoc Routing Paradigms

## Flooding of Data Packets

- Simple approach, extremely high overhead
- Many protocols perform (limited) flooding of control packets
  - To discover routes
  - Overhead of control packet flooding is amortized over data packets transmitted between consecutive control packet floods

## Non-Uniform Protocols

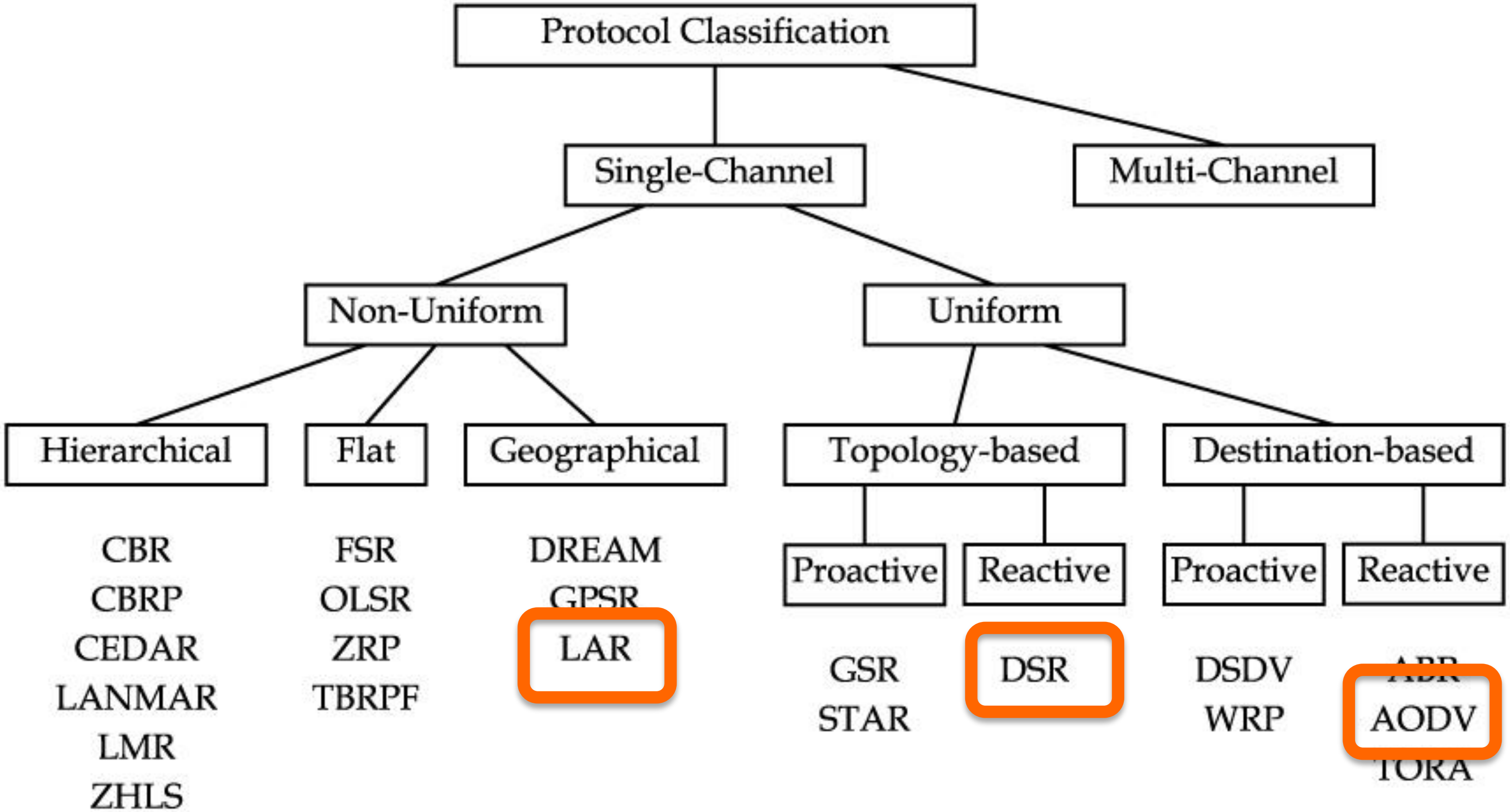
- Hierarchical protocols, Cluster-based, flat protocols
- Geographical protocols
- Hybrid protocols (e.g. combination of proactive and reactive)

**→ There is no "BEST" ad hoc routing**

## Uniform Protocols

- Topology-based (e.g. source routing)
- Destination-based (usually distance vector paradigm)
- Proactive
  - (table-driven) vs.
- Reactive
  - (on-demand) paradigms

# Taxonomy of Routing Protocols




**above mentioned protocols are only a selection – the ones which will move forward to Experimental RFC (within IETF) will be highlighted**

# Some Routing Protocols / Frameworks

**AODV – Ad Hoc On Demand Distance Vector**
- Perkins, NOKIA; Belding-Royer, UCSB; Das, UC

**CEDAR – Core-Extraction Distributed Ad Hoc Routing**

**DREAM – Distance Routing Effect Algorithm for Mobility**

**DSDV – Destination-Sequenced Distance Vector**

**DSR – Dynamic Source Routing**
- Johnson, CMU

**FSR – Fisheye State Routing**

**LANMAR – Landmark Ad Hoc Routing**

**LAR – Location Aided Routing**

**OLSR – Optimized Link State Routing**
- Clausen, Jacquet, INRIA

**TBRPF – Topology Broadcast based on Reverse-Path Forwarding**
- Ogier,Templin, SRI

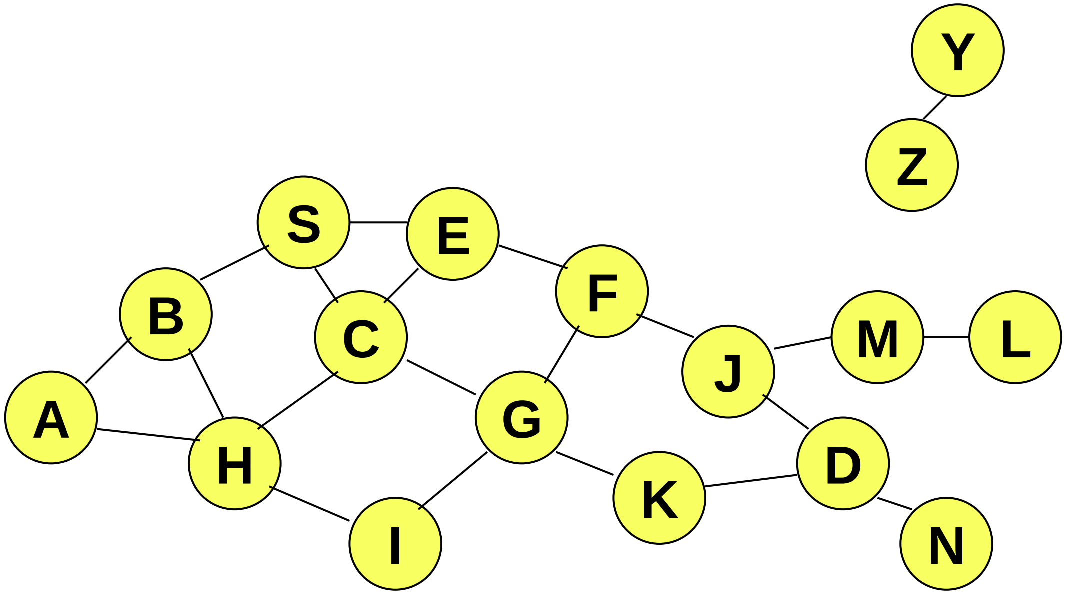
**Tora / IMEP – Temporally-Ordered Routing Algorithm / Internet Manet Encapsulation Protocol**

**ZRP – Zone Routing Protocol**
- Haas, Cornell

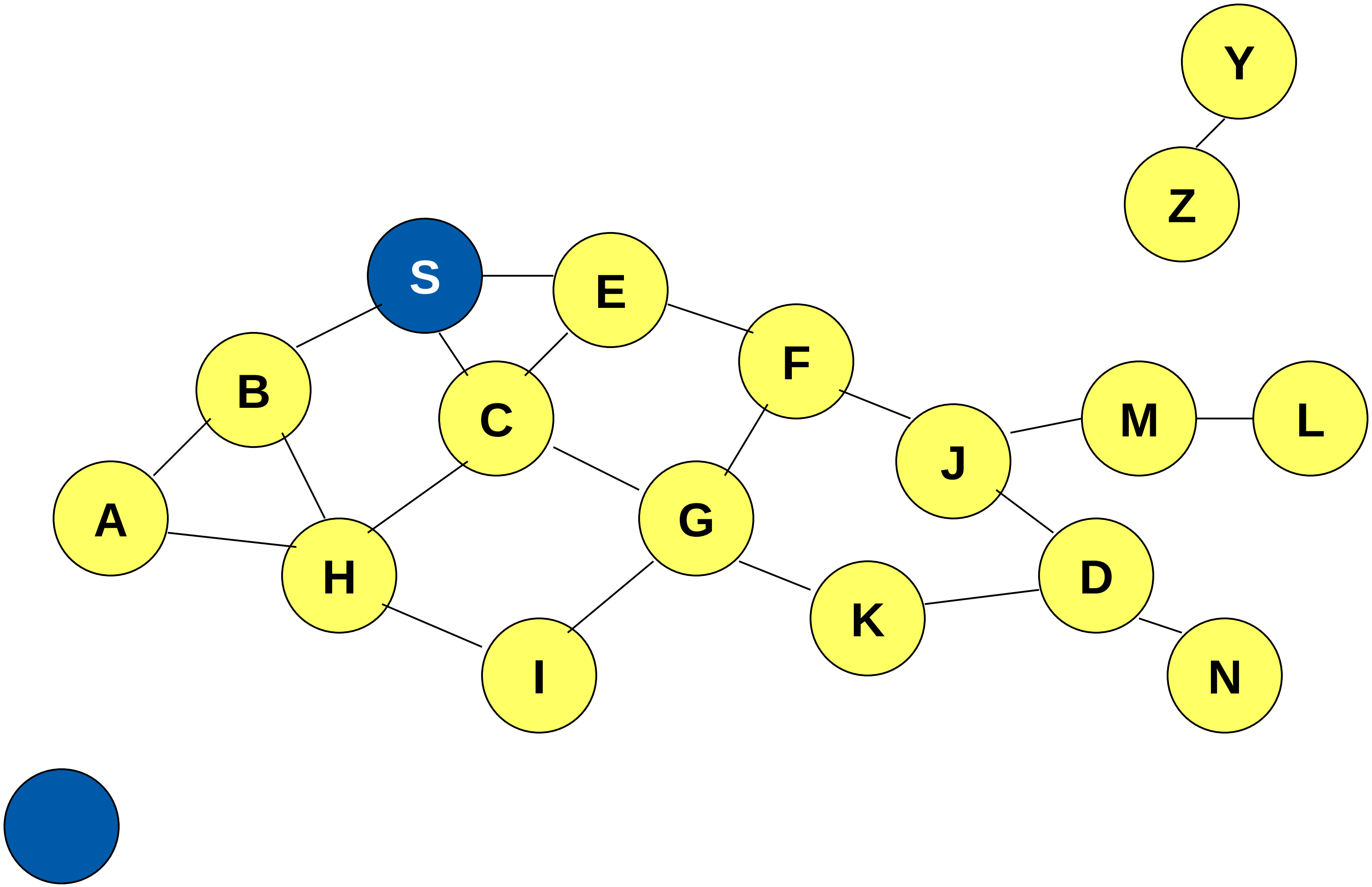
**…**

## Shares some principles with AODV

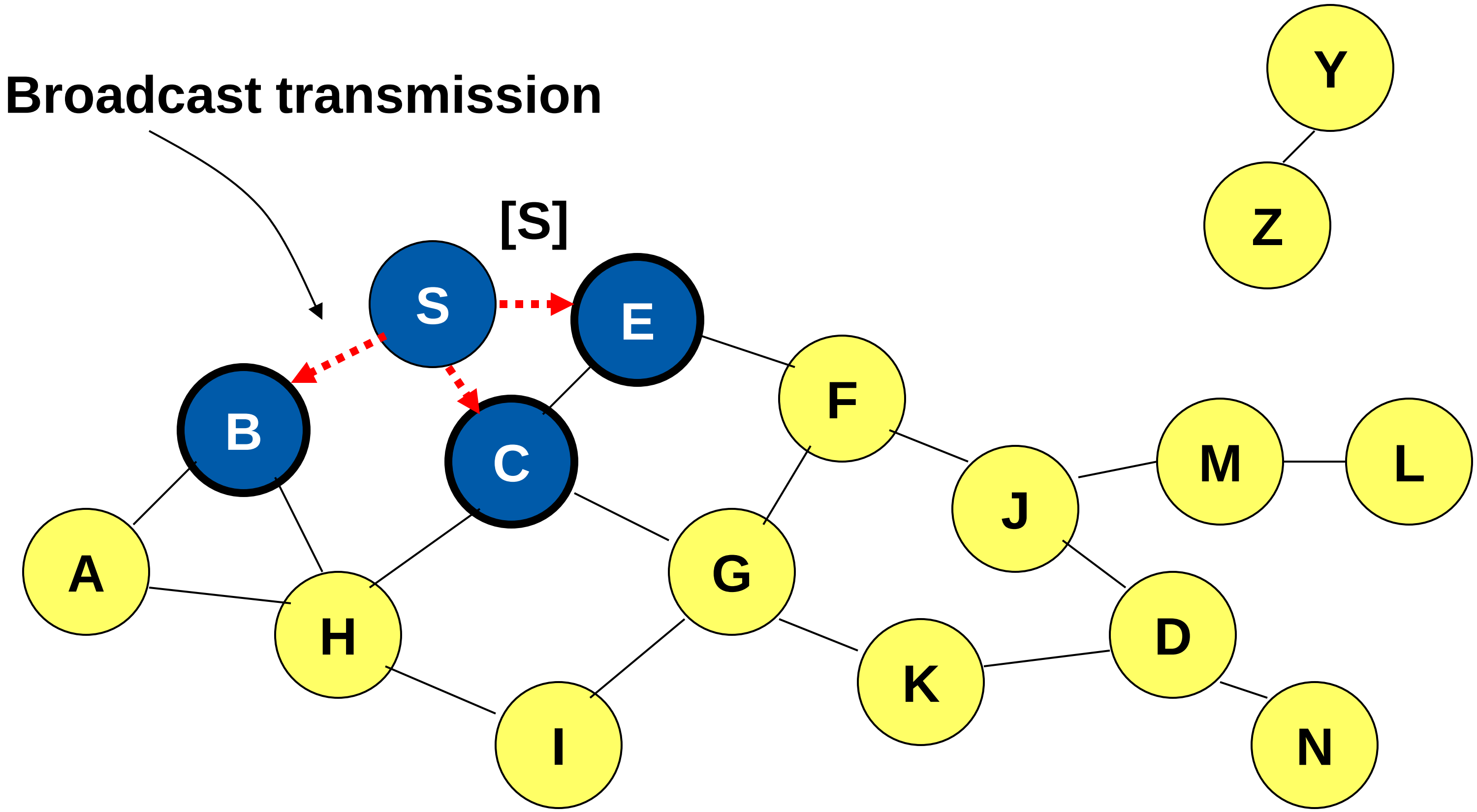
- Reactive routing protocol
- When node S wants to send a packet to node D,
  but does not know a route to D,
  node S initiates a route discovery
- Source node S floods Route Request (RREQ)
- Each node appends own identifier when forwarding RREQ
- Following an example for a route discovery from source S to destination D



# Route Discovery in DSR



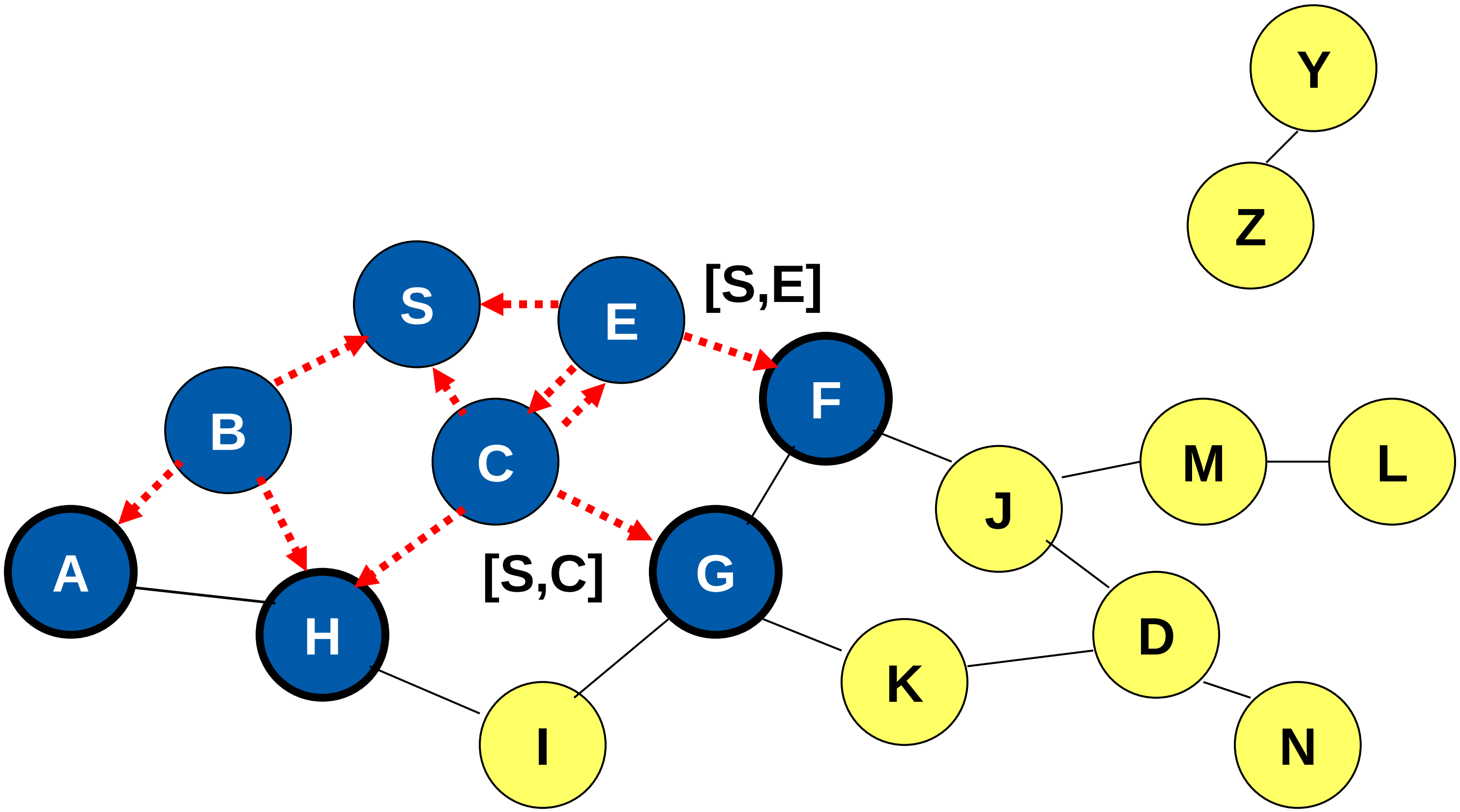
# Route Discovery in DSR




Represents transmission of RREQ

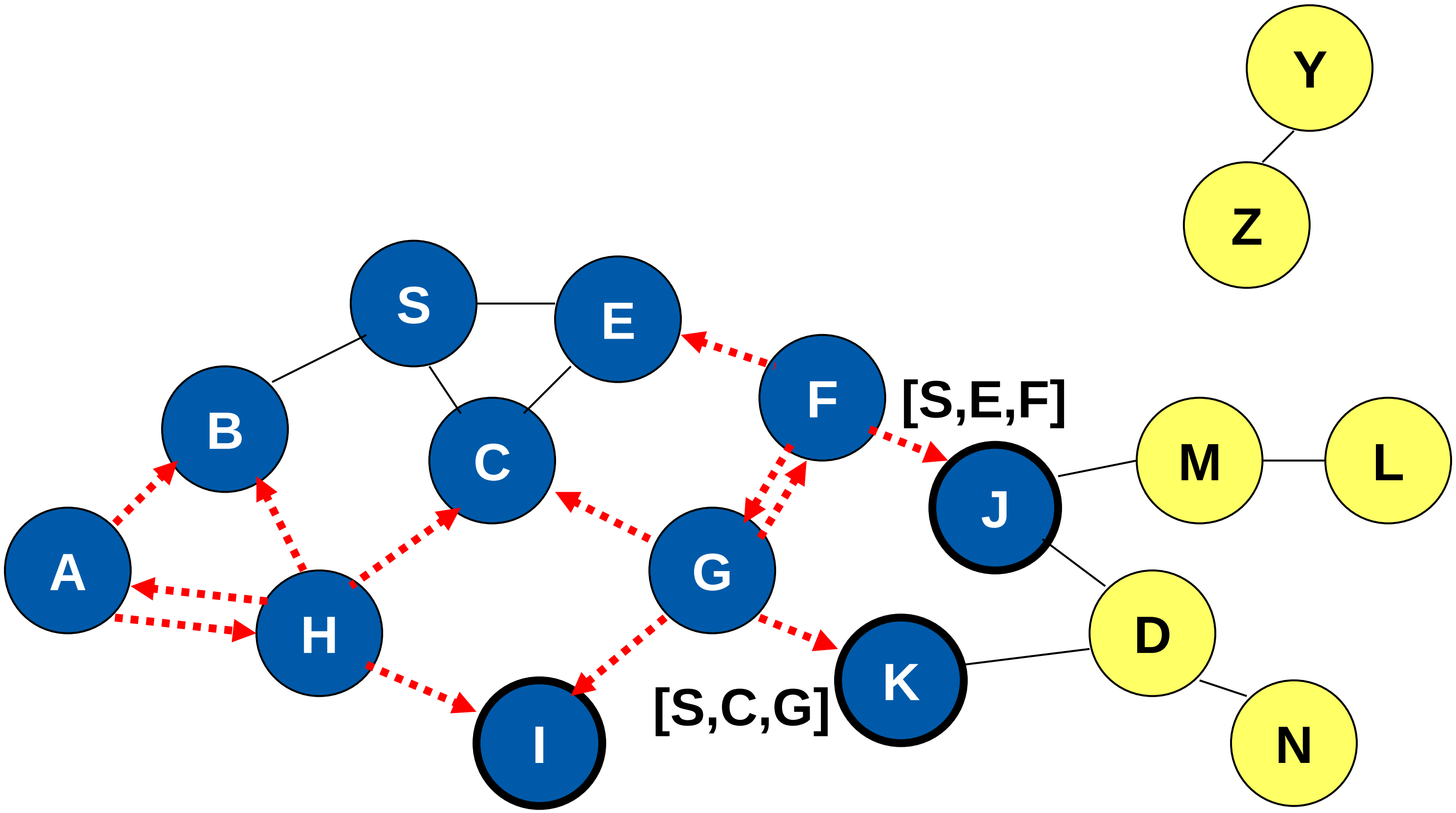
[X,Y] Represents list of identifiers appended to RREQ

# Route Discovery in DSR



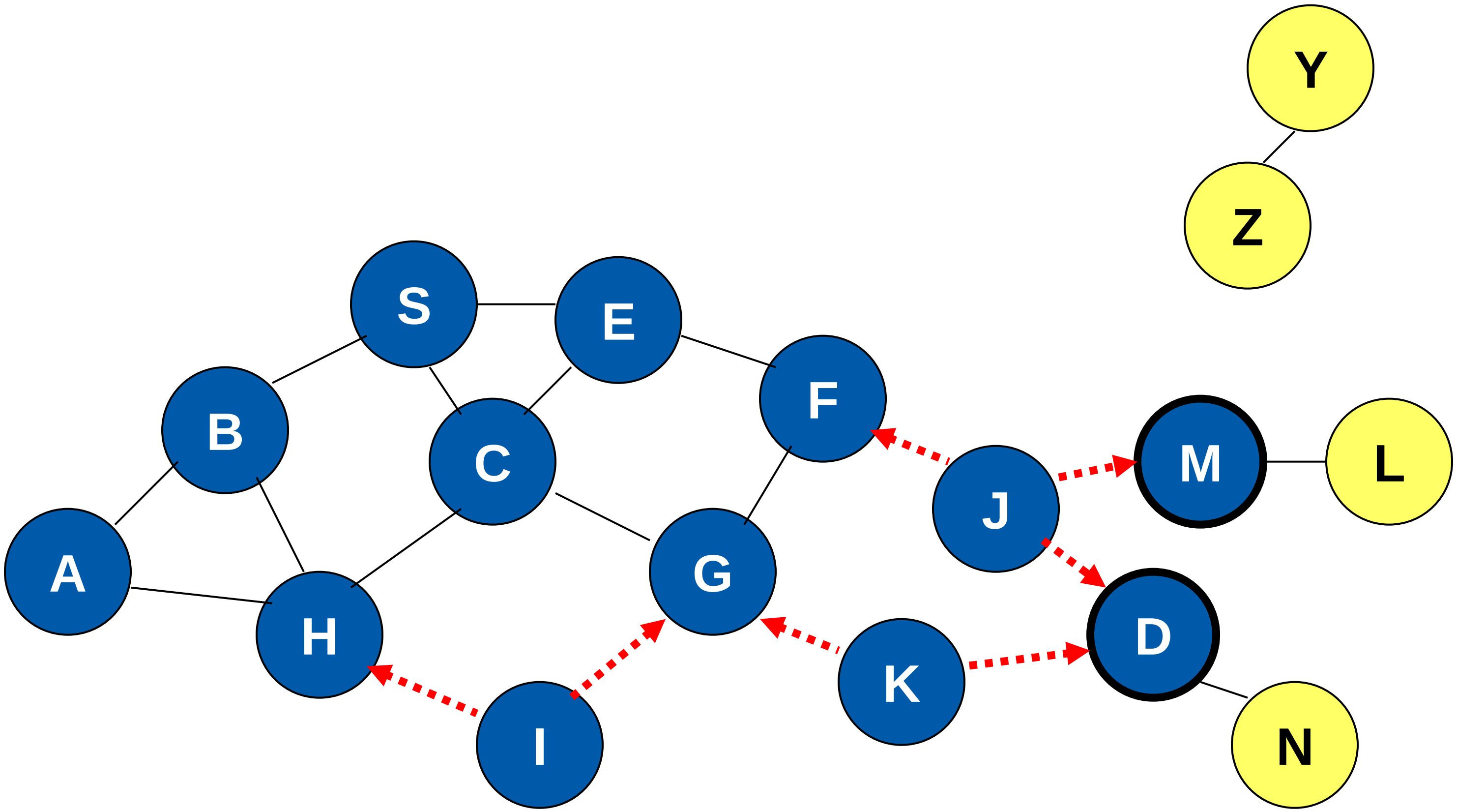

Node H receives packet RREQ from two neighbors:
potential for collision

# Route Discovery in DSR



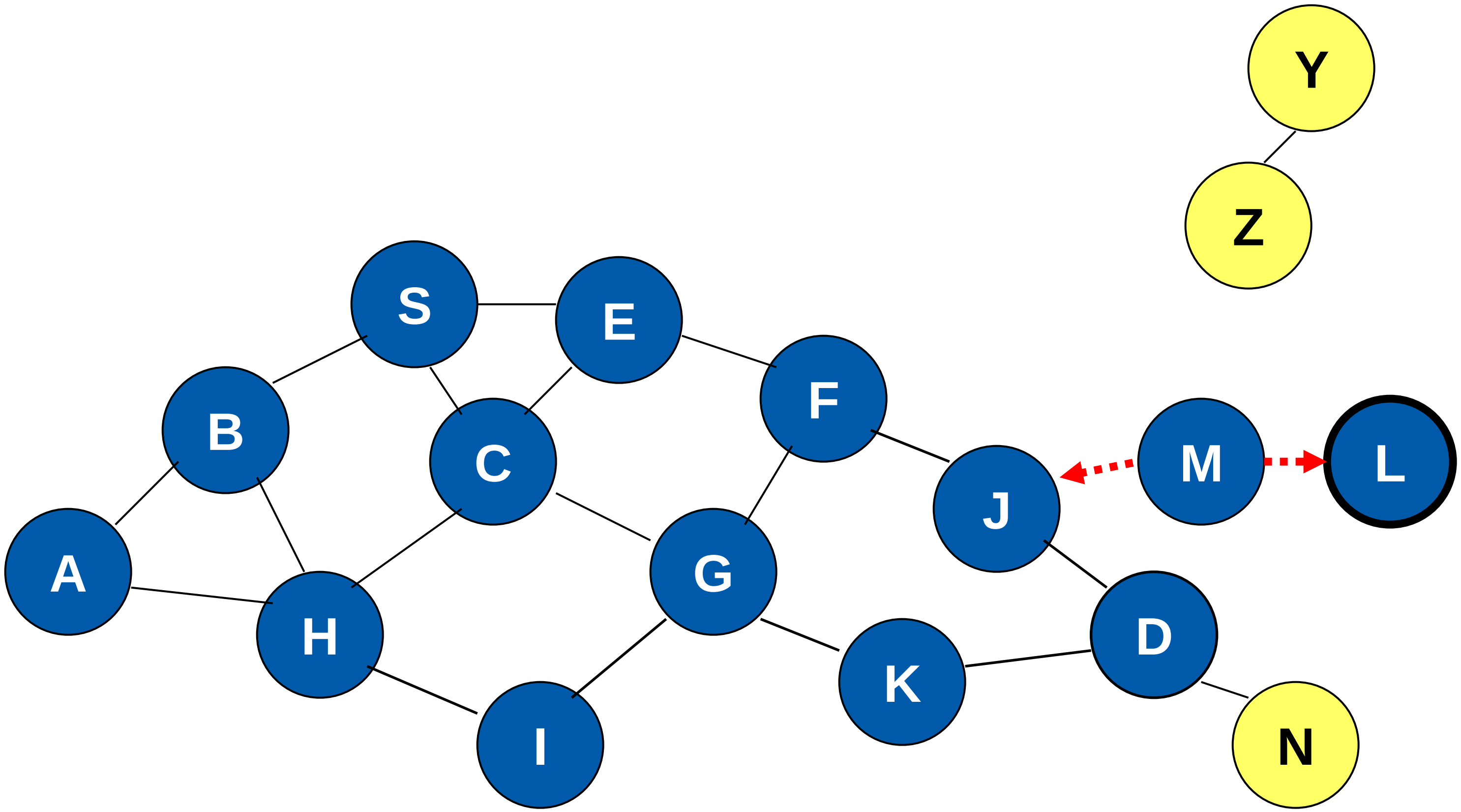

Node C receives RREQ from G and H, but does not forward it again, because node C has already forwarded RREQ once

# 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




Node D does not forward RREQ, because node D is the intended target of the route discovery

# Route Discovery in DSR

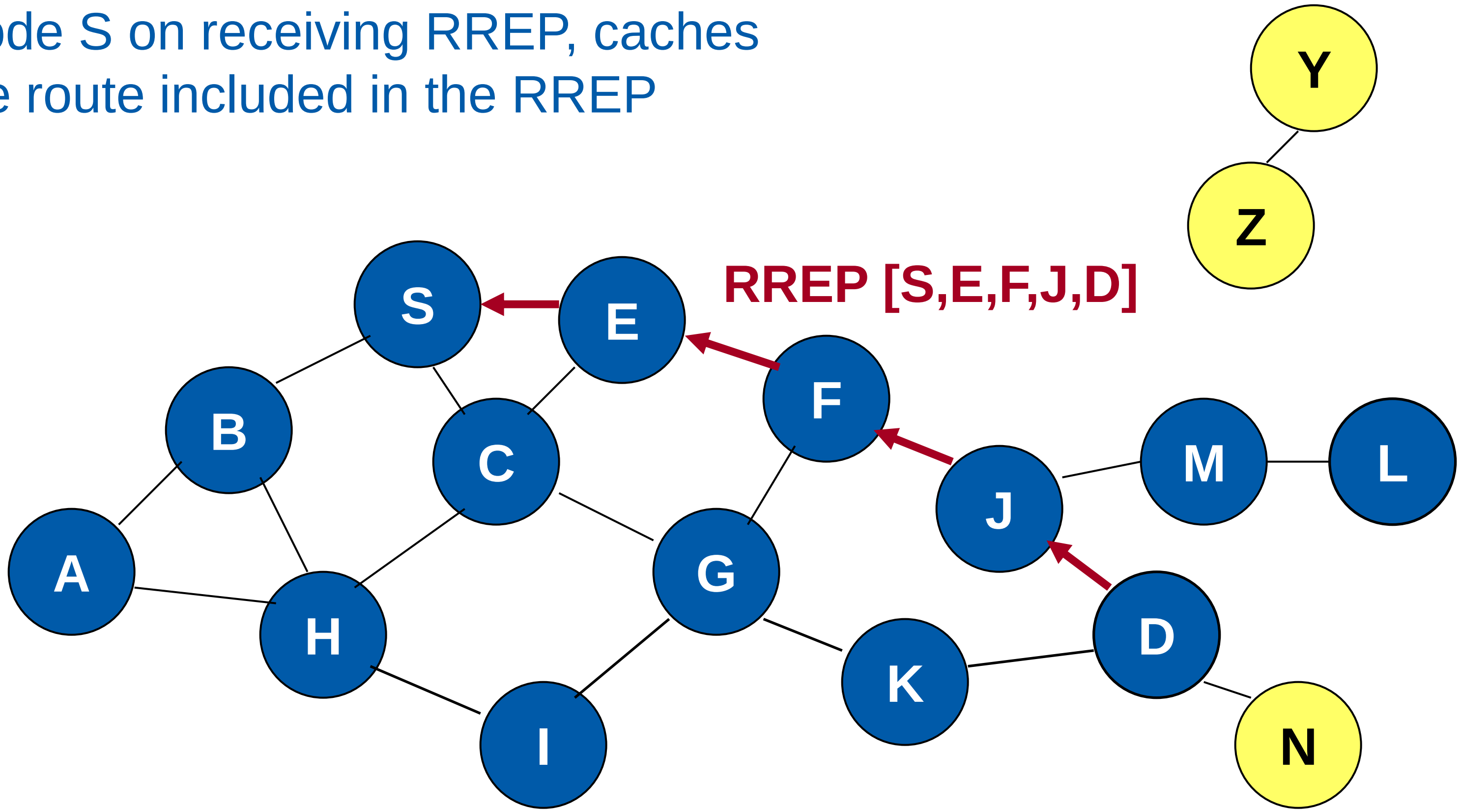
## Route Reply (RREP)

- Destination D on receiving the first RREQ, sends a (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 can be sent by reversing the route in Route Request (RREQ) only if links are guaranteed to be bi-directional
- If unidirectional (asymmetric) links are allowed, then RREP may need a route discovery for S from node D
  - Unless node D already knows a route to node S

# Route Reply in DSR

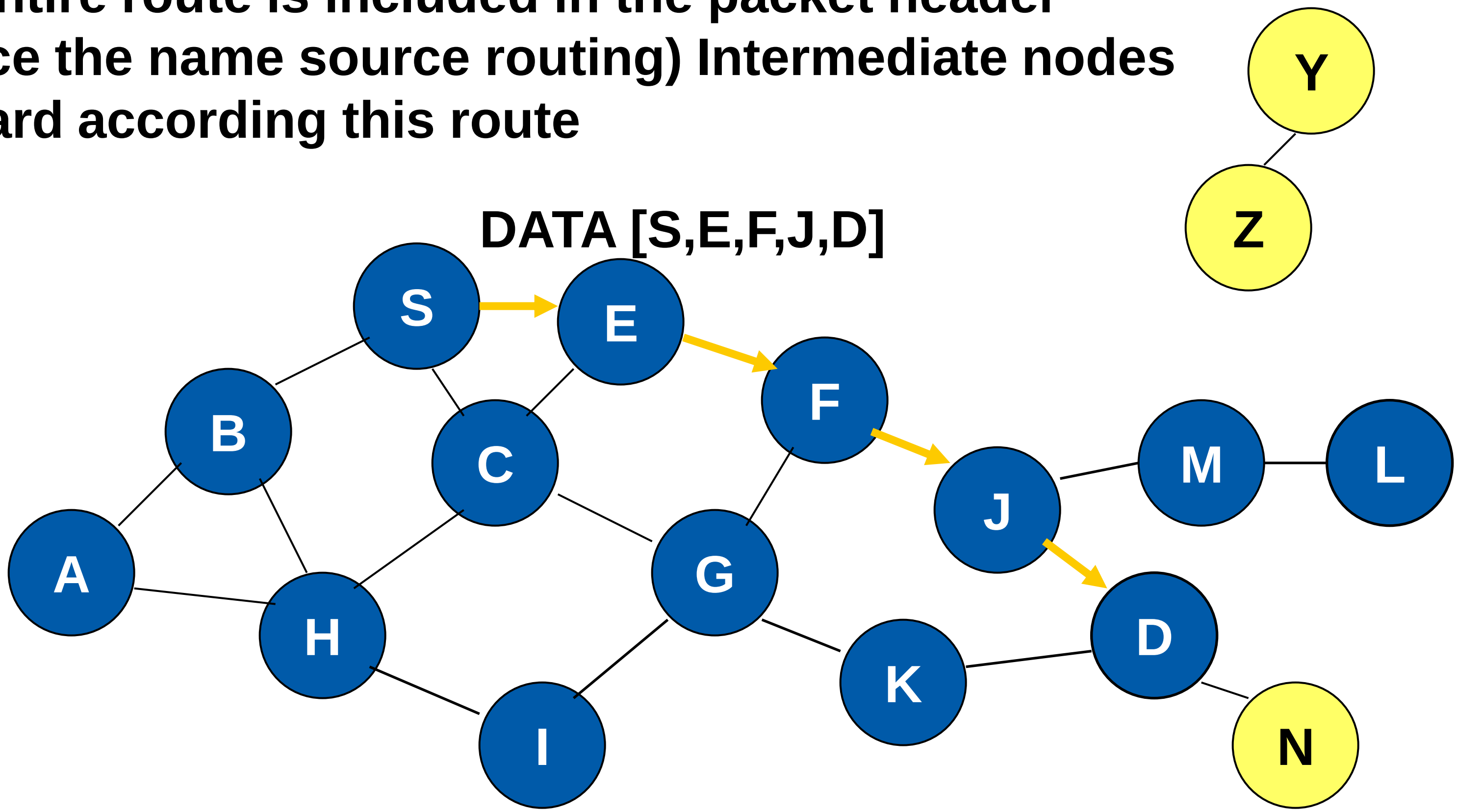
Node S on receiving RREP, caches the route included in the RREP




Represents RREP control message

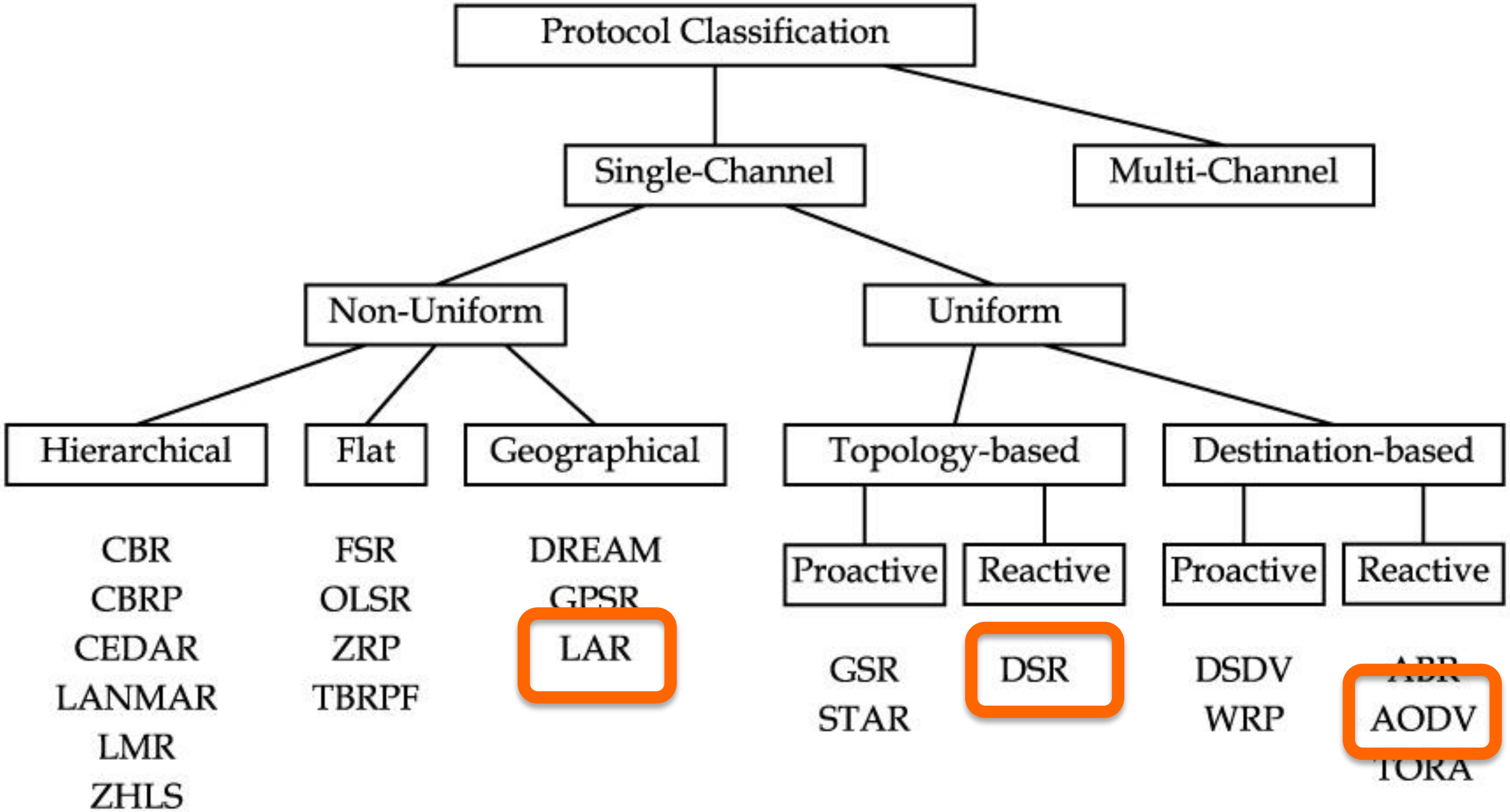
# Data Delivery in DSR

When node S sends a data packet to D,
the entire route is included in the packet header (hence the name source routing) Intermediate nodes forward according this route




Packet header size grows with route length

# Taxonomy of Routing Protocols




**above mentioned protocols are only a selection – the ones which will move forward to Experimental RFC (within IETF) will be highlighted**

## Routing: basic principles

- Reactive routing protocol
- All nodes are treated equal
- Based on distance vector principle

## Routing: some Details

- Route discovery cycle for route finding
  - Flooded / Broadcast Route Request (RREQ)
  - Unicast Route Reply (RREP) along reverse path of RREQ
  - Unicast Route Error (RERR)

## Some characteristics

- No overhead on data packets
- Loop freedom is achieved through sequence numbers
  - also solves “count to infinity” problem

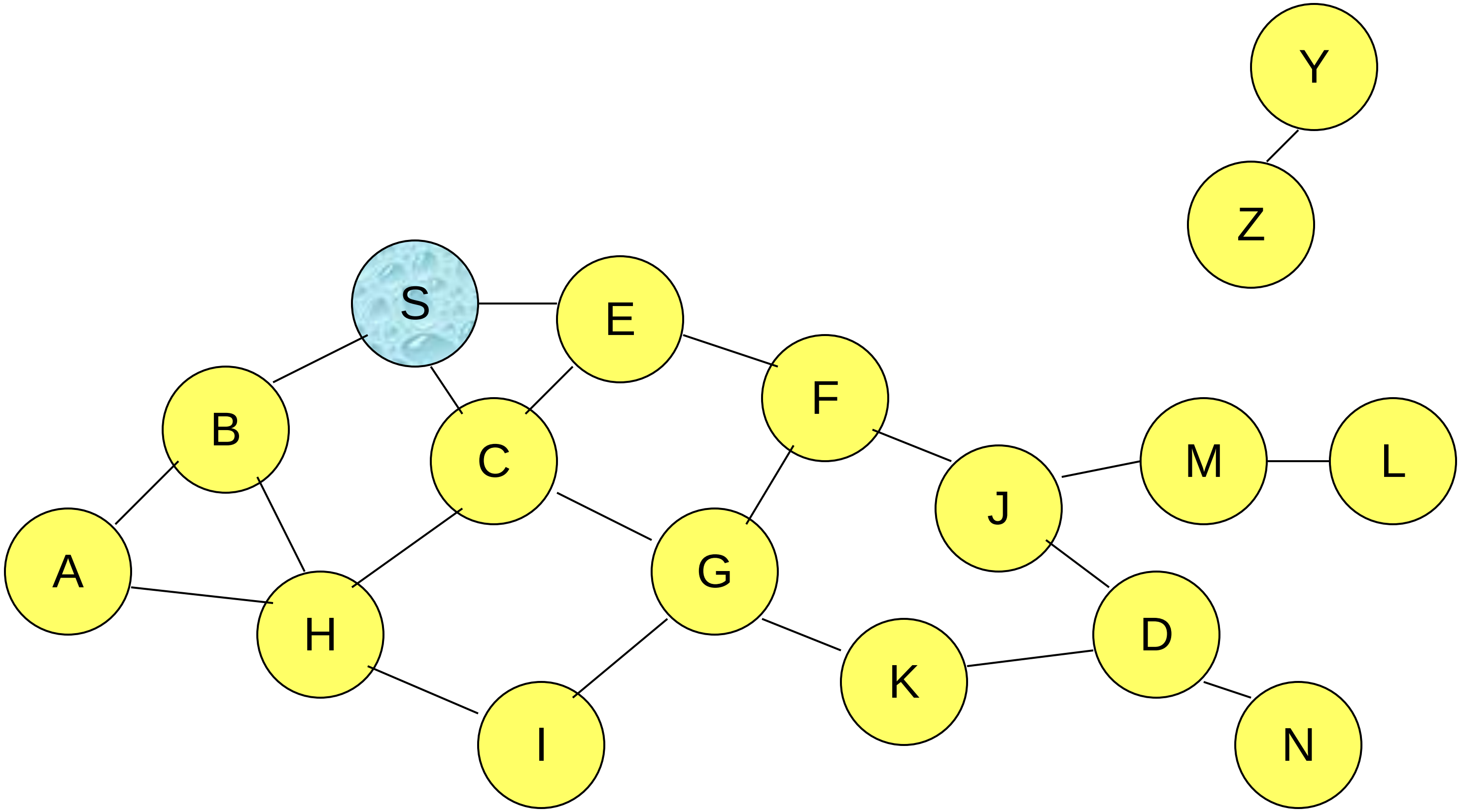
# AODV – Route Discovery – Route Request

## Route discovery

- Broadcast flood acquisition using Route Request (RREQ)
- A RREQ must never be broadcast more than once by any node

- Nodes sets up a reverse path pointing towards the source
- Route Reply (RREP) propagation

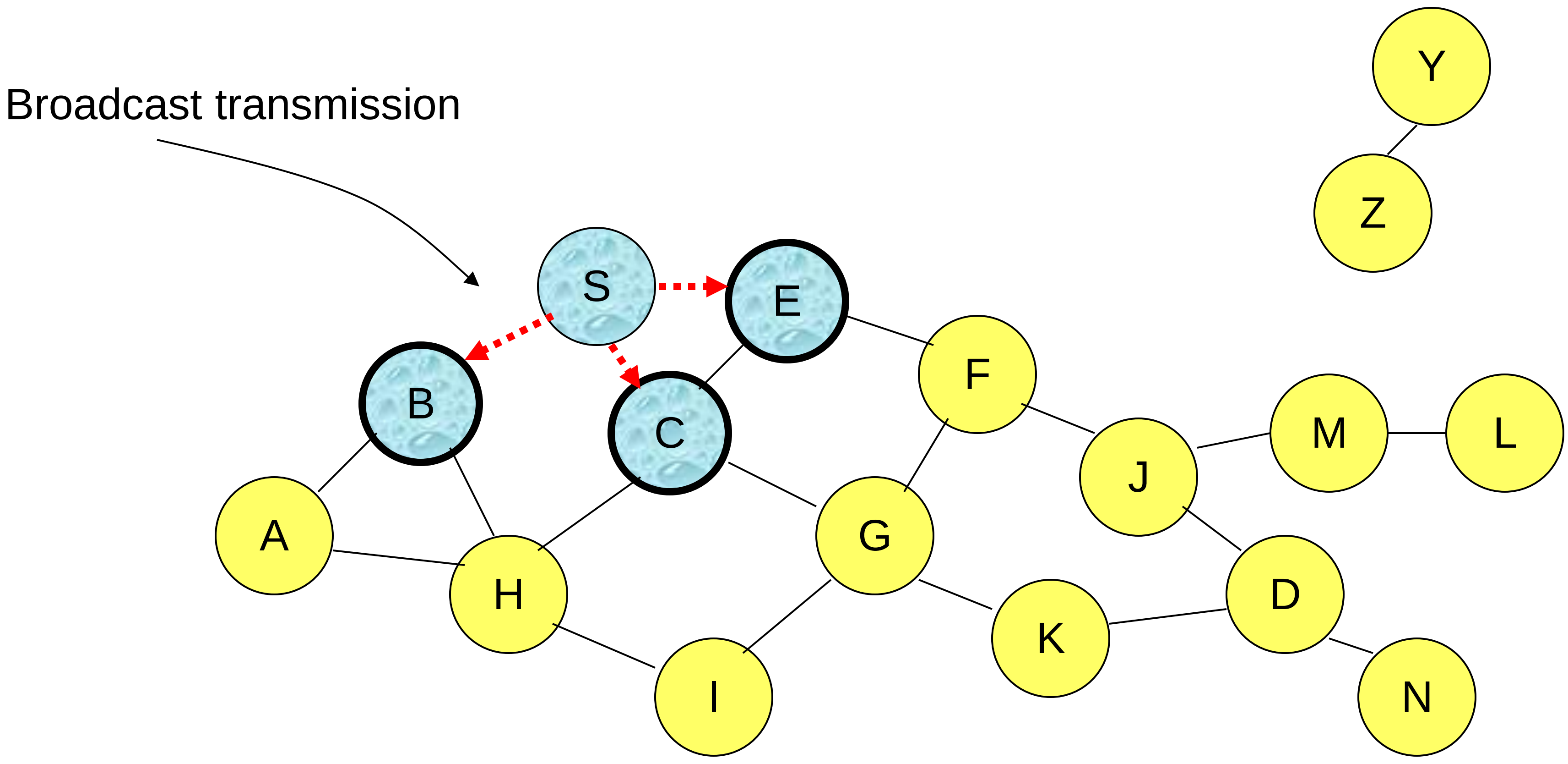
# Route Requests in AODV




Represents a node that has received RREQ for D from S

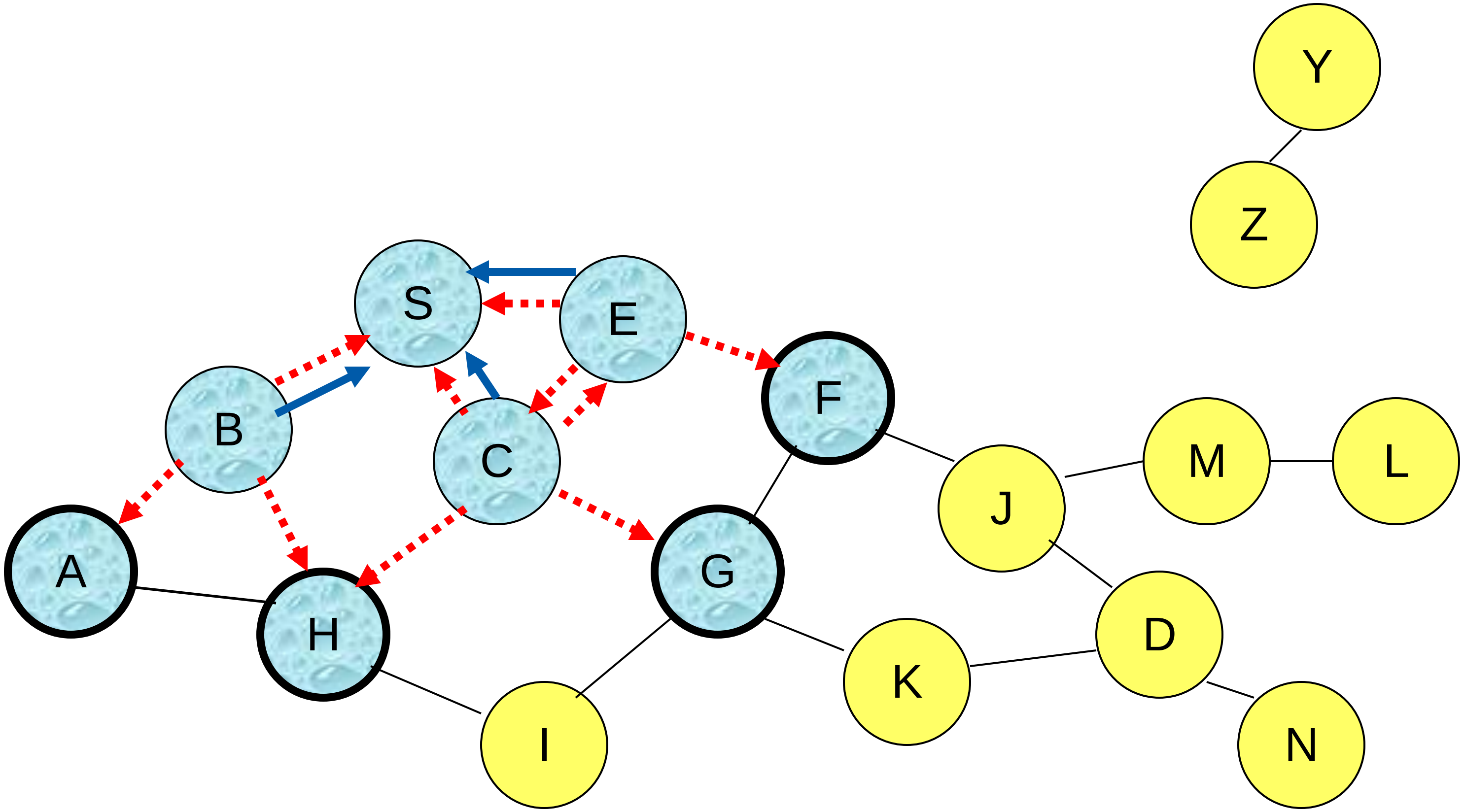
**Content of slides provided from Nitin H. Vaidya**
**University of Illinois at Urbana-Champaign**

# Route Requests in AODV



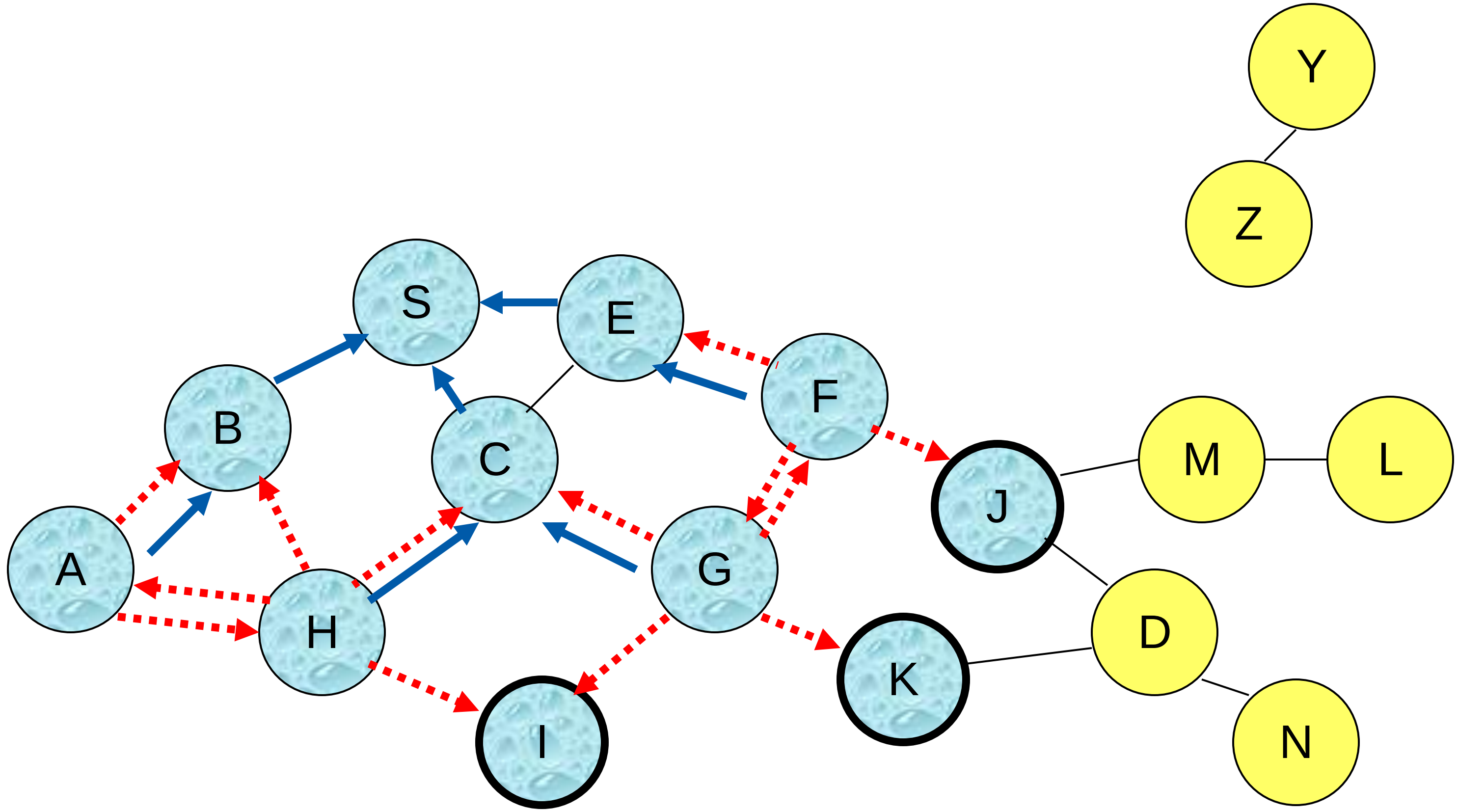

Represents transmission of RREQ

# Route Requests in AODV



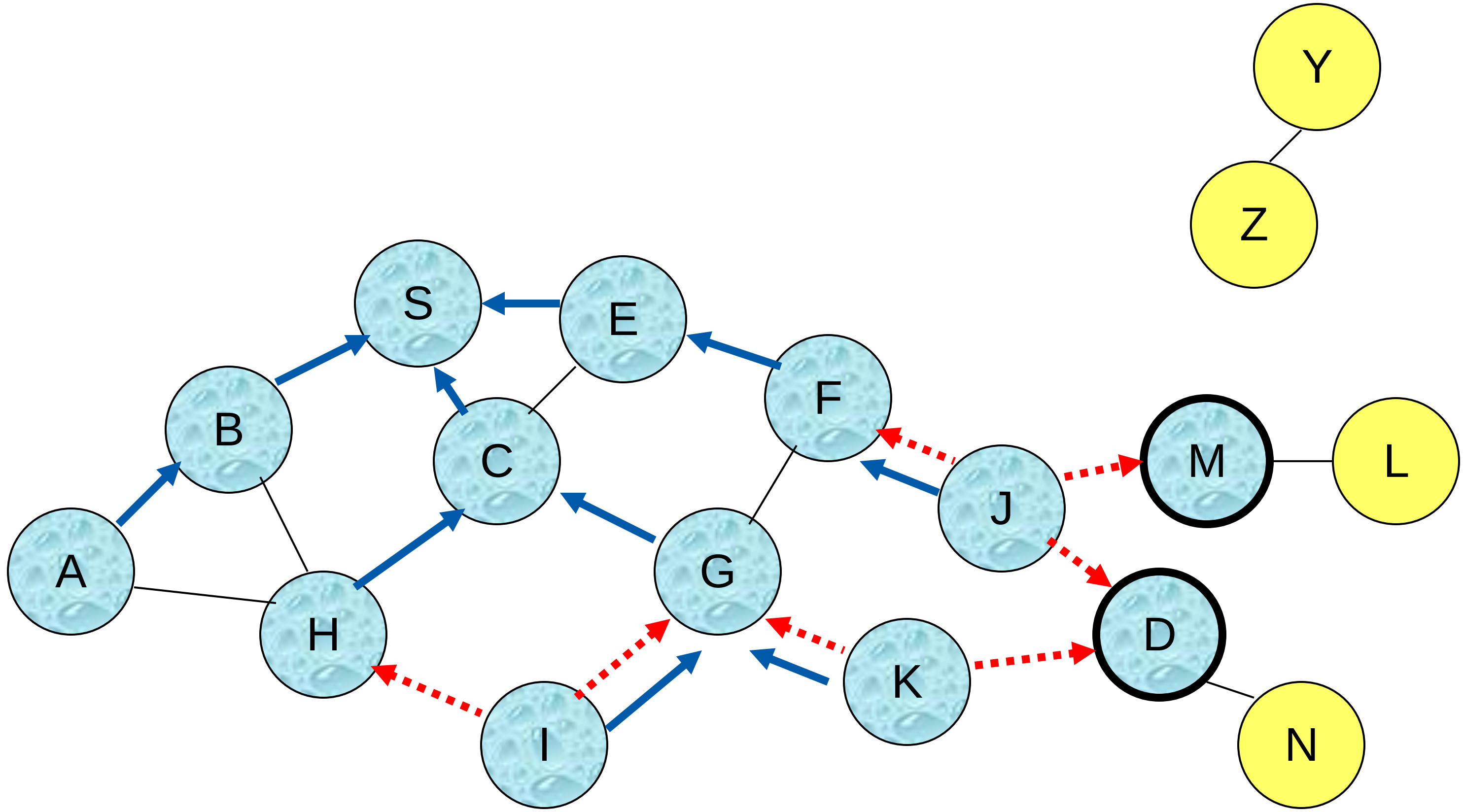

Represents links on Reverse Path

# Reverse Path Setup in AODV

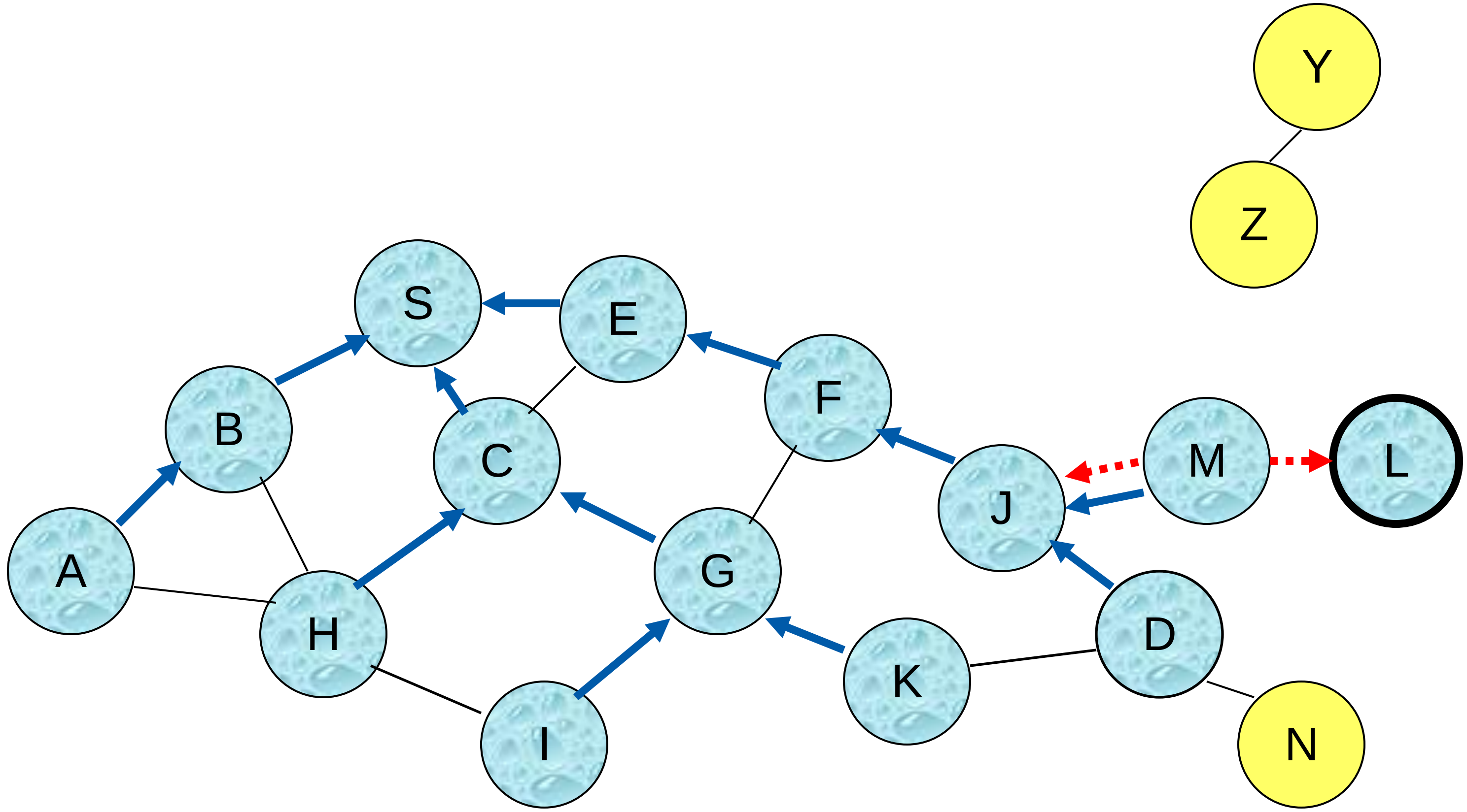



- Node C receives RREQ from G and H, but does not forward it again, because node C has already forwarded RREQ once

# Reverse Path Setup in AODV

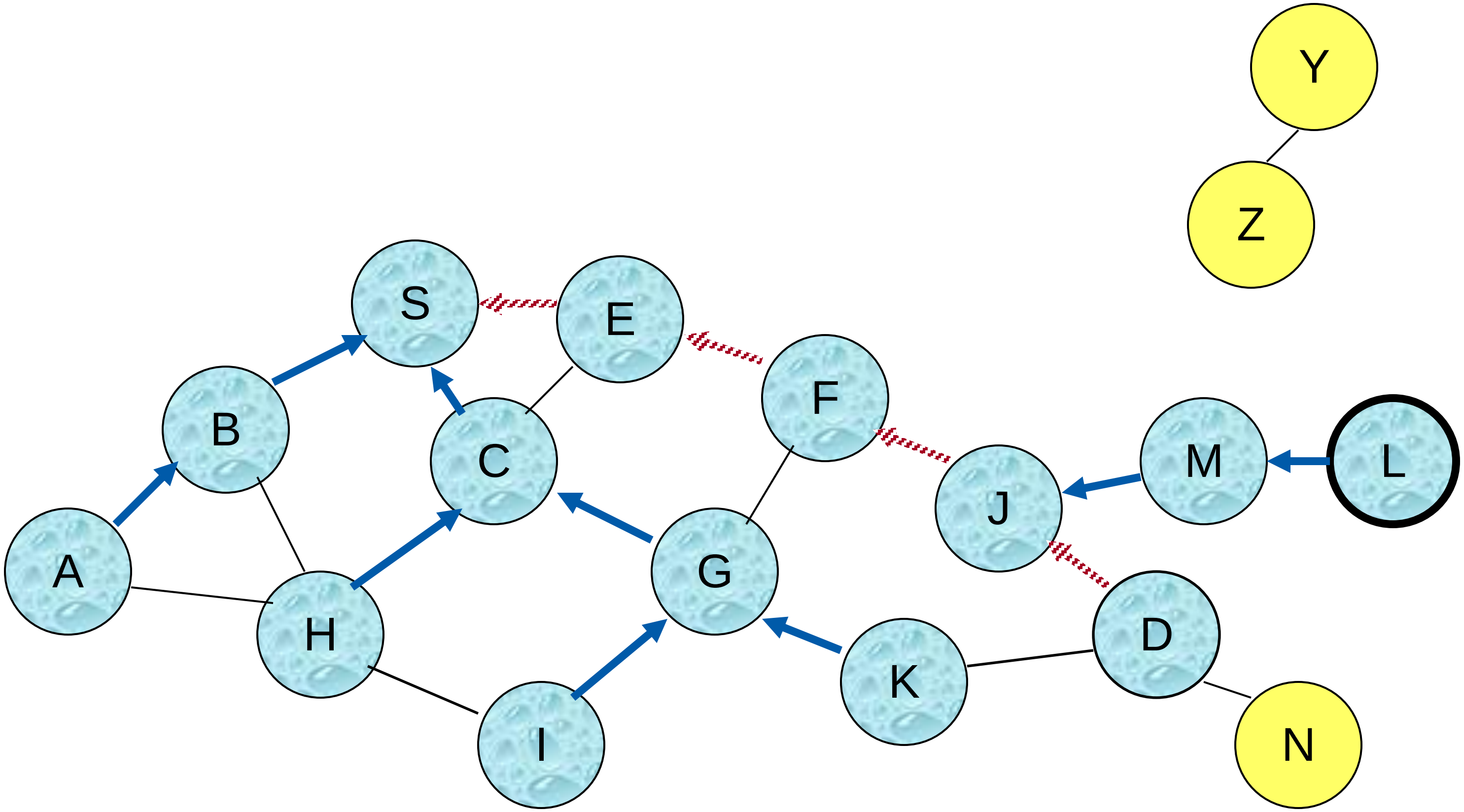


# Reverse Path Setup in AODV




- 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

# Route Reply in AODV

**An intermediate node (not the destination) may also send**

- A Route Reply (RREP) provided that it knows a more recent path than the one previously known to sender S

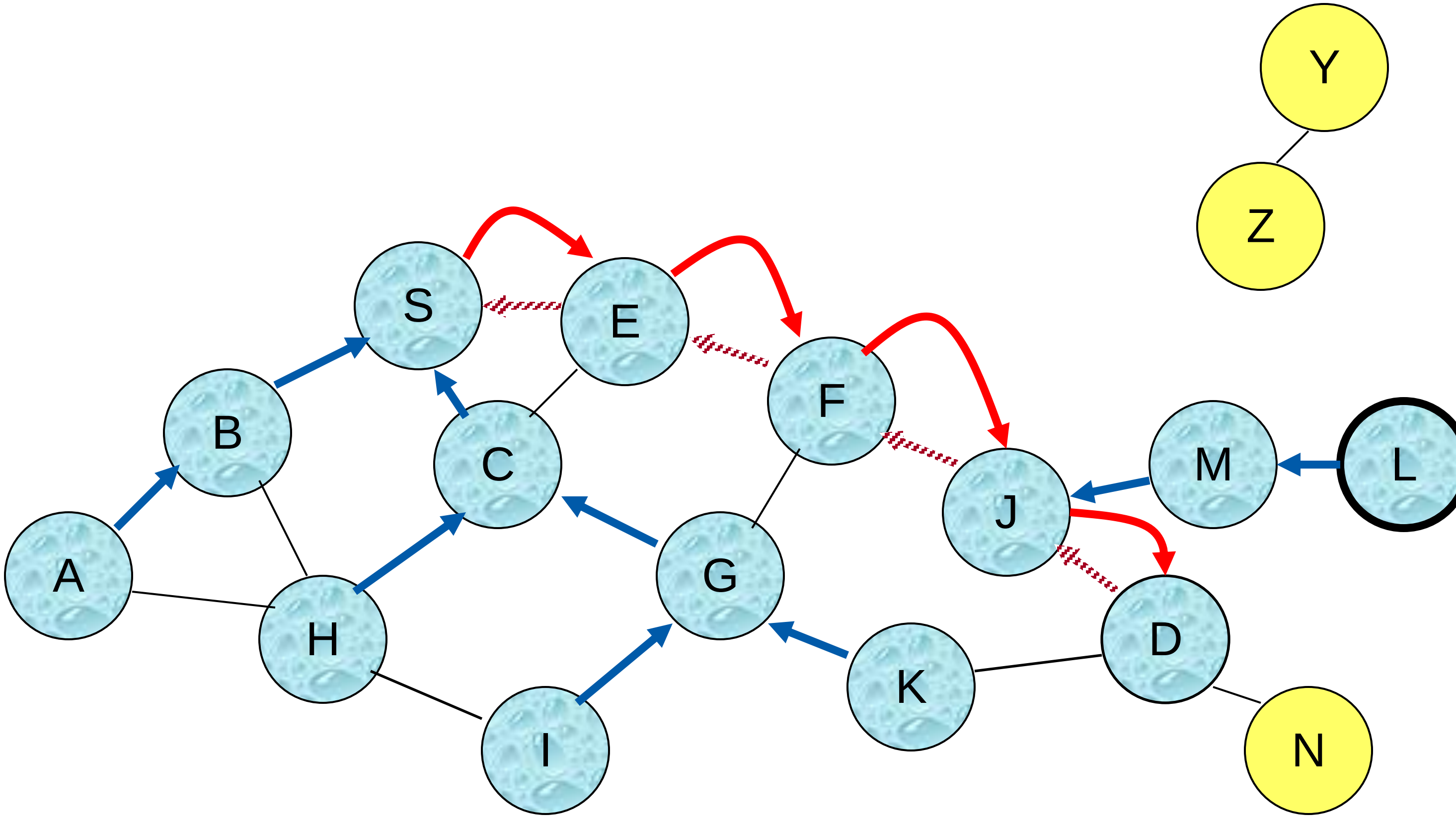
**To determine whether the path known to an intermediate node is more recent,**

- Destination sequence numbers are used

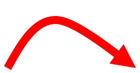
**The likelihood that an intermediate node will send a Route Reply when using AODV not as high as DSR**

- A new Route Request by node S for a destination is assigned a higher destination sequence number.
- An intermediate node which knows a route, but with a smaller sequence number, cannot send Route Reply

# Forward Path Setup in AODV

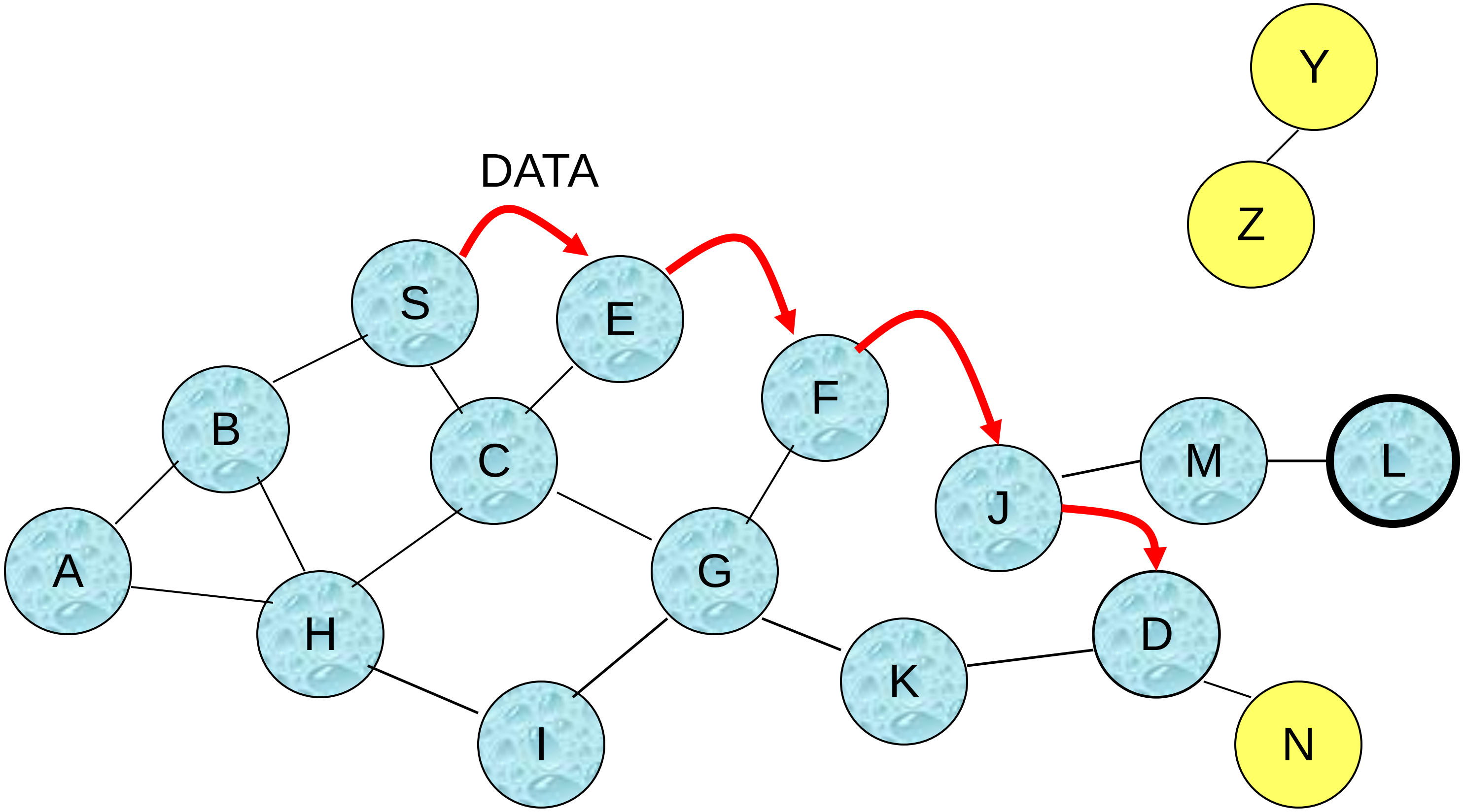



Forward links are setup when RREP travels along the reverse path

 Represents a link on the forward path

46

# Data Delivery in AODV




Routing table entries used to forward data packet.

Route is *not* included in packet header.

47

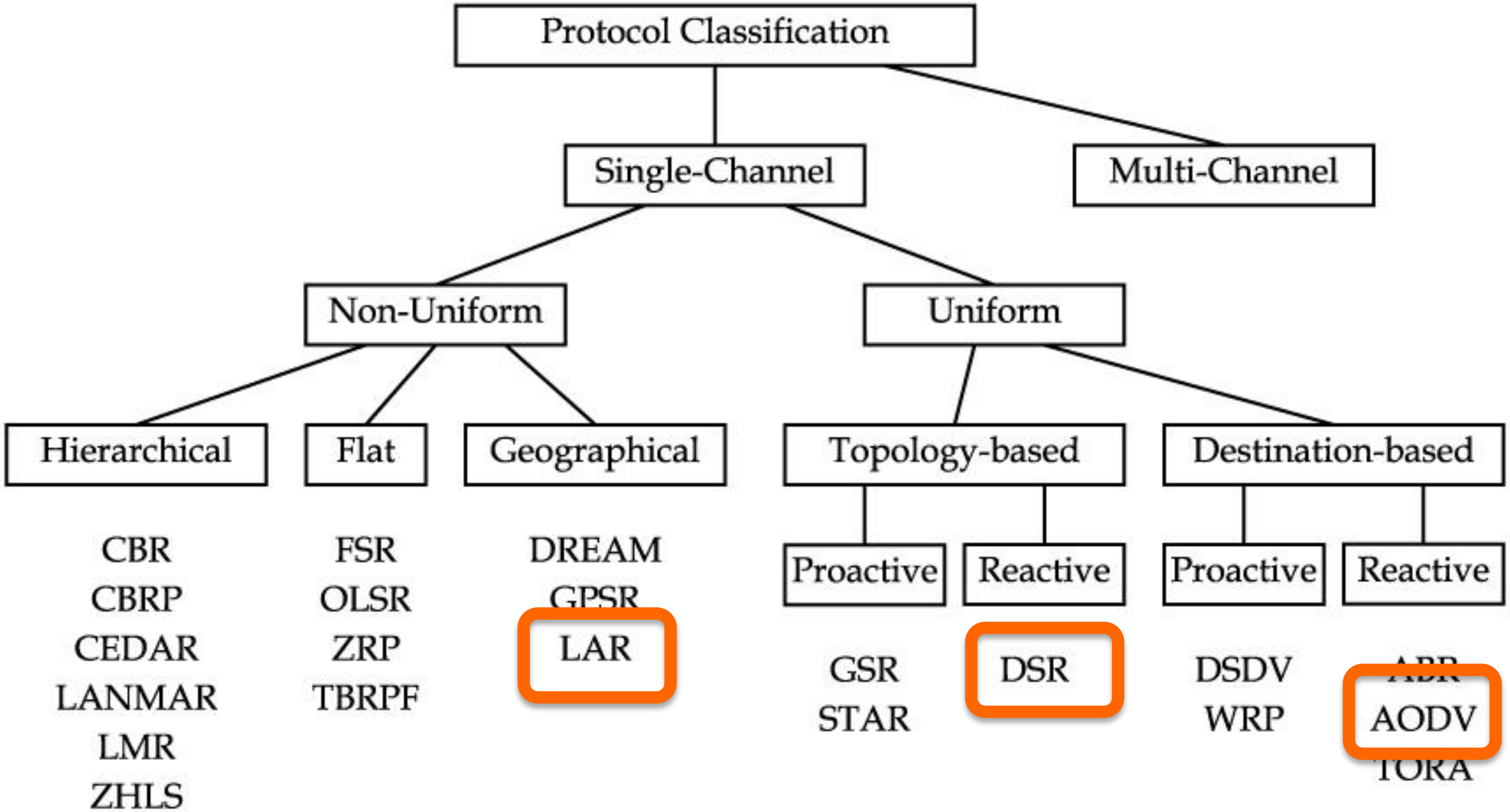
# AODV – Route Maintenance & Link Errors

## Timers to keep route alive

## Destination Sequence numbers to determine fresh routes

## Link failure reporting / repairing routes

# Taxonomy of Routing Protocols




**above mentioned protocols are only a selection – the ones which will move forward to Experimental RFC (within IETF) will be highlighted**

**Based on flooding**

**Exploits location information to limit scope of flooding for route request**

- Location information may be obtained using GPS

**EXPECTED ZONE is determined as a region that is expected to hold the current location of the destination node (D)**

- Expected region determined based on potentially old location information, and knowledge of the destination's speed

**Route requests limited to a REQUESTED ZONE that contains**

- the Expected Zone and
- location of the sender node (S)

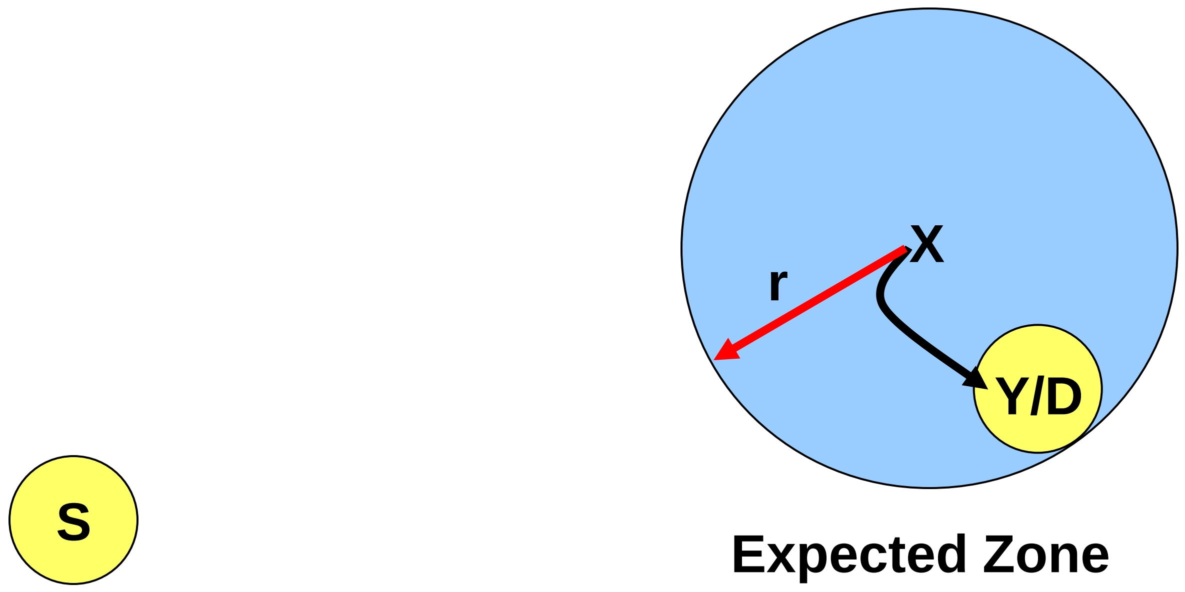
# Expected Zone in LAR

S = Source node, D = Destination node

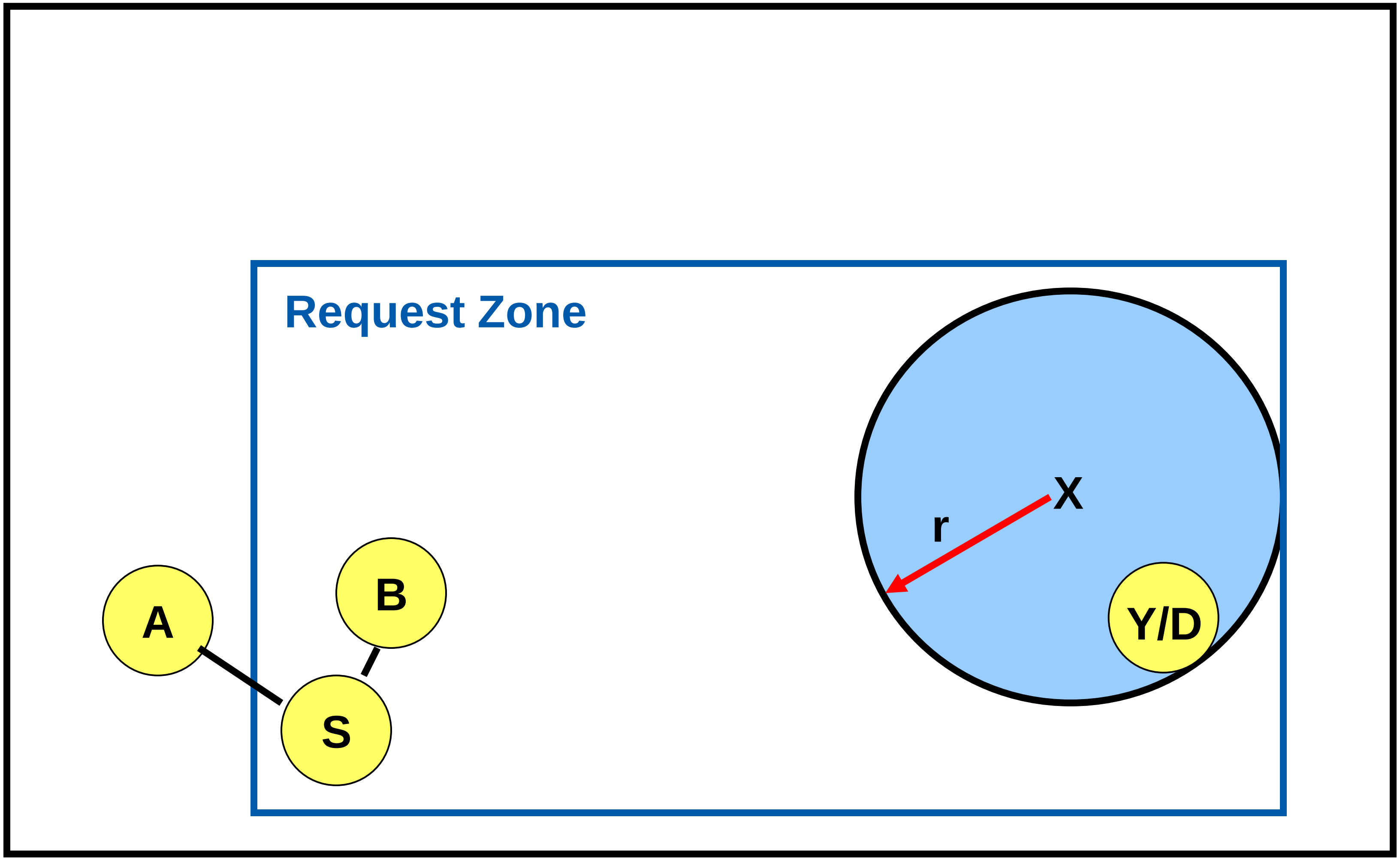
X = last known location of node D, at time t0

Y = location of node D at current time t1, unknown to sender S

r = (t1 - t0) * estimate of D's speed



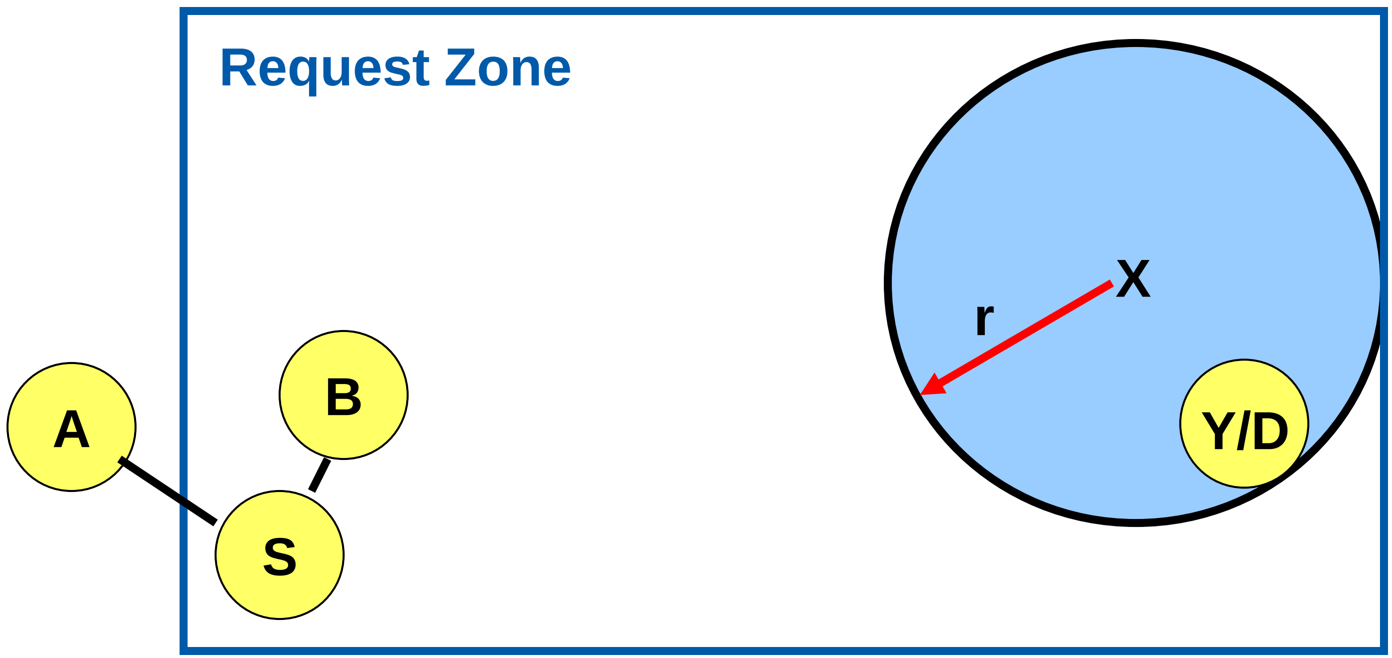
# Request Zone in LAR



# Operation of LAR (1)

## Only nodes within the request zone forward route requests

- Node A does not forward RREQ,
  but node B does
- Request zone explicitly specified in the route request
- Each node must know its physical location
  to determine whether it is within the request zone



## Operation of LAR (1)

**Only nodes within the request zone forward route requests**

**If route discovery using the smaller request zone fails to find a route, the sender initiates another route discovery (after a timeout) using a larger request zone**

- the larger request zone may be the entire network

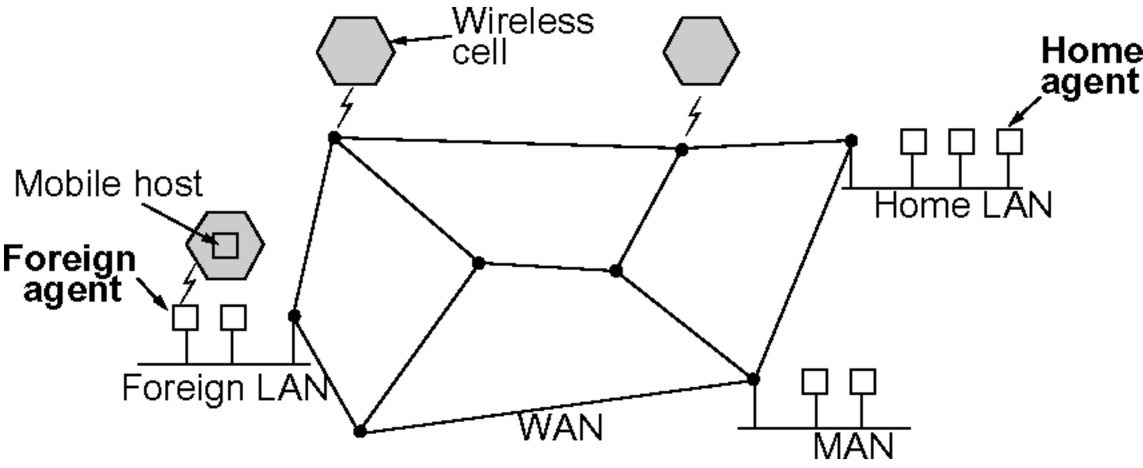
**Rest of route discovery protocol similar to DSR**

## Recall: Two aspects of mobility

- User mobility:
  - users communicate (wireless) “anytime, anywhere, with anyone”
- Device portability:
  - devices can be connected anytime, anywhere to the network

| Wireless | vs. mobile | Examples |
|---|---|---|
| ✘ | ✘ | stationary computer |
| ✘ | ✓ | notebook in hotel |
| ✓ | ✘ | wireless LANs in historic buildings |
| ✓ | ✓ | Personal Digital Assistant |

# Routing with Mobility

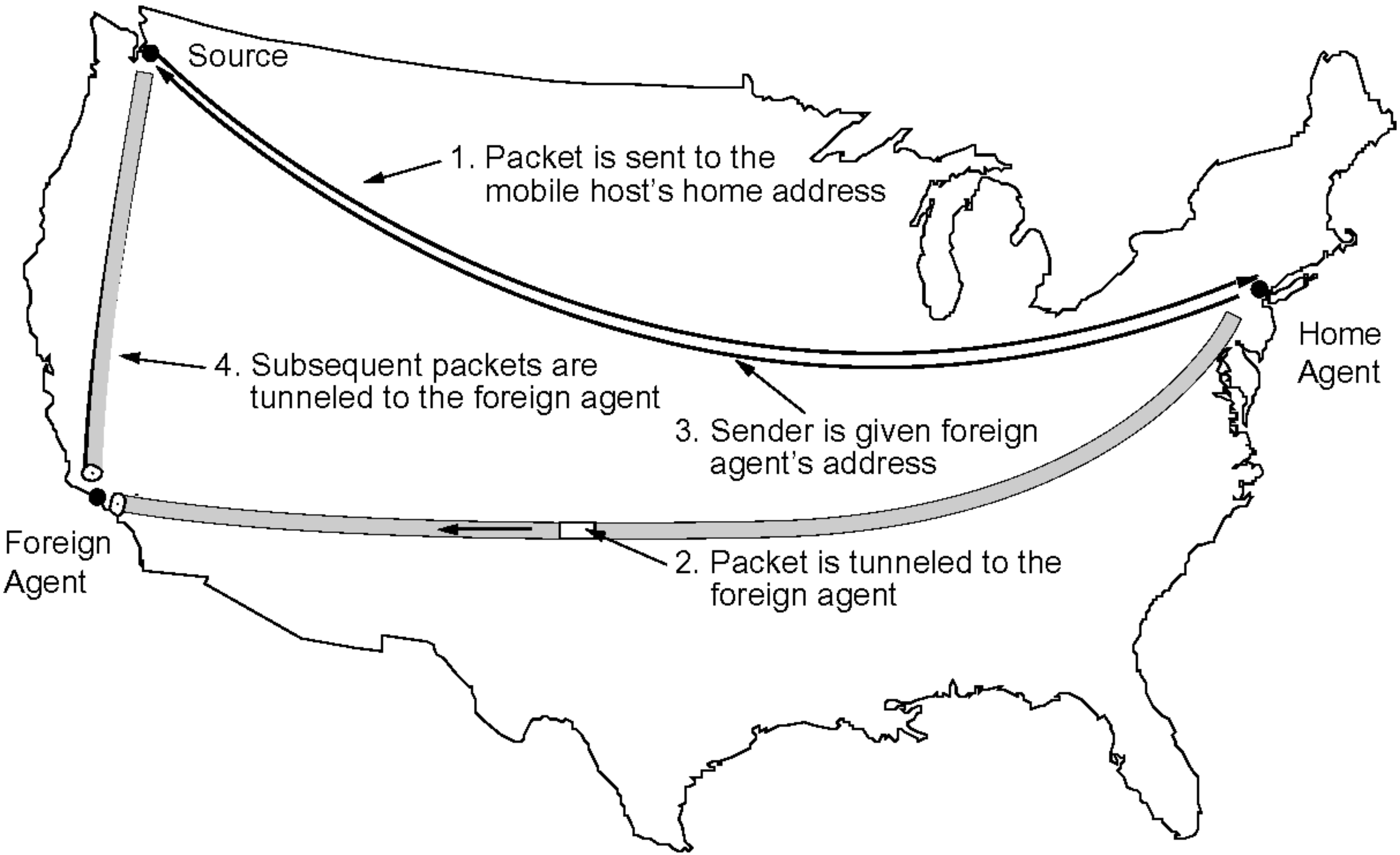



## Principle

- End system identified by its local home address
- No modifications in existing IS
- I.e.,
  - Home-Agent: stationary address
  - Foreign Agent: knows mobile end system

# Routing with Mobility

## Tunneling and Rerouting Procedures



# 5 Further Issues in Mobile Networking

## Interesting problems spanning multiple layers

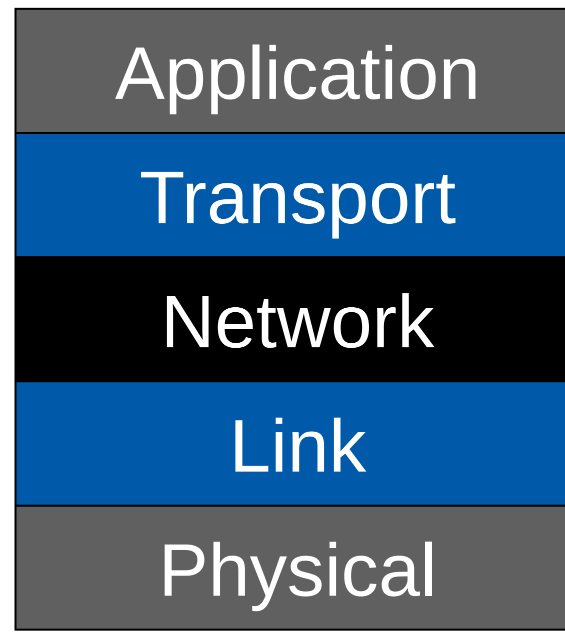
- Security, QoS, Scalability, Heterogeneity, Adaptation, Dependability

## Application Layer

- Feasibility of Client-Server paradigm (DNS, Certificate Authorities)
- Discovery of Services, where to place services, service awareness

## Transport Layer

- Esp. TCP-performance




## Network Layer

- Adaptation of routing protocols, multicast routing
- Autoconfiguration of IP-Addresses
- Deal with routing misbehavior

## Link Layer

- Medium Access Control / Scheduling
- Multiple Channels

## Physical Layer

- Adaptive Modulation, Smart Antennas
- Power Control (to maximize power-usage / to minimize interference)

# Clustering of Mobile Networks

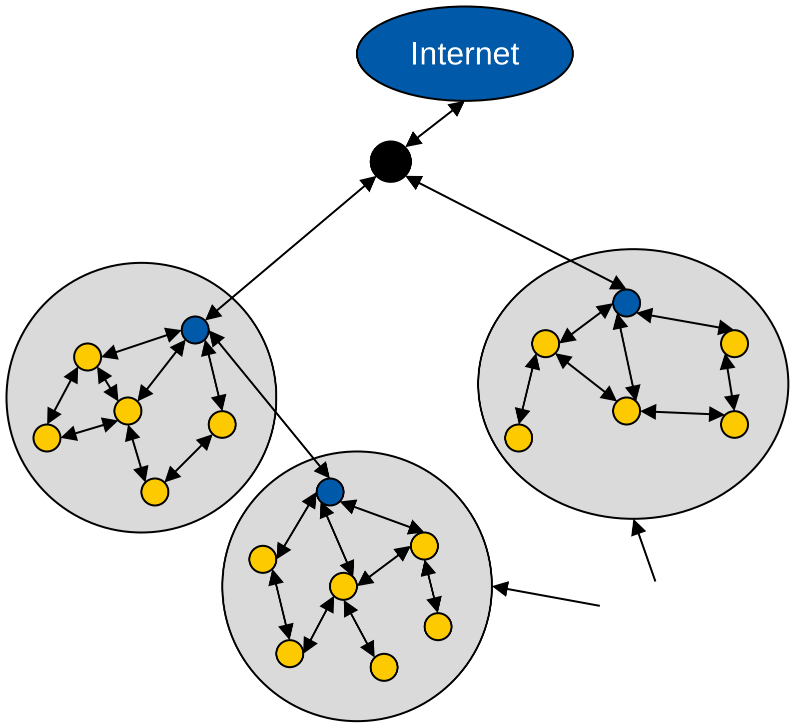
## Hierarchical routing applies also to mobile networks

## Divide nodes into clusters based on distance

- Nearby nodes for a cluster

## Basic idea:

- Use proactive routing within („intra“-)cluster
- Use reactive routing „inter“-cluster




## Small cluster:

- Possible to know all nodes
- Proactive routing works

## Many clusters:

- Mostly no communication
- Better to use reactive routing