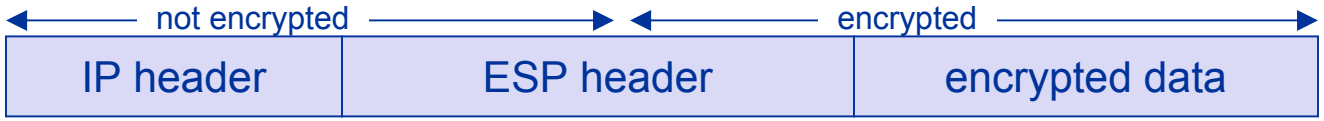
IP security architecture I

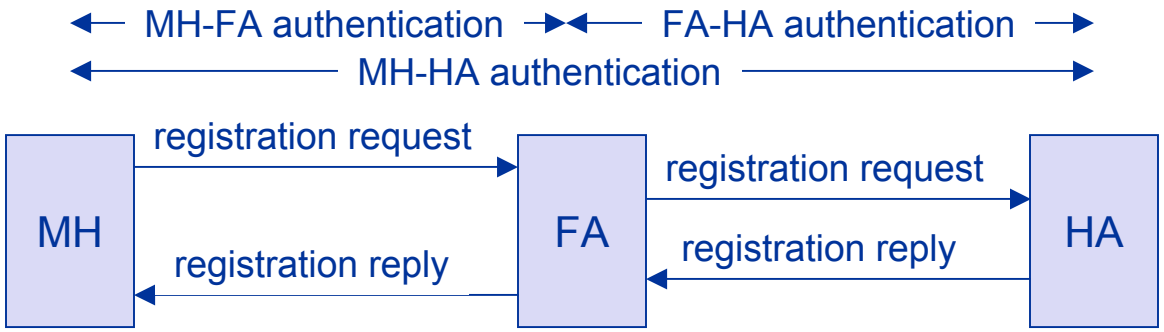
- Two or more partners have to negotiate security mechanisms to setup a security association
  - typically, all partners choose the same parameters and mechanisms
- Two headers have been defined for securing IP packets:
  - Authentication-Header
    - guarantees integrity and authenticity of IP packets
    - if asymmetric encryption schemes are used, non-repudiation can also be guaranteed

  - Encapsulation Security Payload
    - protects confidentiality between communication partners



IP security architecture II

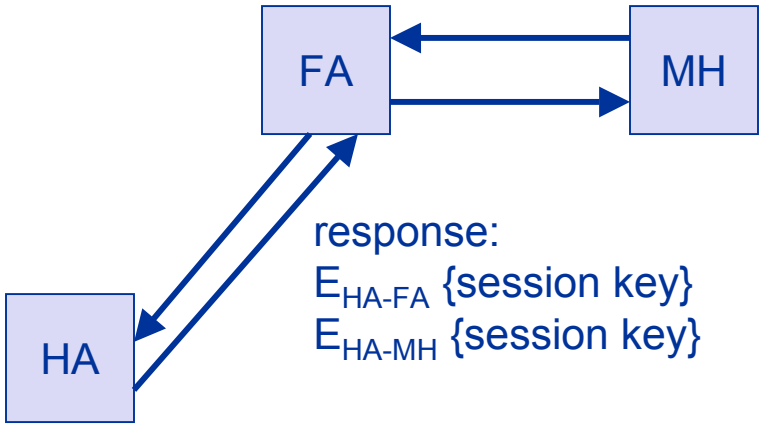
- Mobile Security Association for registrations
  - parameters for the mobile host (MH), home agent (HA), and foreign agent (FA)
- Extensions of the IP security architecture
  - extended authentication of registration



  - prevention of replays of registrations
    - time stamps: 32 bit time stamps + 32 bit random number
    - nonces: 32 bit random number (MH) + 32 bit random number (HA)

Key distribution

- Home agent distributes session keys



- foreign agent has a security association with the home agent
- mobile host registers a new binding at the home agent
- home agent answers with a new session key for foreign agent and mobile node

IP Micro-mobility support

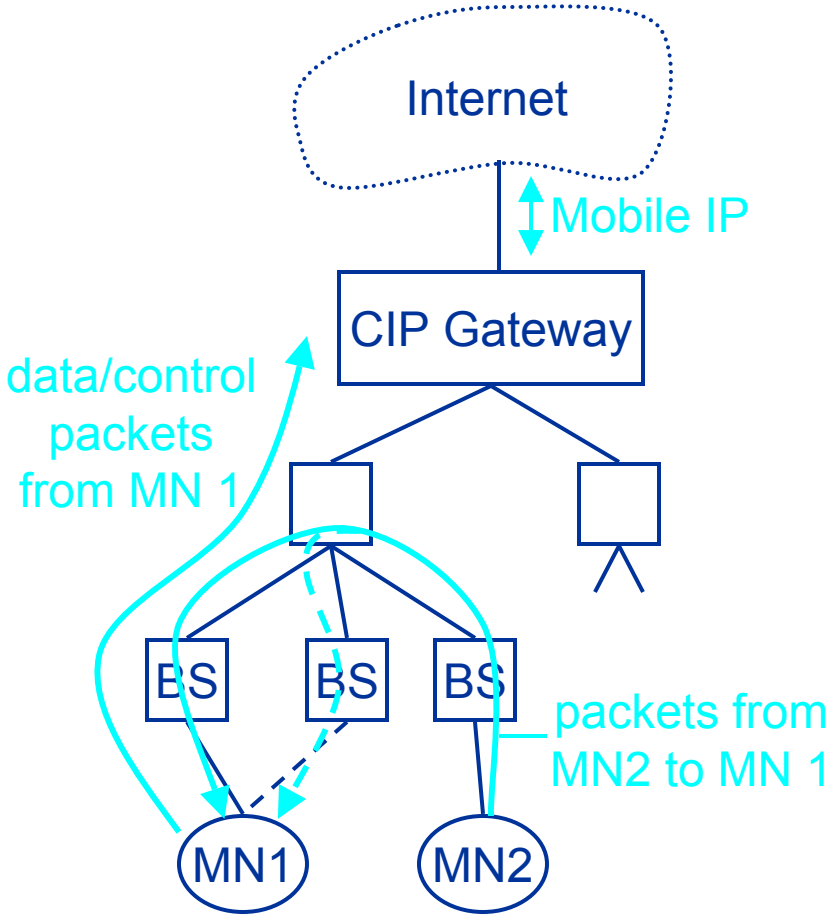
- Micro-mobility support:
  - Efficient local handover inside a foreign domain without involving a home agent
  - Reduces control traffic on backbone
  - Especially needed in case of route optimization

- Example approaches (research, not products):
  - Cellular IP
  - HAWAII
  - Hierarchical Mobile IP (HMIP)

- Important criteria:
  Security Efficiency, Scalability, Transparency, Manageability

Cellular IP

- Operation:
  - "CIP Nodes" maintain routing entries (soft state) for MNs
  - Multiple entries possible
  - Routing entries updated based on packets sent by MN
- CIP Gateway:
  - Mobile IP tunnel endpoint
  - Initial registration processing
- Security provisions:
  - all CIP Nodes share "network key"
  - MN key: MD5(net key, IP addr)
  - MN gets key upon registration



Cellular IP: Security

- Advantages:
  - Initial registration involves authentication of MNs and is processed centrally by CIP Gateway
  - All control messages by MN's are authenticated
  - Replay-protection (using timestamps)

- Potential problems:
  - MN's can directly influence routing entries
  - Network key known to many entities (increases risk of compromise)
  - No re-keying mechanisms for network key
  - No choice of algorithm (always MD5, prefix+suffix mode)
  - Proprietary mechanisms (not, e.g., IPSec AH)

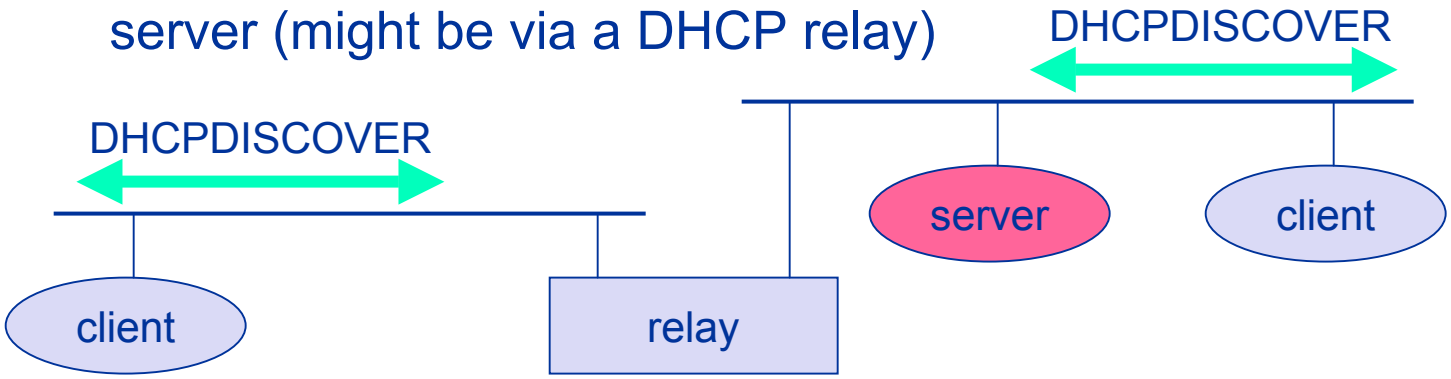
Cellular IP: Other issues

- Advantages:
  - Simple and elegant architecture
  - Mostly self-configuring (little management needed)
  - Integration with firewalls / private address support possible

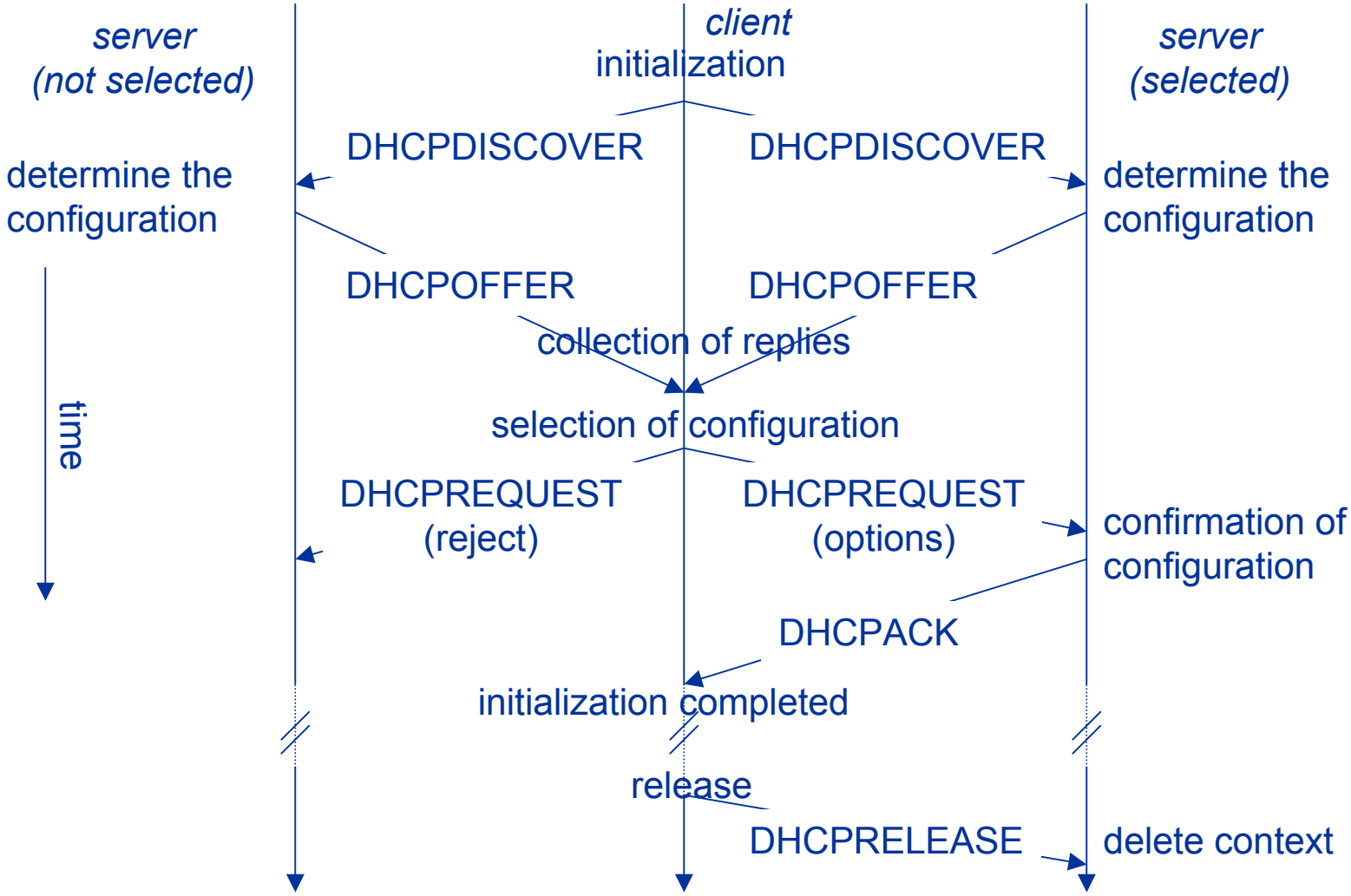
- Potential problems:
  - Not transparent to MN's (additional control messages)
  - Public-key encryption of MN keys may be a problem for resource-constrained MN's
  - Multiple-path forwarding may cause inefficient use of available bandwidth

DHCP: Dynamic Host Configuration Protocol

- Application
  - simplification of installation and maintenance of networked computers
  - supplies systems with all necessary information, such as IP address, DNS server address, domain name, subnet mask, default router etc.
  - enables automatic integration of systems into an Intranet or the Internet, can be used to acquire a COA for Mobile IP
- Client/Server-Model
  - the client sends via a MAC broadcast a request to the DHCP server (might be via a DHCP relay)



DHCP - protocol mechanisms

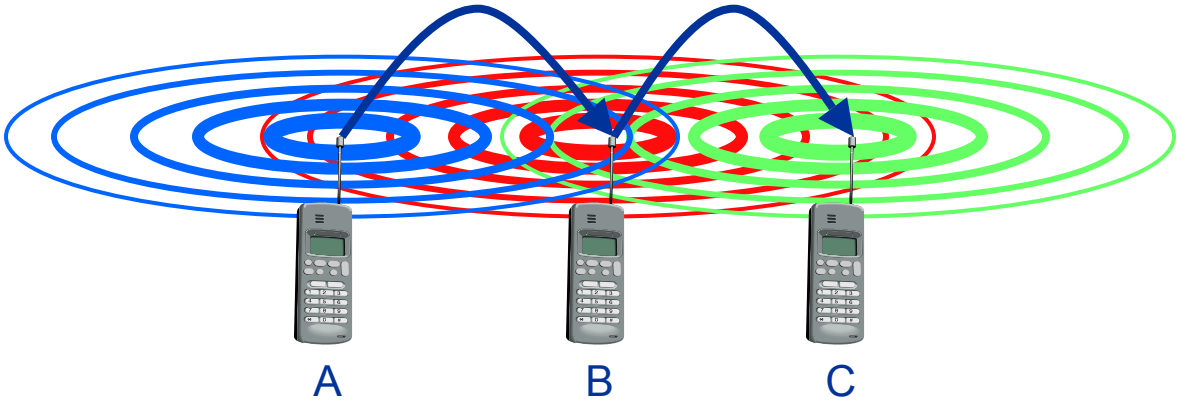


DHCP characteristics

- Server
  - several servers can be configured for DHCP, coordination not yet standardized (i.e., manual configuration)
- Renewal of configurations
  - IP addresses have to be requested periodically, simplified protocol
- Options
  - available for routers, subnet mask, NTP (network time protocol) timeserver, SLP (service location protocol) directory, DNS (domain name system)

Mobile ad hoc networks

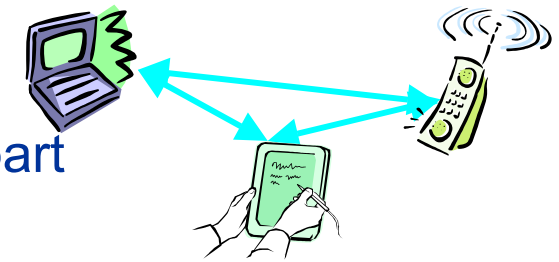
- Standard Mobile IP needs an infrastructure
  - Home Agent/Foreign Agent in the fixed network
  - DNS, routing etc. are not designed for mobility
- Sometimes there is no infrastructure!
  - remote areas, ad-hoc meetings, disaster areas
  - cost can also be an argument against an infrastructure!
- Main topic: routing
  - no default router available
  - every node should be able to forward



Solution: Wireless ad-hoc networks

- Network without infrastructure
  - Use components of participants for networking

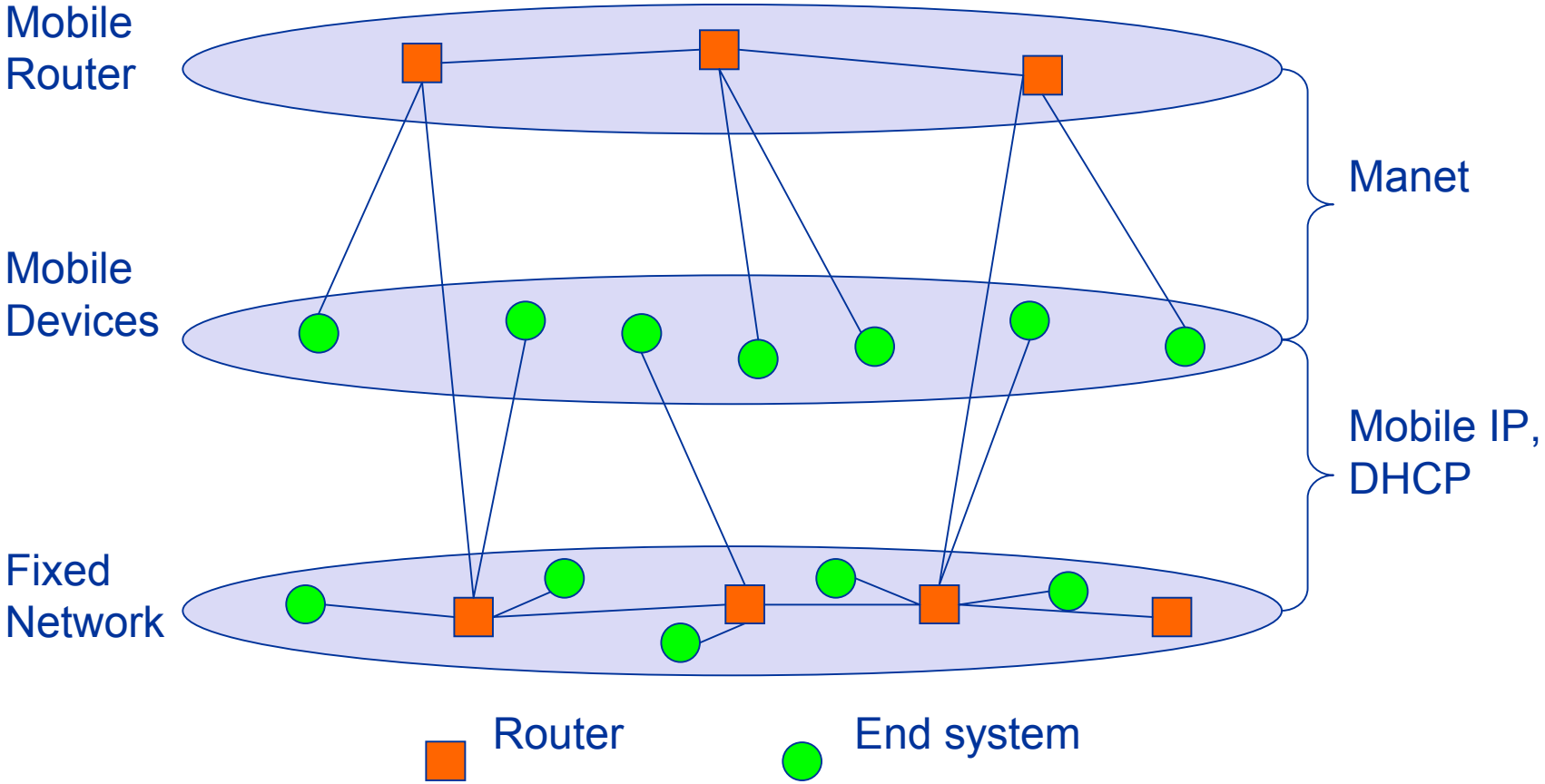
- Examples
  - Single-hop: All partners max. one hop apart
    - Bluetooth piconet, PDAs in a room, gaming devices…



  - Multi-hop: Cover larger distances, circumvent obstacles
    - Bluetooth scatternet, TETRA police network, car-to-car networks…

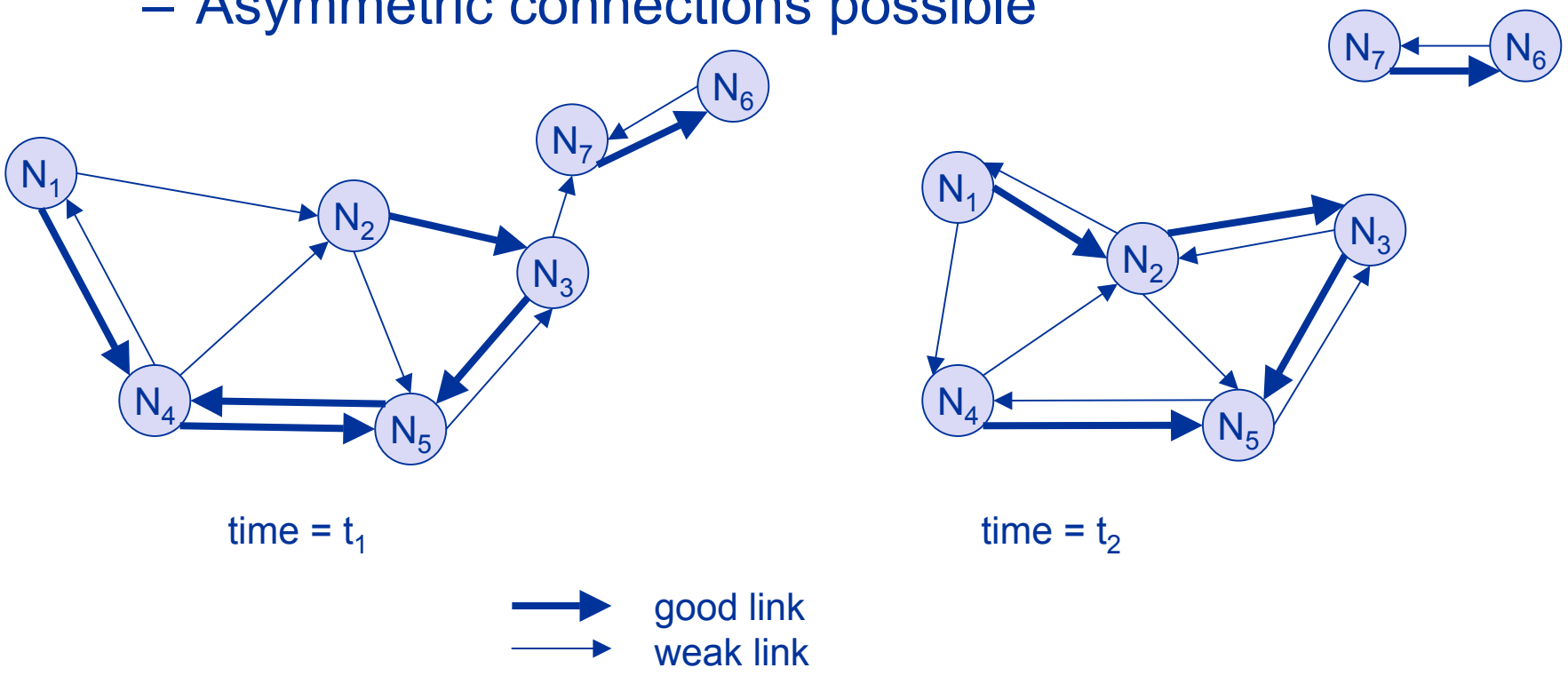
- Internet: MANET (Mobile Ad-hoc Networking) group

Manet: Mobile Ad-hoc Networking



Problem No. 1: Routing

- Highly dynamic network topology
  - Device mobility plus varying channel quality
  - Separation and merging of networks possible
  - Asymmetric connections possible



Traditional routing algorithms

- Distance Vector
  - periodic exchange of messages with all physical neighbors that contain information about who can be reached at what distance
  - selection of the shortest path if several paths available
- Link State
  - periodic notification of all routers about the current state of all physical links
  - router get a complete picture of the network
- Example
  - ARPA packet radio network (1973), DV-Routing
  - every 7.5s exchange of routing tables including link quality
  - updating of tables also by reception of packets
  - routing problems solved with limited flooding

Routing in ad-hoc networks

- THE big topic in many research projects
  - Far more than 50 different proposals exist
  - The most simplest one: Flooding!

- Reasons
  - Classical approaches from fixed networks fail
    - Very slow convergence, large overhead
  - High dynamicity, low bandwidth, low computing power

- Metrics for routing
  - Minimal
    - Number of nodes, loss rate, delay, congestion, interference …
  - Maximal
    - Stability of the logical network, battery run-time, time of connectivity …

Problems of traditional routing algorithms

- Dynamic nature of the topology
  - frequent changes of connections, connection quality, participants
- Limited performance of mobile systems
  - periodic updates of routing tables need energy without contributing to the transmission of user data, sleep modes difficult to realize
  - limited bandwidth of the system is reduced even more due to the exchange of routing information
  - links can be asymmetric, i.e., they can have a direction dependent transmission quality

DSDV (Destination Sequenced Distance Vector, historical)

- Early work
  - on demand version: AODV
- Expansion of distance vector routing
- Sequence numbers for all routing updates
  - assures in-order execution of all updates
  - avoids loops and inconsistencies
- Decrease of update frequency
  - store time between first and best announcement of a path
  - inhibit update if it seems to be unstable (based on the stored time values)

Dynamic source routing I

- Split routing into discovering a path and maintaining a path
- Discover a path
  - only if a path for sending packets to a certain destination is needed and no path is currently available
- Maintaining a path
  - only while the path is in use one has to make sure that it can be used continuously
- No periodic updates needed!

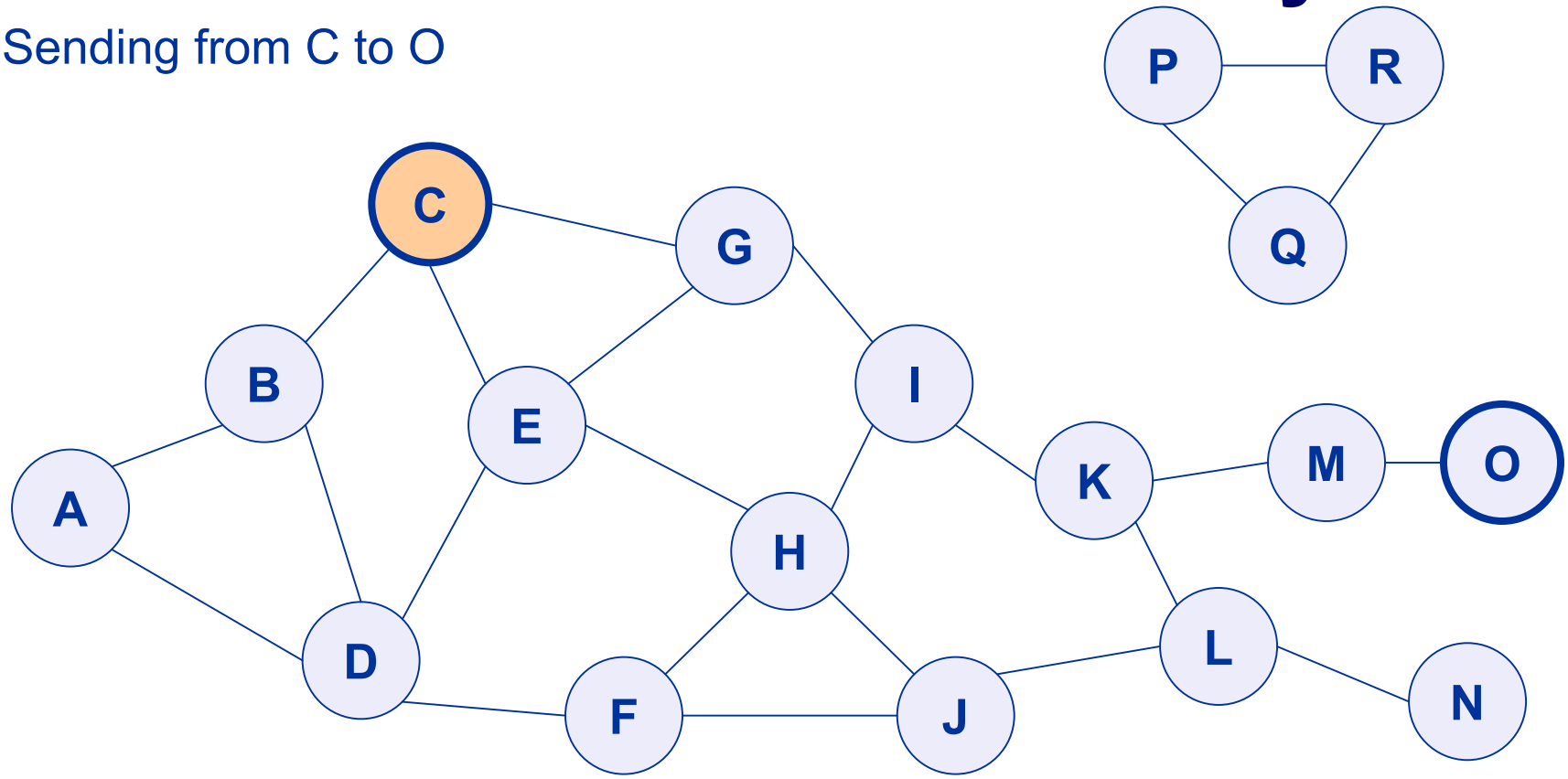
Dynamic source routing II

- Path discovery
  - broadcast a packet with destination address and unique ID
  - if a station receives a broadcast packet
    - if the station is the receiver (i.e., has the correct destination address) then return the packet to the sender (path was collected in the packet)
    - if the packet has already been received earlier (identified via ID) then discard the packet
    - otherwise, append own address and broadcast packet
  - sender receives packet with the current path (address list)

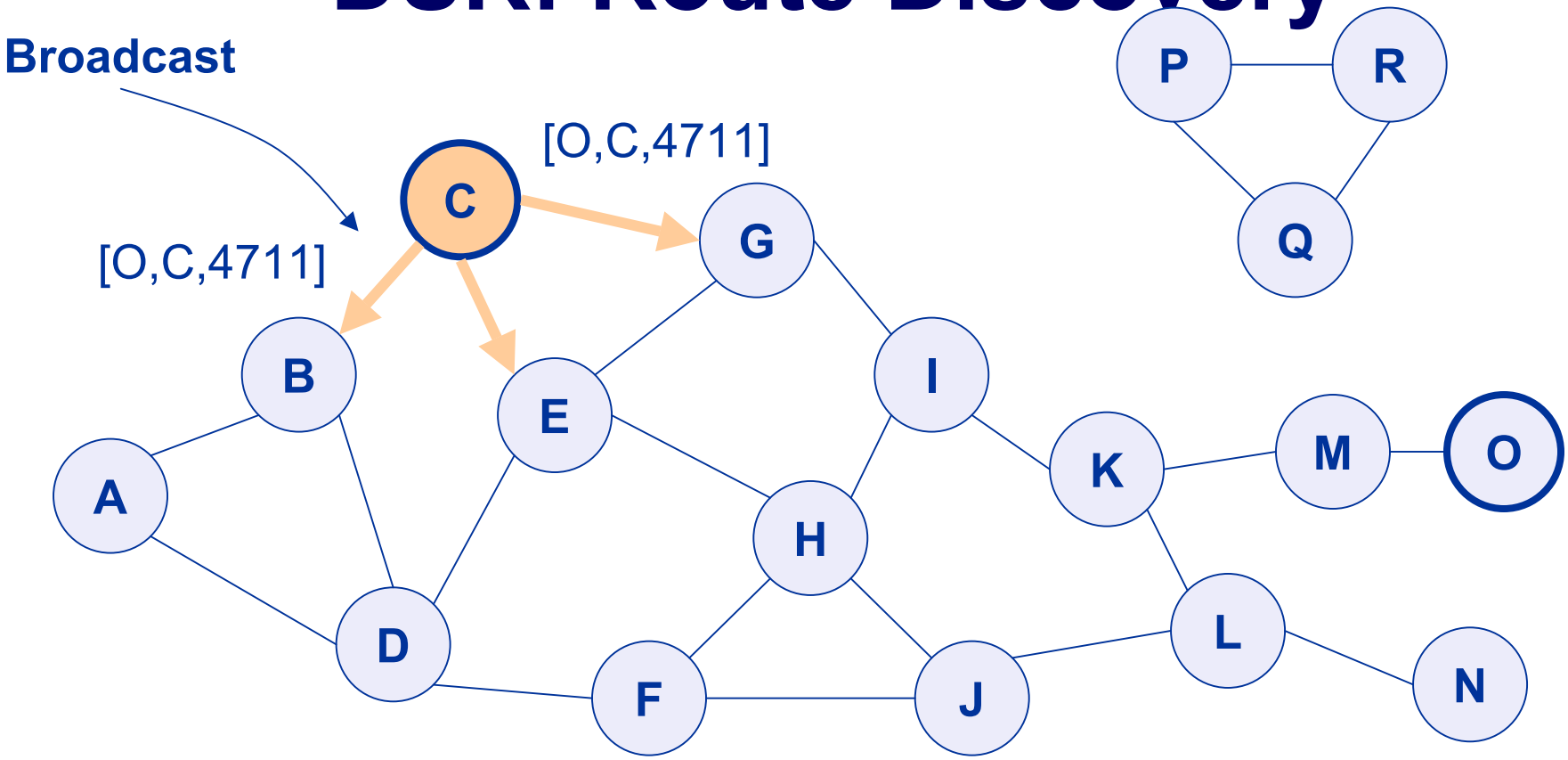
- Optimizations
  - limit broadcasting if maximum diameter of the network is known
  - caching of address lists (i.e. paths) with help of passing packets
    - stations can use the cached information for path discovery (own paths or paths for other hosts)

DSR: Route Discovery

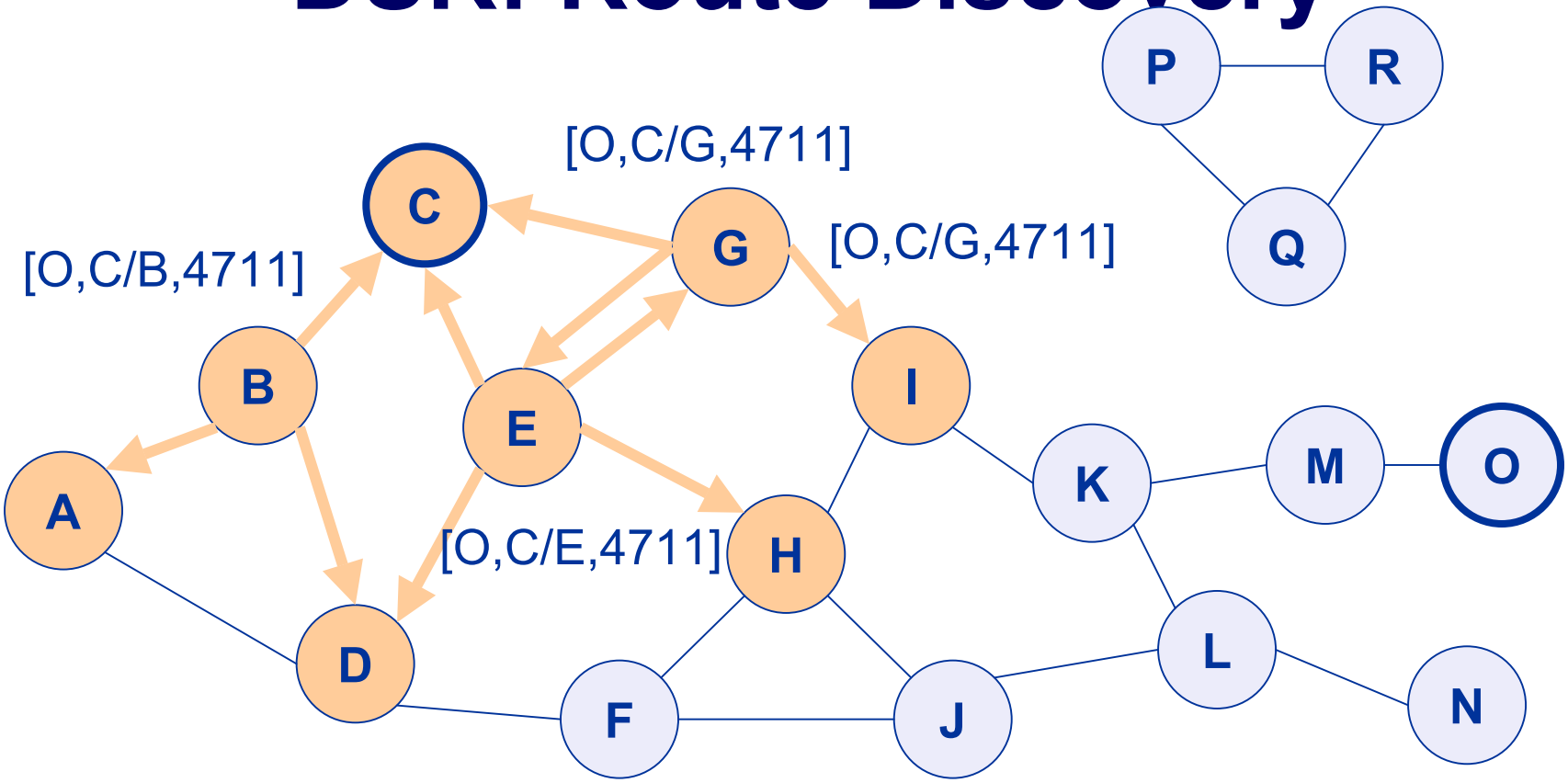
Sending from C to O



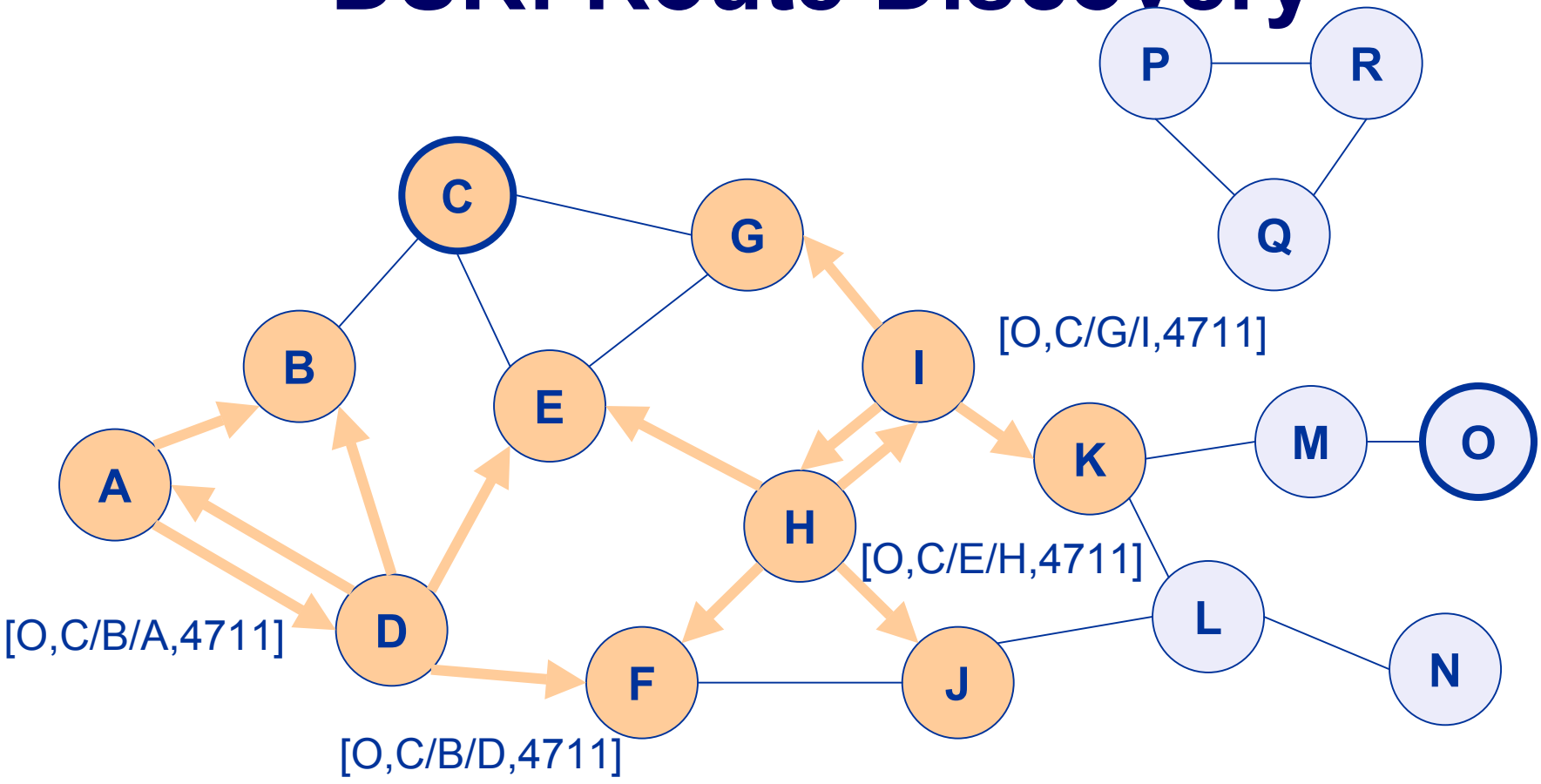
DSR: Route Discovery



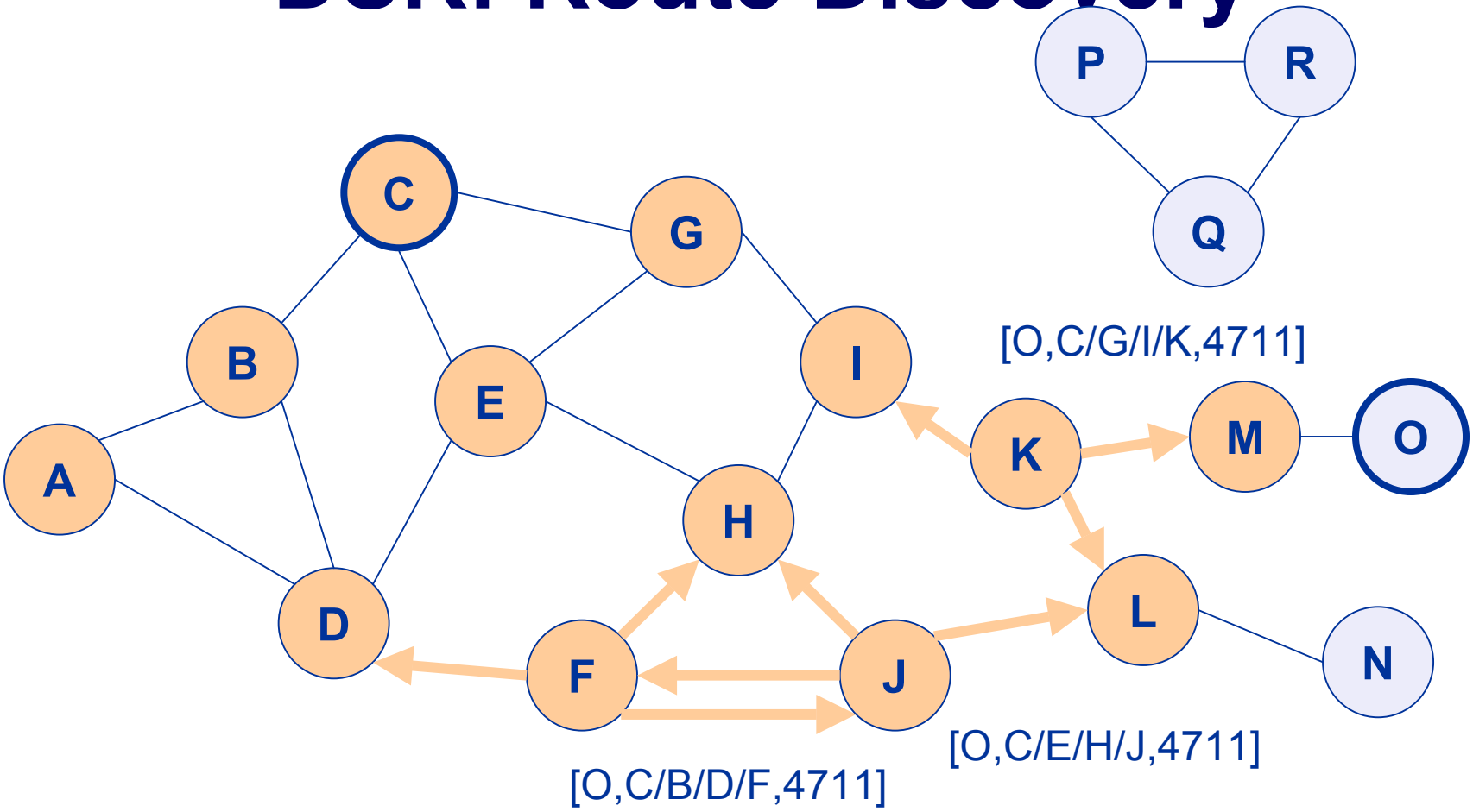
DSR: Route Discovery



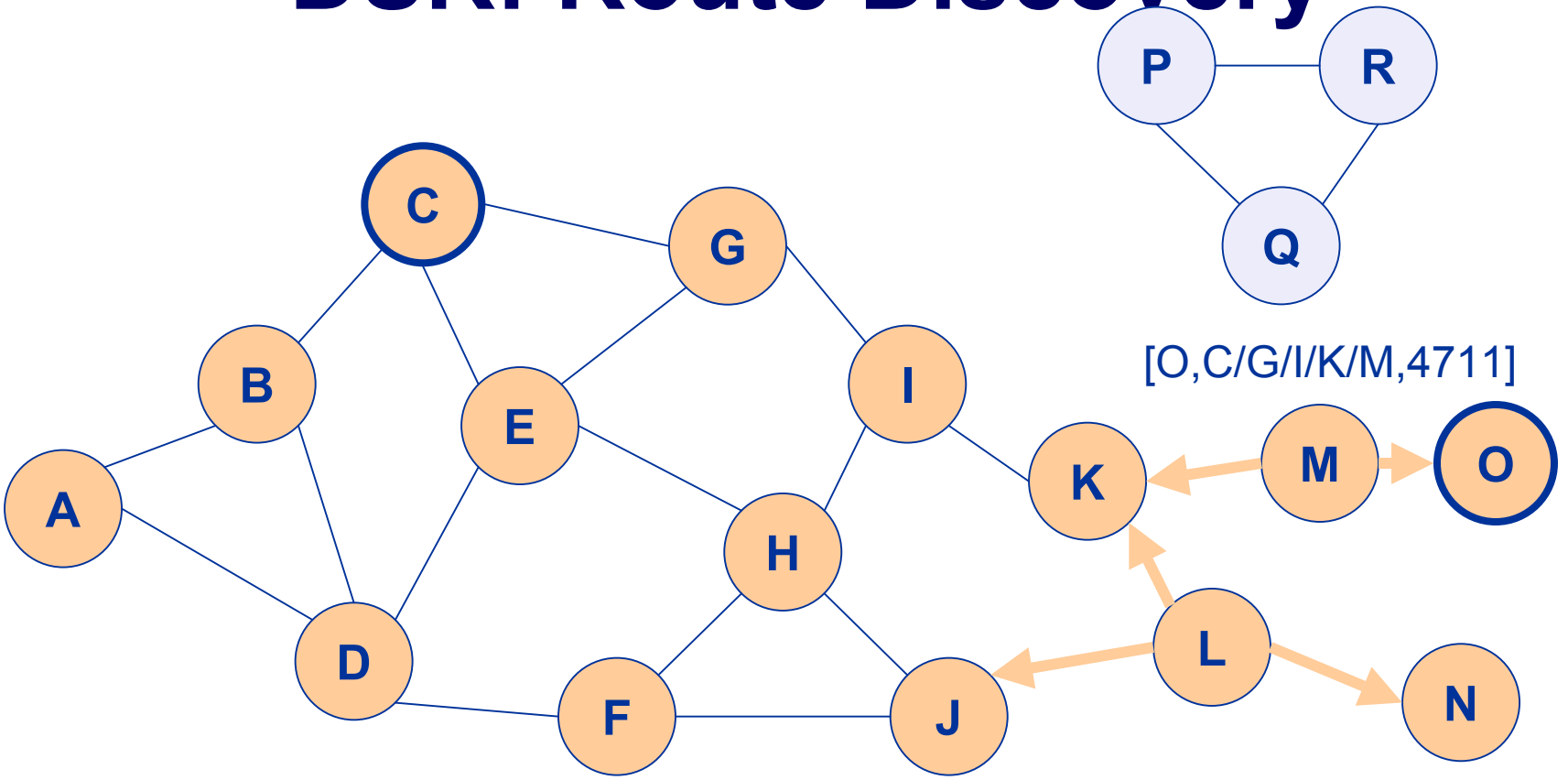
DSR: Route Discovery



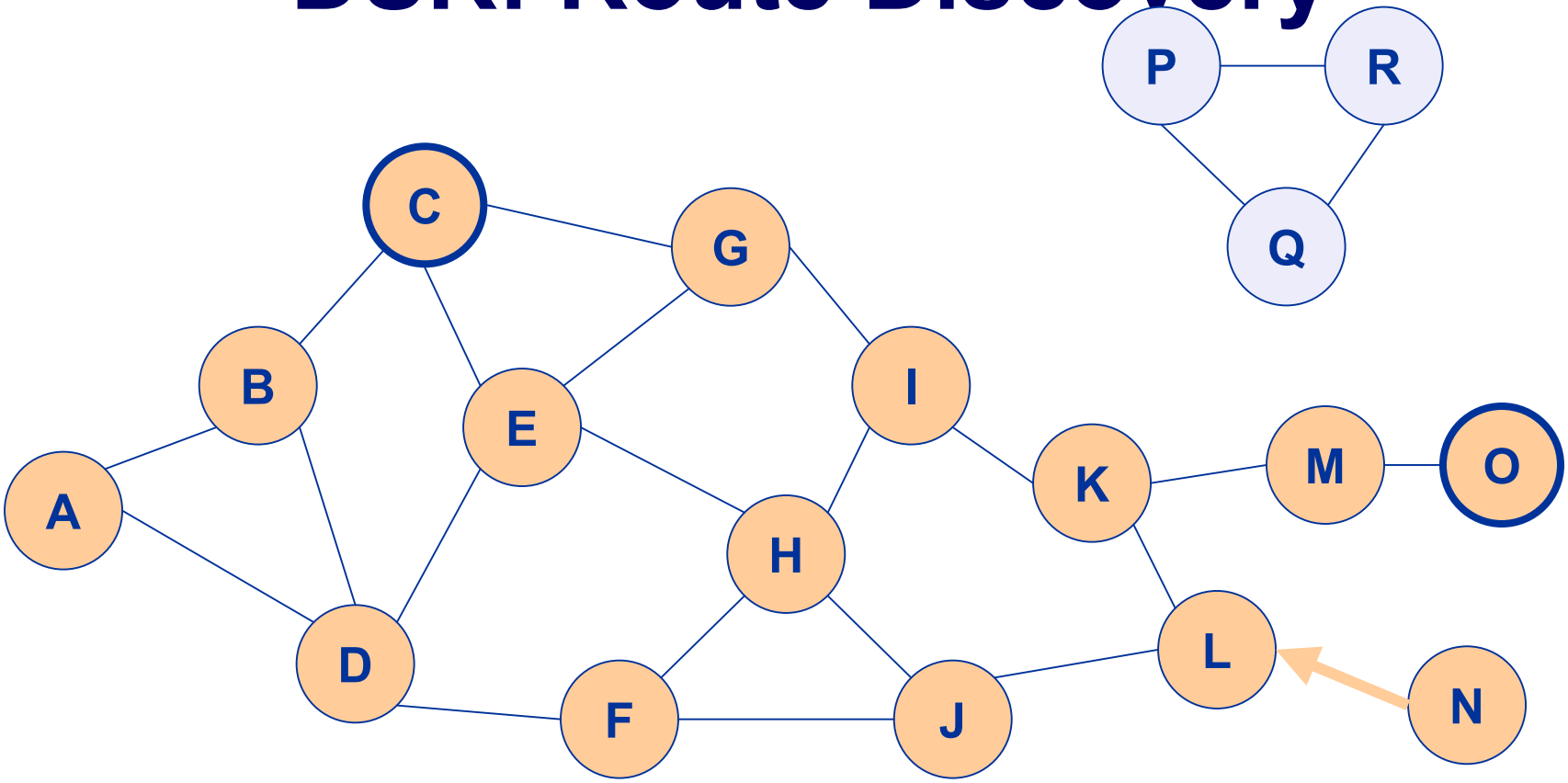
DSR: Route Discovery



DSR: Route Discovery

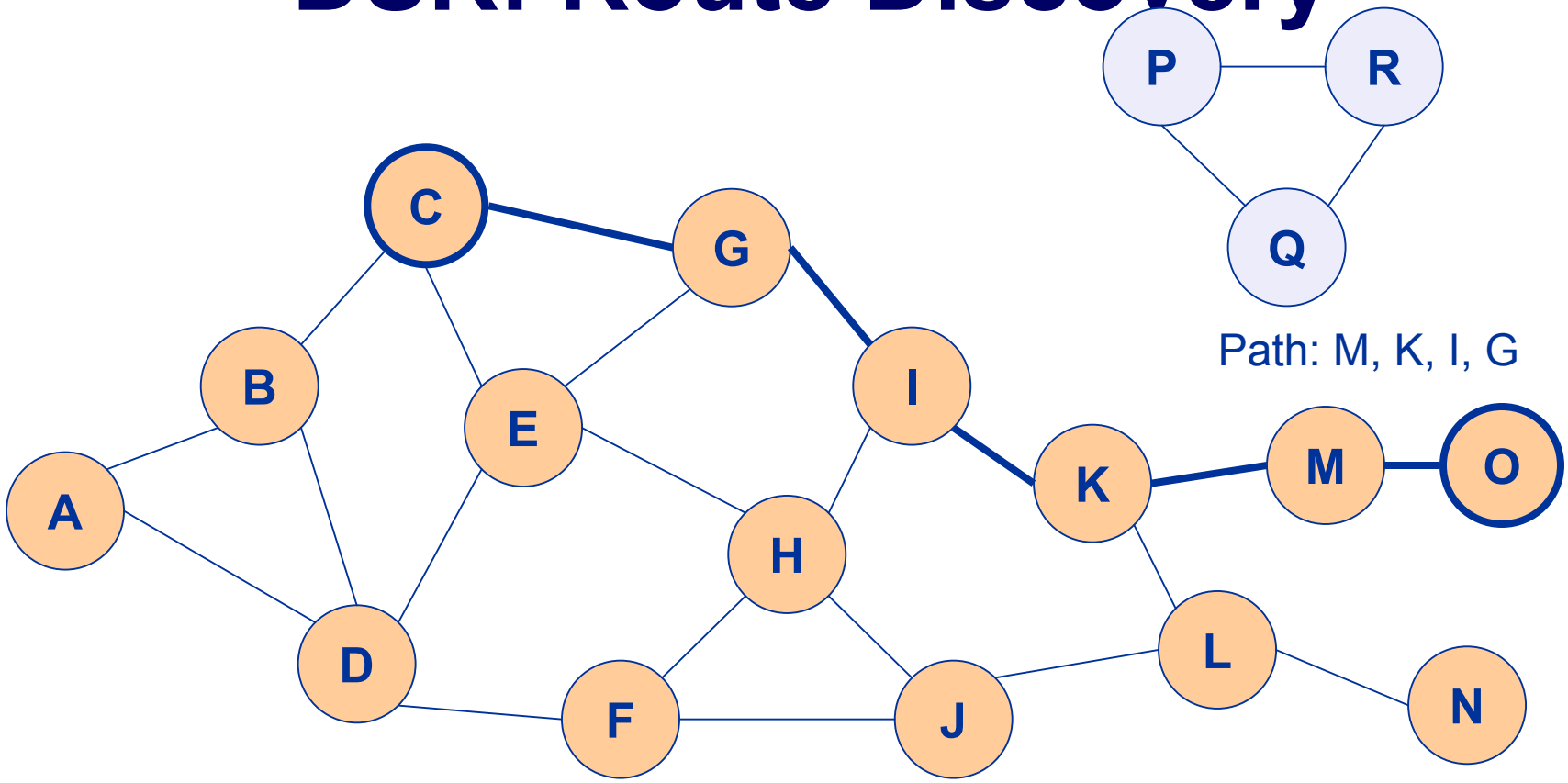


DSR: Route Discovery



[O,C/E/H/J/L/N,4711]

DSR: Route Discovery

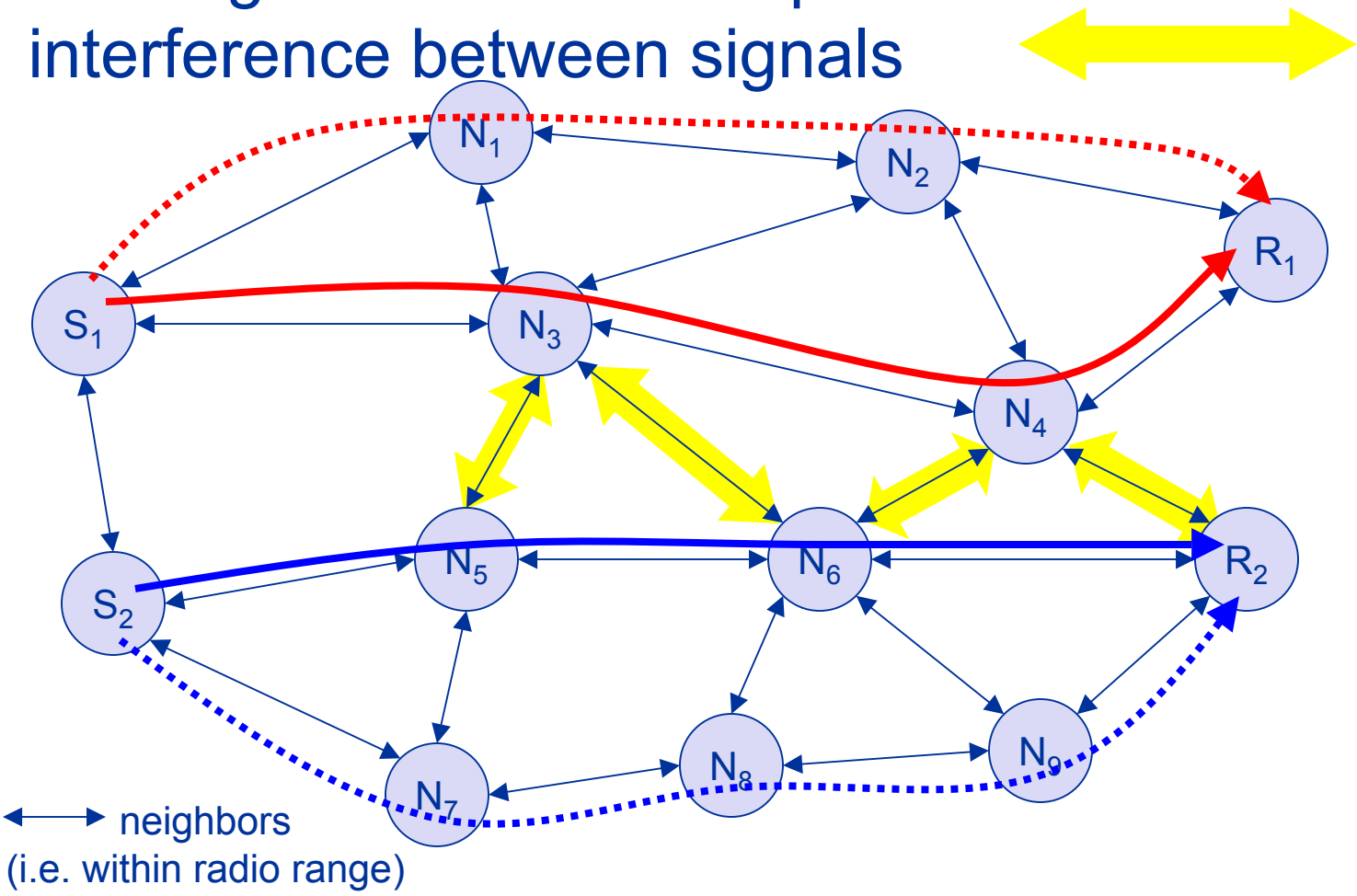


Dynamic Source Routing III

- Maintaining paths
  - after sending a packet
    - wait for a layer 2 acknowledgement (if applicable)
    - listen into the medium to detect if other stations forward the packet (if possible)
    - request an explicit acknowledgement
  - if a station encounters problems it can inform the sender of a packet or look-up a new path locally

Interference-based routing

- Routing based on assumptions about interference between signals



Examples for interference based routing

- Least Interference Routing (LIR)
  - calculate the cost of a path based on the number of stations that can receive a transmission
- Max-Min Residual Capacity Routing (MMRCR)
  - calculate the cost of a path based on a probability function of successful transmissions and interference
- Least Resistance Routing (LRR)
  - calculate the cost of a path based on interference, jamming and other transmissions

- LIR is very simple to implement, only information from direct neighbors is necessary

Other ad hoc routing protocols

- Flat
  - **proactive**
    - FSLS – Fuzzy Sighted Link State
    - FSR – Fisheye State Routing
    - **OLSR** – Optimized Link State Routing Protocol (RFC 3626)
    - TBRPF – Topology Broadcast Based on Reverse Path Forwarding
  - reactive
    - **AODV** – Ad hoc On demand Distance Vector (RFC 3561)
    - **DSR** – Dynamic Source Routing (RFC 4728)
    - **DYMO** – Dynamic MANET On-demand
- Hierarchical
  - CGSR – Clusterhead-Gateway Switch Routing
  - HSR – Hierarchical State Routing
  - LANMAR – Landmark Ad Hoc Routing
  - ZRP – Zone Routing Protocol
- Geographic position assisted
  - DREAM – Distance Routing Effect Algorithm for Mobility
  - GeoCast – Geographic Addressing and Routing
  - GPSR – Greedy Perimeter Stateless Routing
  - LAR – Location-Aided Routing

Two promising candidates: OLSRv2 and DYMO

Problems, research areas

- Auto-Configuration
  - Assignment of addresses, function, profile, program, …
- Service discovery
  - Discovery of services and service providers
- Multicast
  - Transmission to a selected group of receivers
- Quality-of-Service
  - Maintenance of a certain transmission quality
- Power control
  - Minimizing interference, energy conservation mechanisms
- Security
  - Data integrity, protection from attacks (e.g. Denial of Service)
- Scalability
  - 10 nodes? 100 nodes? 1000 nodes? 10000 nodes?
- Integration with fixed networks

Clustering of ad-hoc networks