Prof. Dr.-Ing Jochen H. Schiller
Inst. of Computer Science
Freie Universität Berlin
Germany

Mobile Communications
Chapter 8: Network Protocols/Mobile IP

- Motivation
- Data transfer , Encapsulation
- Security, IPv6, Problems
- Micro mobility support
- DHCP, Locator/ID split, HIP/LISP
- Ad-hoc networks, Routing protocols, WSNs

Motivation for Mobile IP

Routing

- based on IP destination address, network prefix (e.g. 129.13.42) determines physical subnet
- change of physical subnet implies change of IP address to have a topological correct address (standard IP) or needs special entries in the routing tables

Specific routes to end-systems?

- change of all routing table entries to forward packets to the right destination
- does not scale with the number of mobile hosts and frequent changes in the location, security problems

Changing the IP-address?

- adjust the host IP address depending on the current location
- almost impossible to find a mobile system, DNS updates take to long time
- TCP connections break, security problems

Requirements for Mobile IPv4 (RFC 5944 was: 3344, was: 3220, was: …, updated by: …)

Transparency
- mobile end-systems keep their IP address
- continuation of communication after interruption of link possible
- point of connection to the fixed network can be changed

Compatibility
- support of the same layer 2 protocols as IP
- no changes to current end-systems and routers required
- mobile end-systems can communicate with fixed systems

Security
- authentication of all registration messages

Efficiency and scalability
- only little additional messages to the mobile system required (connection typically via a low bandwidth radio link)
- world-wide support of a large number of mobile systems in the whole Internet

Terminology

Mobile Node (MN)
- system (node) that can change the point of connection
  to the network without changing its IP address

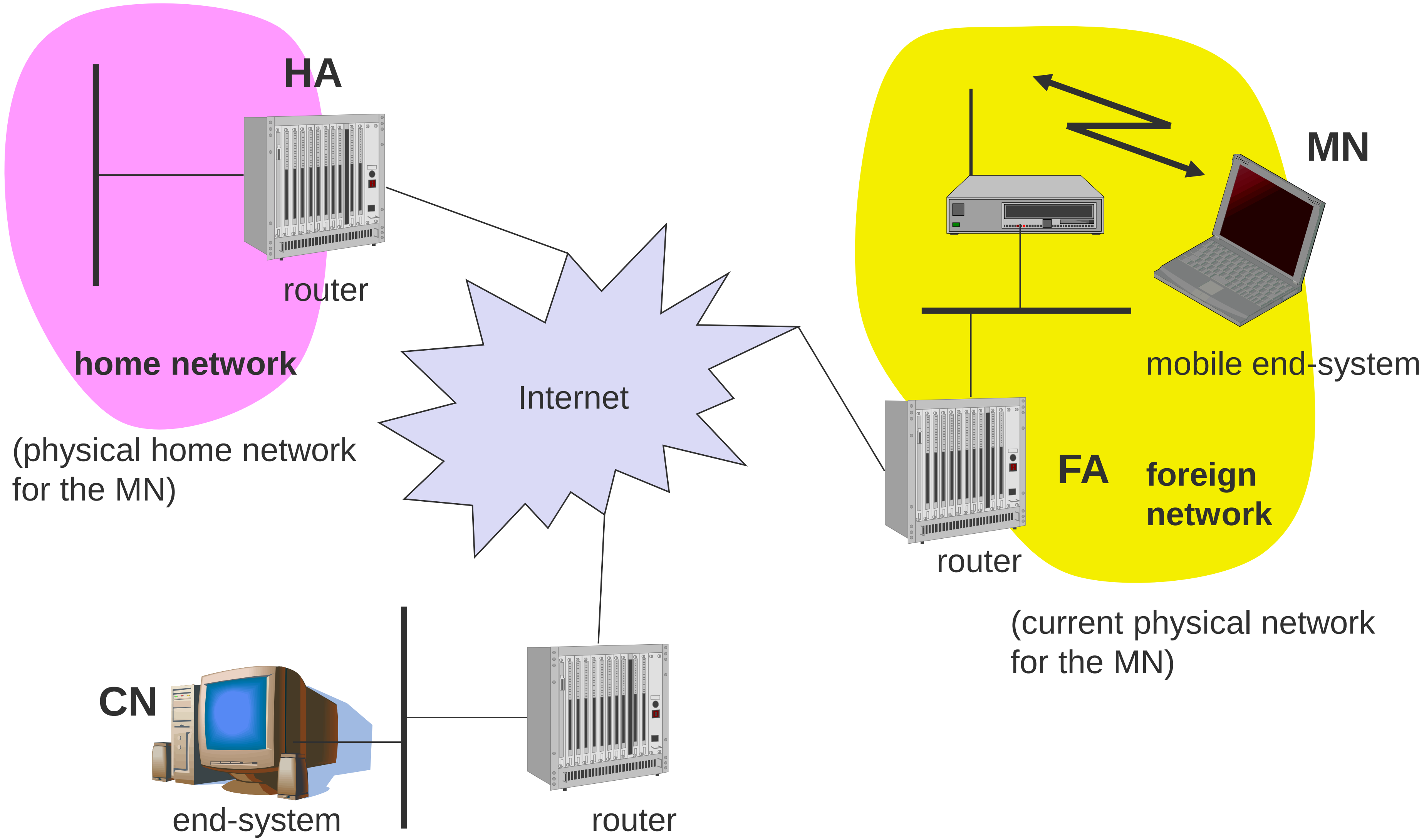
Home Agent (HA)
- system in the home network of the MN, typically a router
- registers the location of the MN, tunnels IP datagrams to the COA

Foreign Agent (FA)
- system in the current foreign network of the MN, typically a router
- forwards the tunneled datagrams to the MN, typically also the default router for the MN

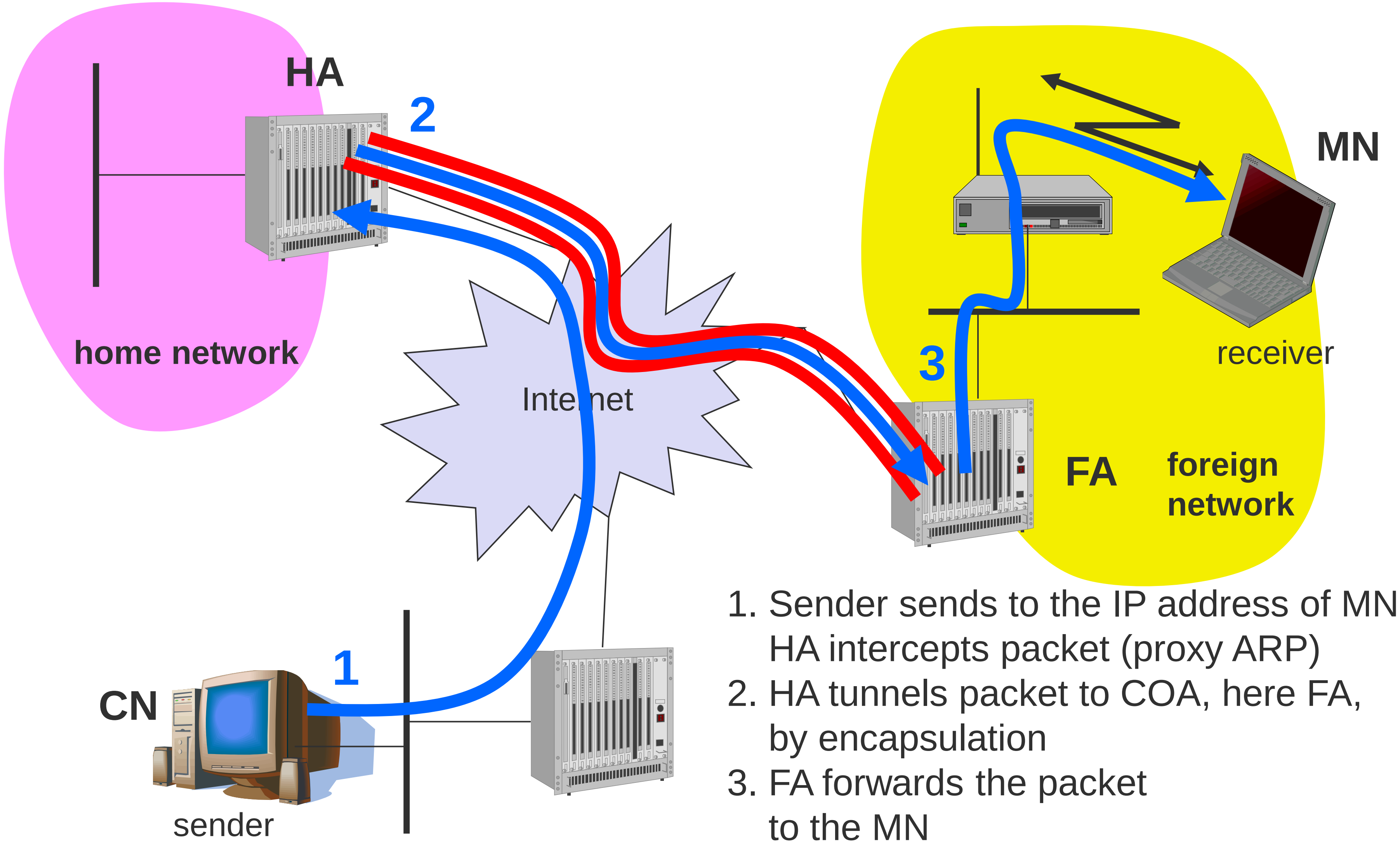
Care-of Address (COA)
- address of the current tunnel end-point for the MN (at FA or MN)
- actual location of the MN from an IP point of view
- can be chosen, e.g., via DHCP

Correspondent Node (CN)
- communication partner

Example network

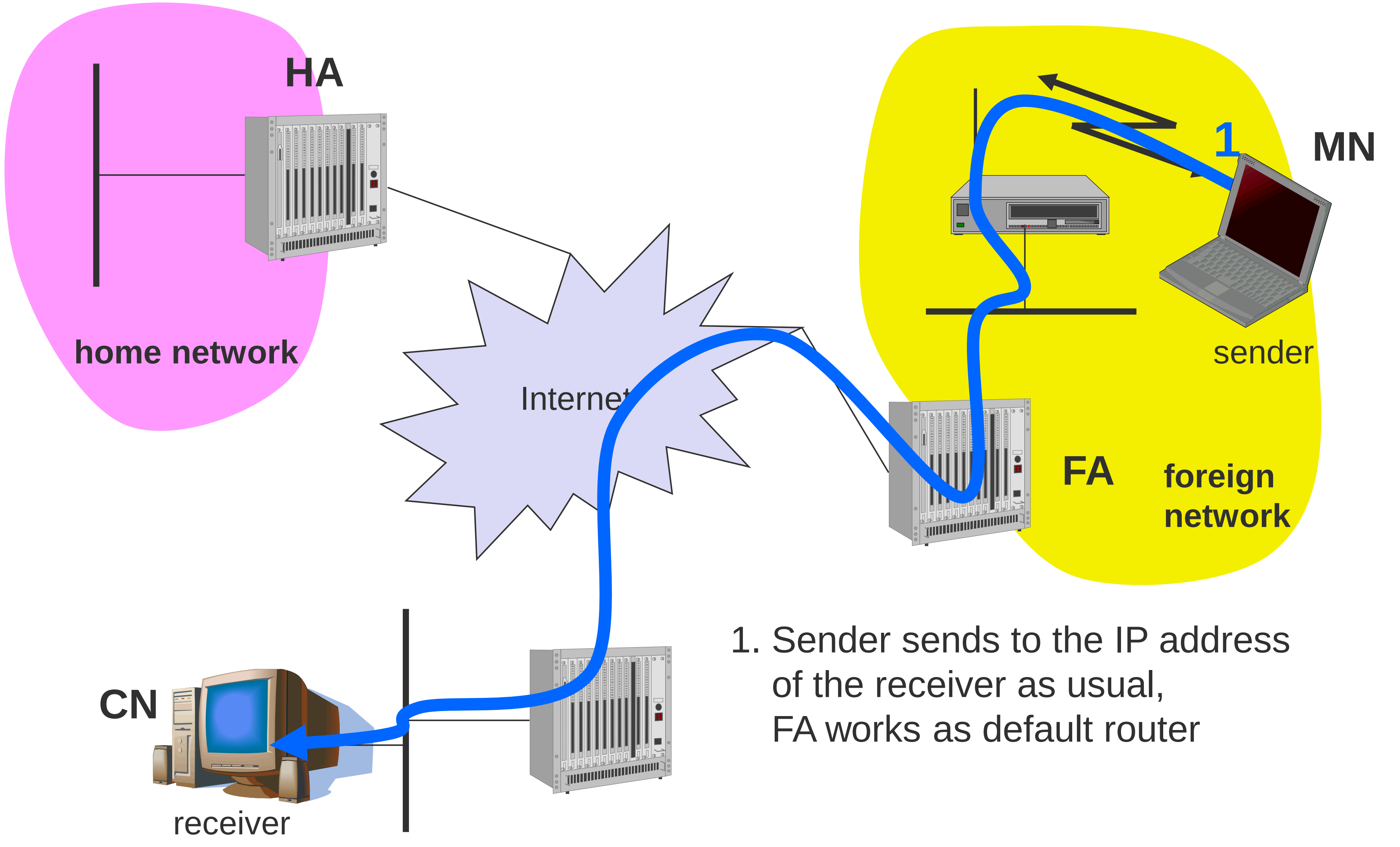


Data transfer to the mobile system



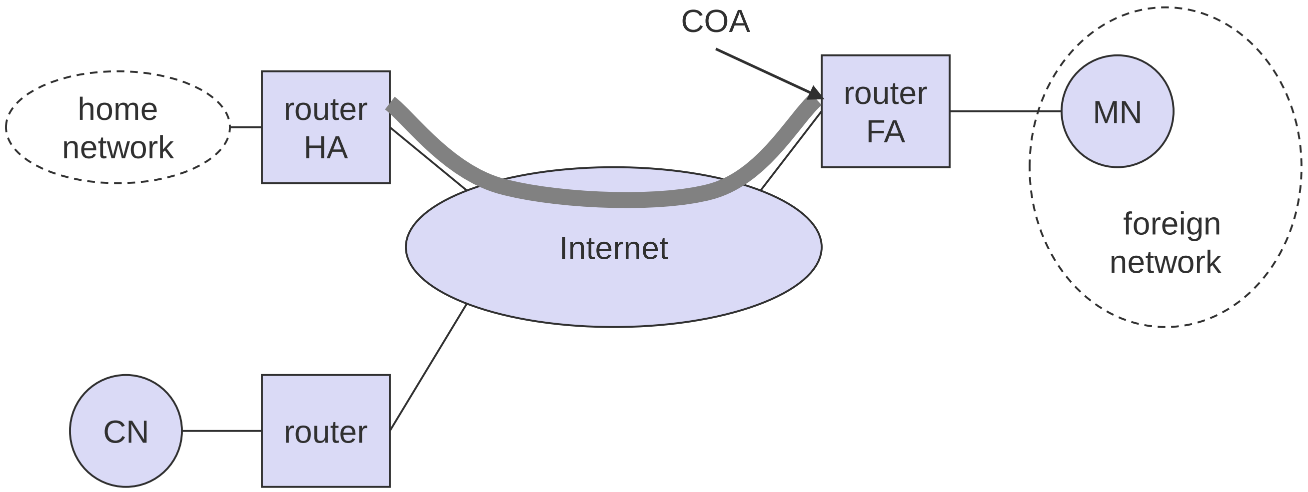
1. Sender sends to the IP address of MN, HA intercepts packet (proxy ARP)
2. HA tunnels packet to COA, here FA, by encapsulation
3. FA forwards the packet to the MN

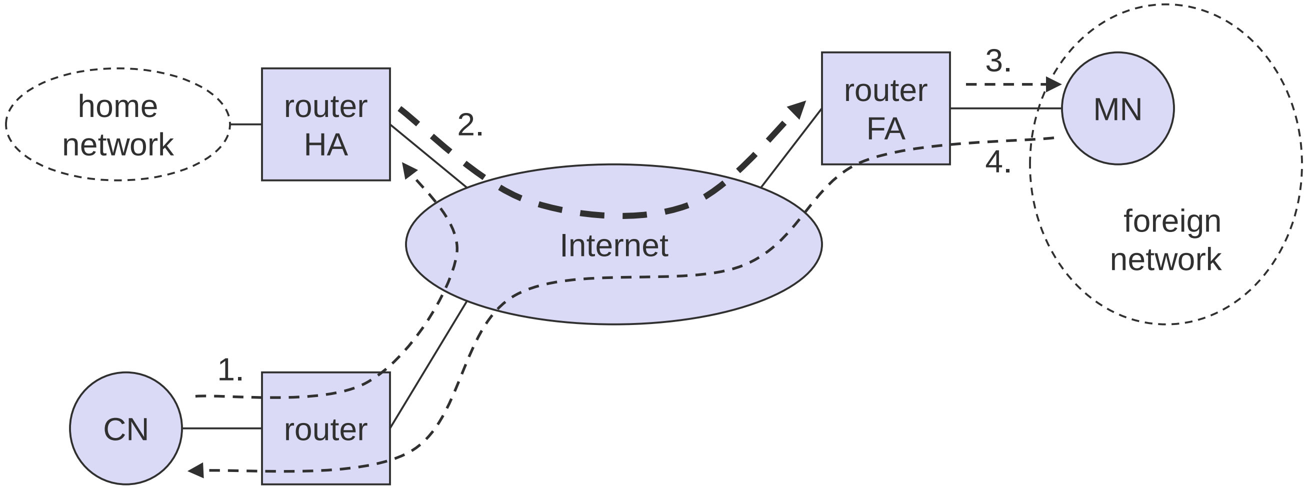
Data transfer from the mobile system



1. Sender sends to the IP address of the receiver as usual, FA works as default router

Overview


COA
home
network
router
HA
router
FA
MN
Internet
foreign
network
CN
router


home
network
router
HA
2.
router
FA
3.
MN
4.
Internet
foreign
network
1.
CN
router

Network integration

Agent Advertisement

- HA and FA periodically send advertisement messages into their physical subnets
- MN listens to these messages and detects, if it is in the home or a foreign network (standard case for home network)
- MN reads a COA from the FA advertisement messages

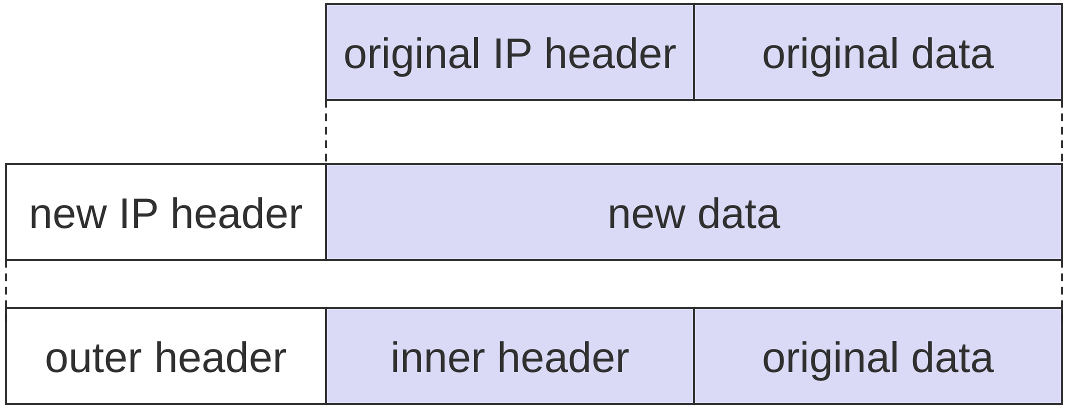
Registration (always limited lifetime!)

- MN signals COA to the HA via the FA, HA acknowledges via FA to MN
- these actions have to be secured by authentication

Advertisement

- HA advertises the IP address of the MN (as for fixed systems), i.e. standard routing information
- routers adjust their entries, these are stable for a longer time (HA responsible for a MN over a longer period of time)
- packets to the MN are sent to the HA,
- independent of changes in COA/FA

Encapsulation



Encapsulation I

Encapsulation of one packet into another as payload

- e.g. IPv6 in IPv4 (6Bone), Multicast in Unicast (Mbone)
- here: e.g. IP-in-IP-encapsulation, minimal encapsulation or GRE (Generic Record Encapsulation)

IP-in-IP-encapsulation (mandatory, RFC 2003)

- tunnel between HA and COA

ver.	IHL	DS (TOS)	length	
IP identification			flags	fragment offset
TTL		*IP-in-IP*	IP checksum	
IP address of HA				
Care-of address COA				
ver.	IHL	DS (TOS)	length	
IP identification			flags	fragment offset
TTL		lay. 4 prot.	IP checksum	
IP address of CN				
IP address of MN				
TCP/UDP/ ... payload				

Optimization of packet forwarding

Problem: Triangular Routing

- sender sends all packets via HA to MN
- higher latency and network load

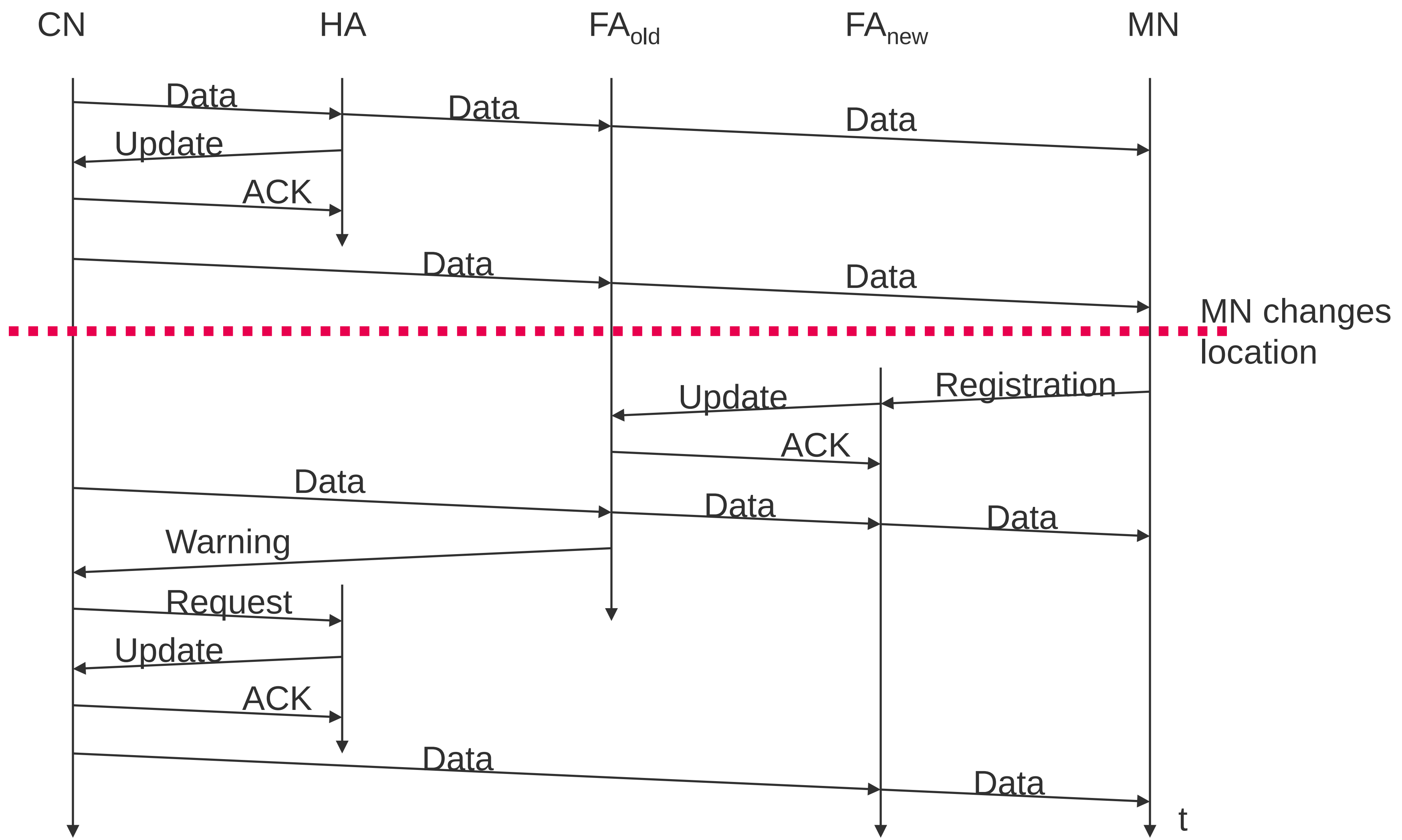
"Solutions"

- sender learns the current location of MN
- direct tunneling to this location
- HA informs a sender about the location of MN
- big security problems!

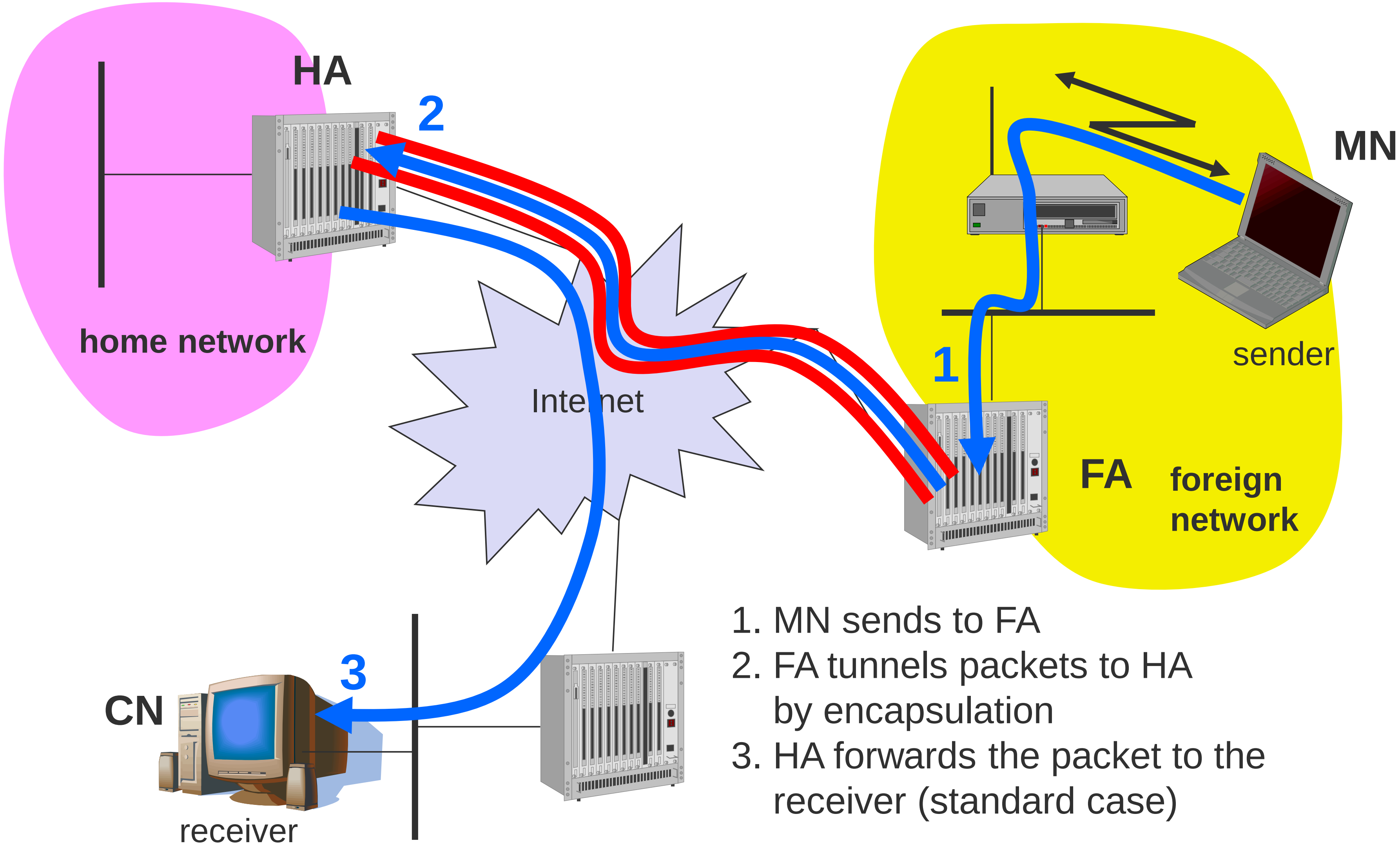
Change of FA

- packets on-the-fly during the change can be lost
- new FA informs old FA to avoid packet loss, old FA now forwards remaining packets to new FA
- this information also enables the old FA to release resources for the MN

Change of foreign agent



Reverse tunneling (RFC 3024, was: 2344)



1. MN sends to FA
2. FA tunnels packets to HA by encapsulation
3. HA forwards the packet to the receiver (standard case)

Mobile IP with reverse tunneling

Router accept often only “topological correct“ addresses (firewall!)

- a packet from the MN encapsulated by the FA is now topological correct
- furthermore multicast and TTL problems solved (TTL in the home network correct, but MN is to far away from the receiver)

Reverse tunneling does not solve

- problems with *firewalls*, the reverse tunnel can be abused to circumvent security mechanisms (tunnel hijacking)
- optimization of data paths, i.e. packets will be forwarded through the tunnel via the HA to a sender (double triangular routing)

The standard is backwards compatible

- the extensions can be implemented easily and cooperate with current implementations without these extensions
- Agent Advertisements can carry requests for reverse tunneling

Mobile IP and IPv6 (RFC 6275, was: 3775)

Mobile IP was developed for IPv4, but IPv6 simplifies the protocols

- security is integrated and not an add-on, authentication of registration is included
- COA can be assigned via auto-configuration (DHCPv6 is one candidate), every node has address auto-configuration
- no need for a separate FA, **all** routers perform router advertisement which can be used instead of the special agent advertisement; addresses are always co-located
- MN can signal a sender directly the COA, sending via HA not needed in this case (automatic path optimization)
- „soft“ hand-over, i.e. without packet loss, between two subnets is supported
    - MN sends the new COA to its old router
    - the old router encapsulates all incoming packets for the MN and forwards them to the new COA
    - authentication is always granted

Problems with mobile IP

Security
- authentication with FA problematic, for the FA typically belongs to another organization
- no common protocol for key management and key distribution widely accepted in the Internet

Firewalls
- typically mobile IP cannot be used together with firewalls, special set-ups are needed (such as reverse tunneling)

QoS
- many new reservations in case of RSVP
- tunneling makes it hard to give a flow of packets a special treatment needed for the QoS

Security, firewalls, QoS etc. are topics of research and discussions

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

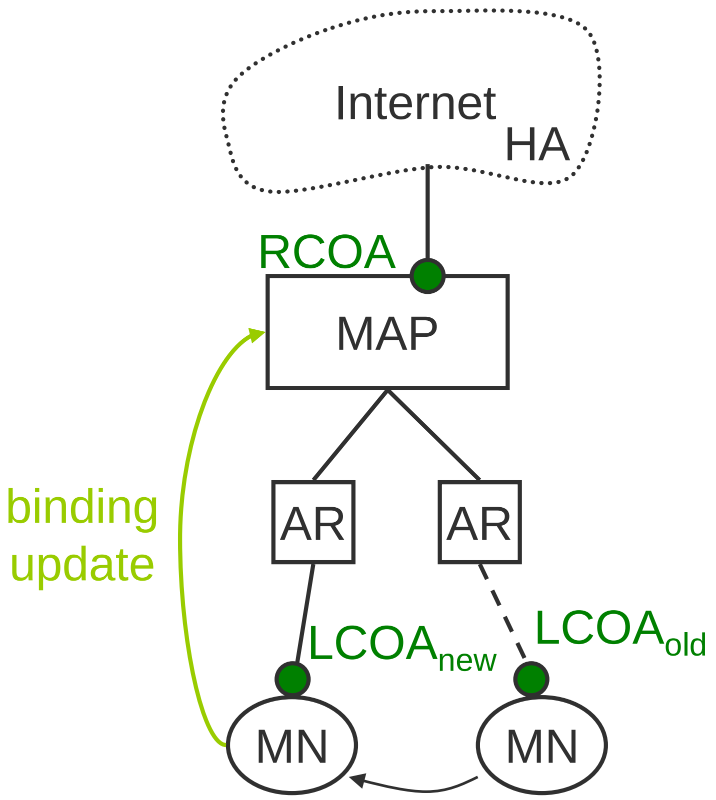
Hierarchical Mobile IPv6 (RFC 5380, was: 4140)

Operation:

- Network contains mobility anchor point (MAP)
  - mapping of regional COA (RCOA) to link COA (LCOA)
- Upon handover, MN informs MAP only
  - gets new LCOA, keeps RCOA
- HA is only contacted if MAP changes

Security provisions:

- no HMIP-specific security provisions
- binding updates should be authenticated



Freie Universität Berlin

Hierarchical Mobile IP: Security

Advantages:

- Local COAs can be hidden,
  which provides at least some location privacy
- Direct routing between CNs sharing the same link is possible (but might be dangerous)

Potential problems:

- Decentralized security-critical functionality
  (handover processing) in mobility anchor points
- MNs can (must!) directly influence routing entries via binding updates (authentication necessary)

Hierarchical Mobile IP: Other issues

Advantages:

- Handover requires minimum number of overall changes to routing tables
- Integration with firewalls / private address support possible

Potential problems:

- Not transparent to MNs
- Handover efficiency in wireless mobile scenarios:
  - Complex MN operations
  - All routing reconfiguration messages sent over wireless link

Host Identity Protocol v2 (HIPv2, RFC 7401, was: 5201, updated by 6253)

Separation of Identification and Localization of mobile device ("Locator/ID split")

- Alternative to Mobile IP
- Introduction of HIP layer between routing and transport
- IP addresses for routing only, change depending on location (must be topological correct!)
- Identification via Host Identity Tag, used e.g. for TCP connection identification instead of IP address
- Host Identity Tag based on public keys
    - Communication requires Diffie Hellman key exchange
- Pro
    - No intermediate agent, normal IP routing
- Con
    - Extra RTT due to key exchange, firewalls, extra layer
- See also RFCs 5202, 5203, 5204, 5205, 5206, 5207, 5770…

Locator/ID Separation Protocol (LISP, RFC 6830)

- New routing concept, tunneling for data transport, no changes to hosts
- RLOC (Routing Locator) and EID (Endpoint Identifier)

Mobile ad hoc networks

Standard Mobile IP needs an infrastructure

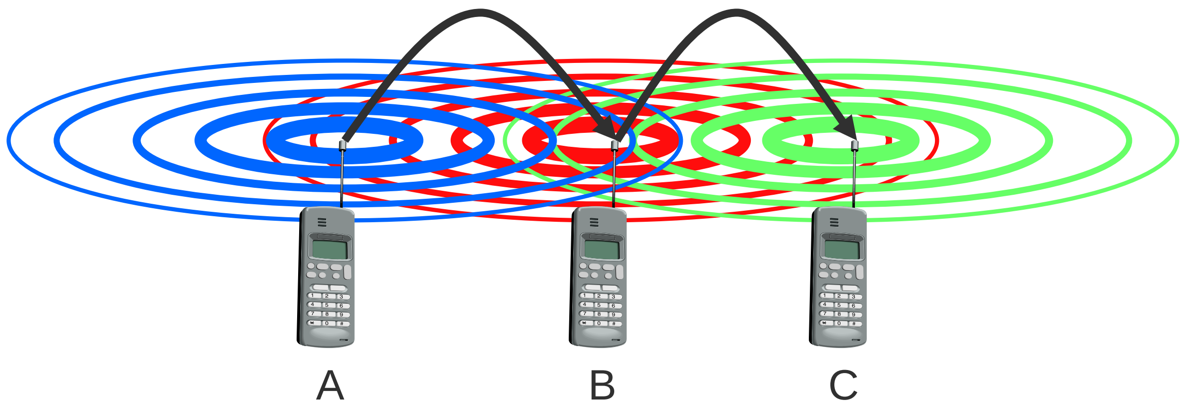
- Home Agent/Foreign Agent in the fixed network
- DNS, routing etc. are not designed for mobility

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



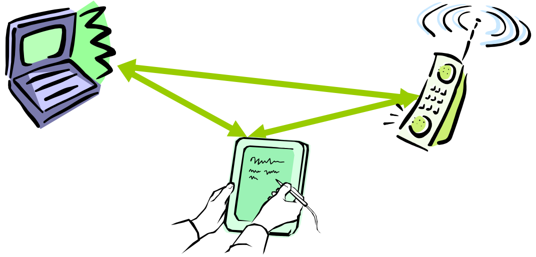
Solution: Wireless ad-hoc networks

Network without infrastructure

- Use components of participants for networking

Examples

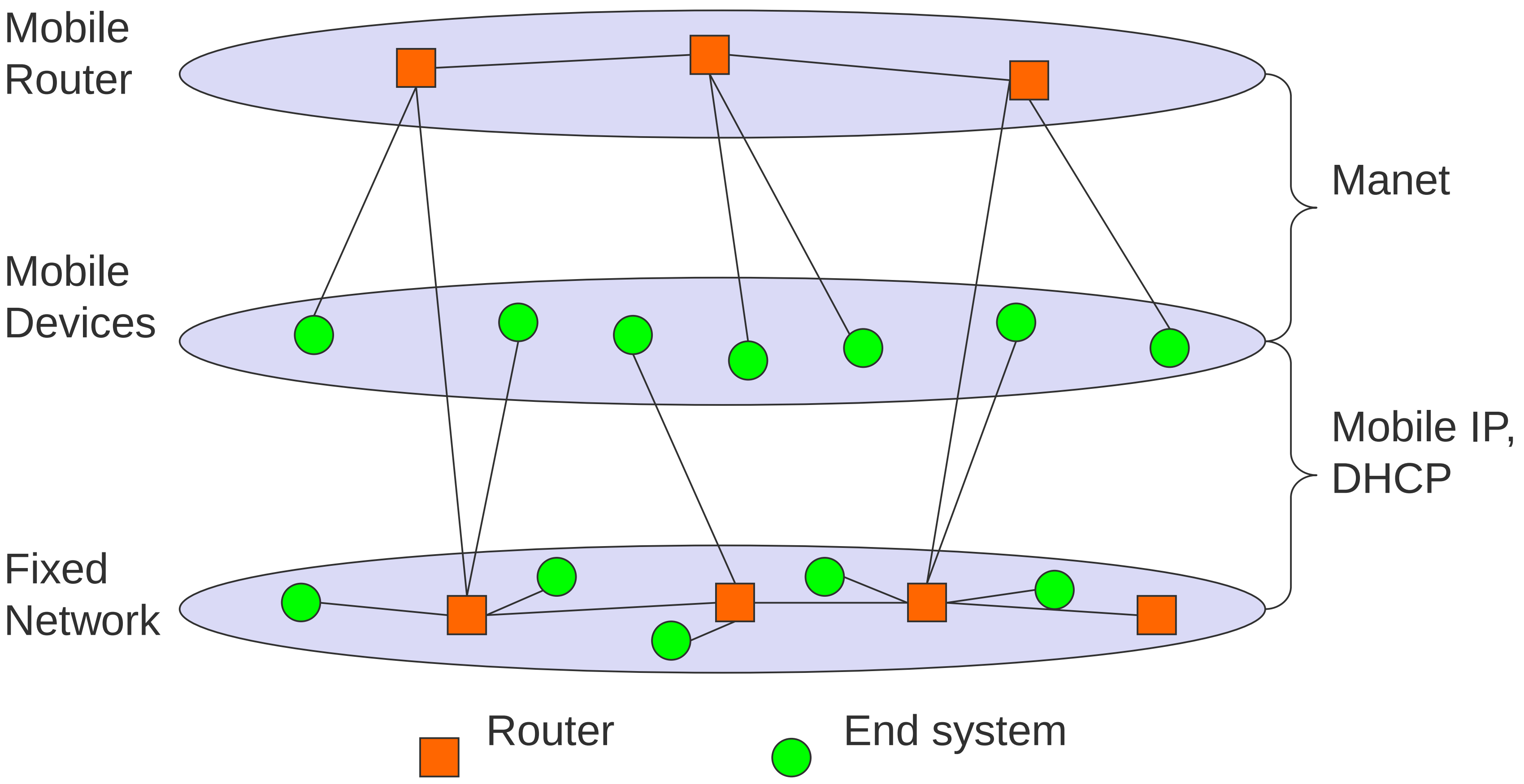
- Single-hop: All partners max. one hop apart
  - Bluetooth piconet, PDAs in a room, gaming devices…



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

Internet: MANET (Mobile Ad-hoc Networking) group

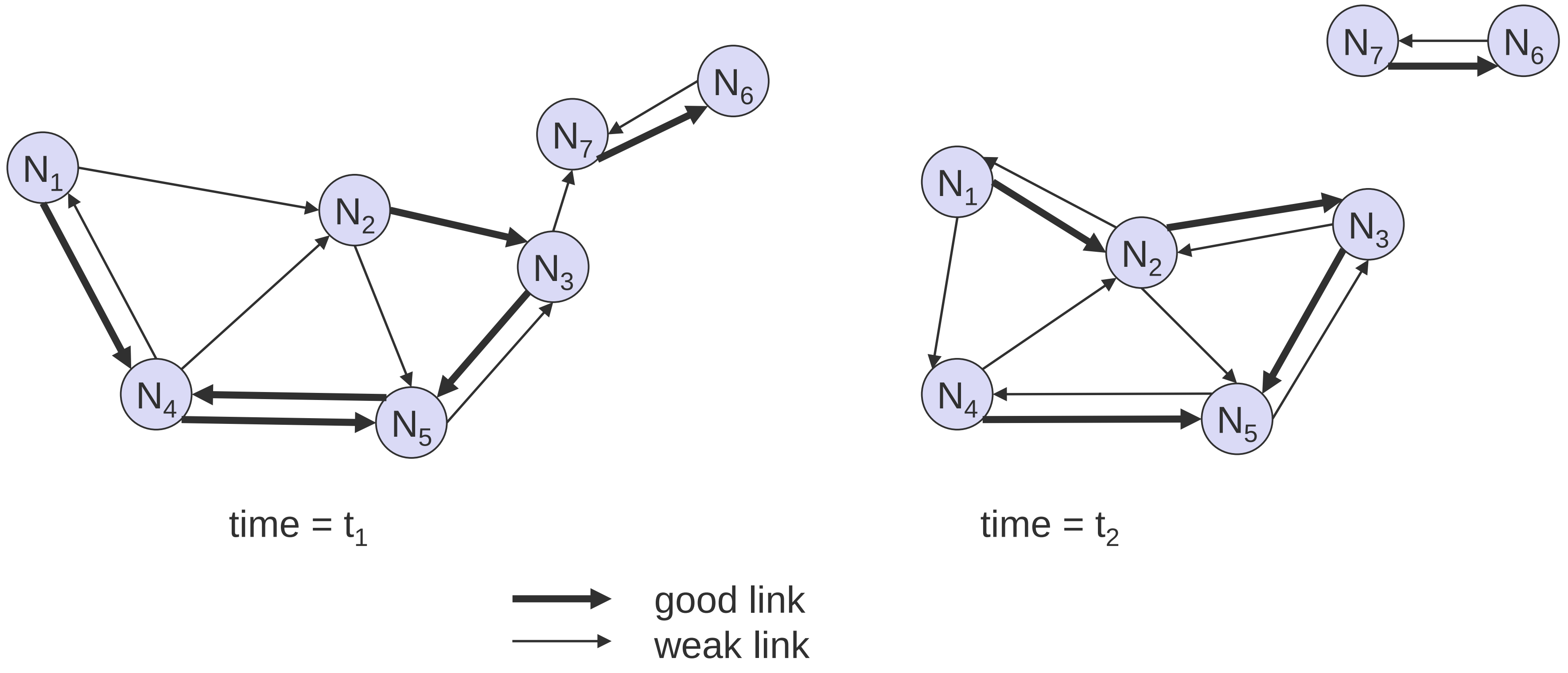
Manet: Mobile Ad-hoc Networking



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, 100, 150, … different proposals exist
- The most simple 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 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

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

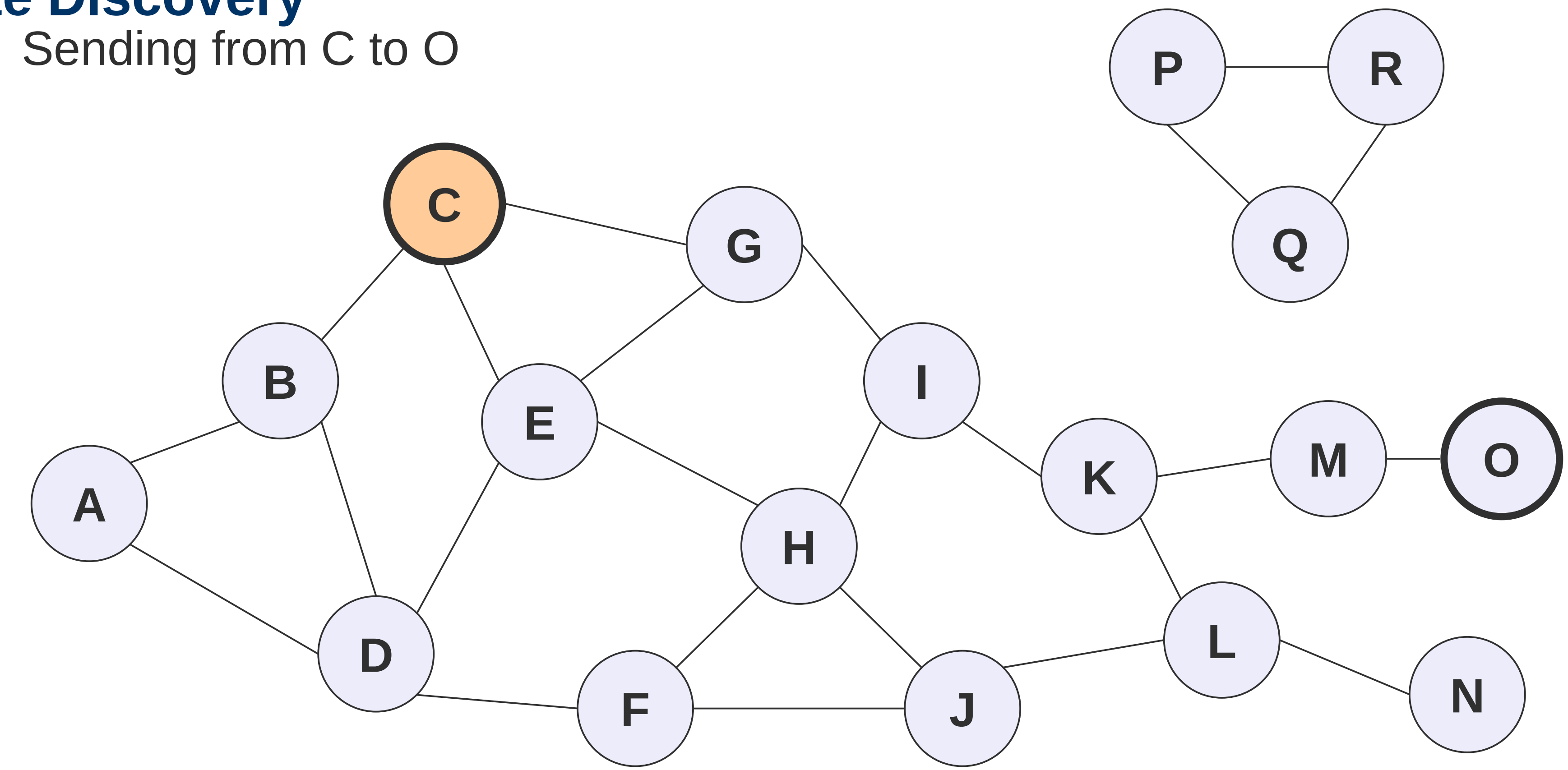
- broadcast a packet with destination address and unique ID
- if a station receives a broadcast packet
  - if the station is the receiver (i.e., has the correct destination address) then return the packet to the sender (path was collected in the packet)
  - if the packet has already been received earlier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

Optimizations

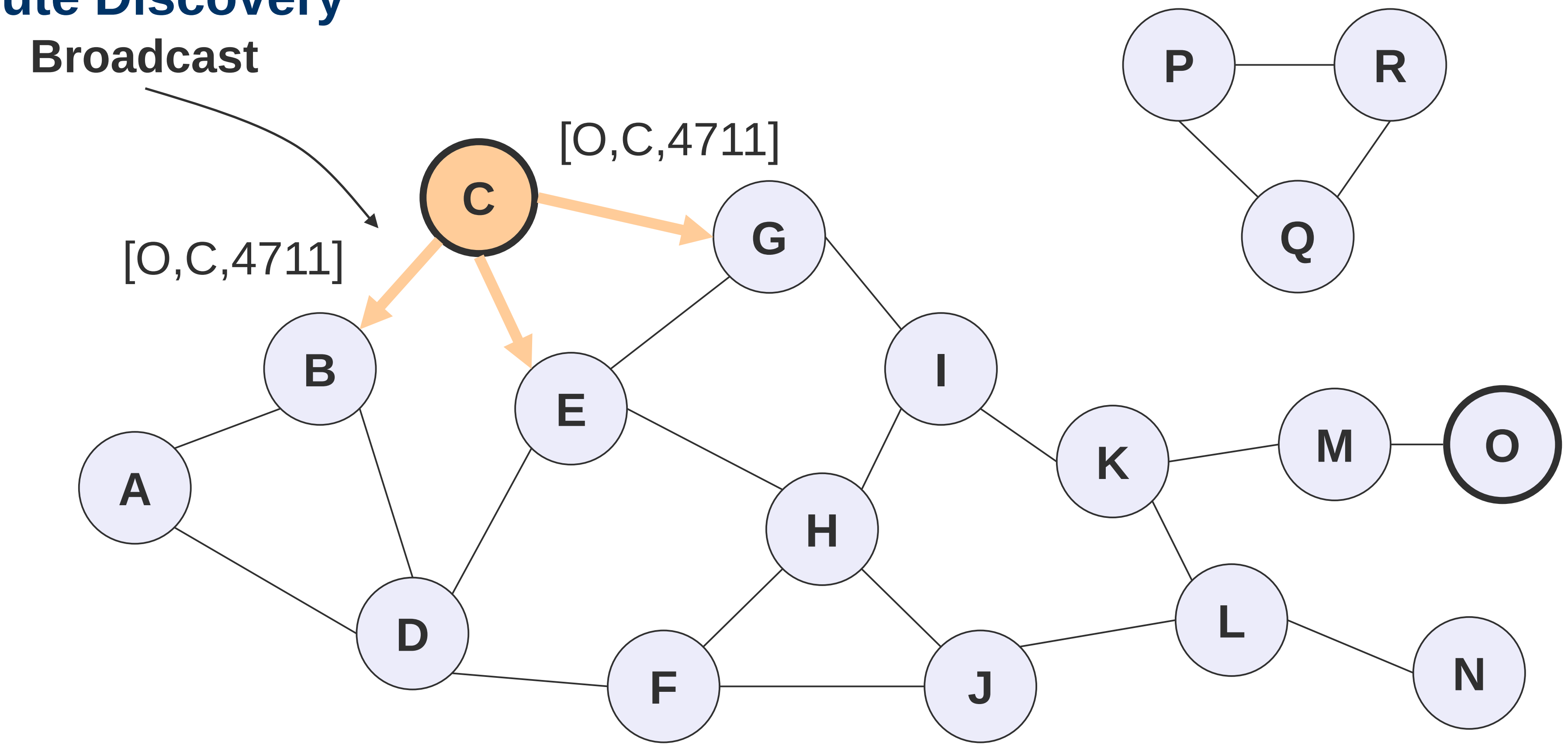
- limit broadcasting if maximum diameter of the network is known
- caching of address lists (i.e. paths) with help of passing packets
  - stations can use the cached information for path discovery (own paths or paths for other hosts)

DSR: Route Discovery

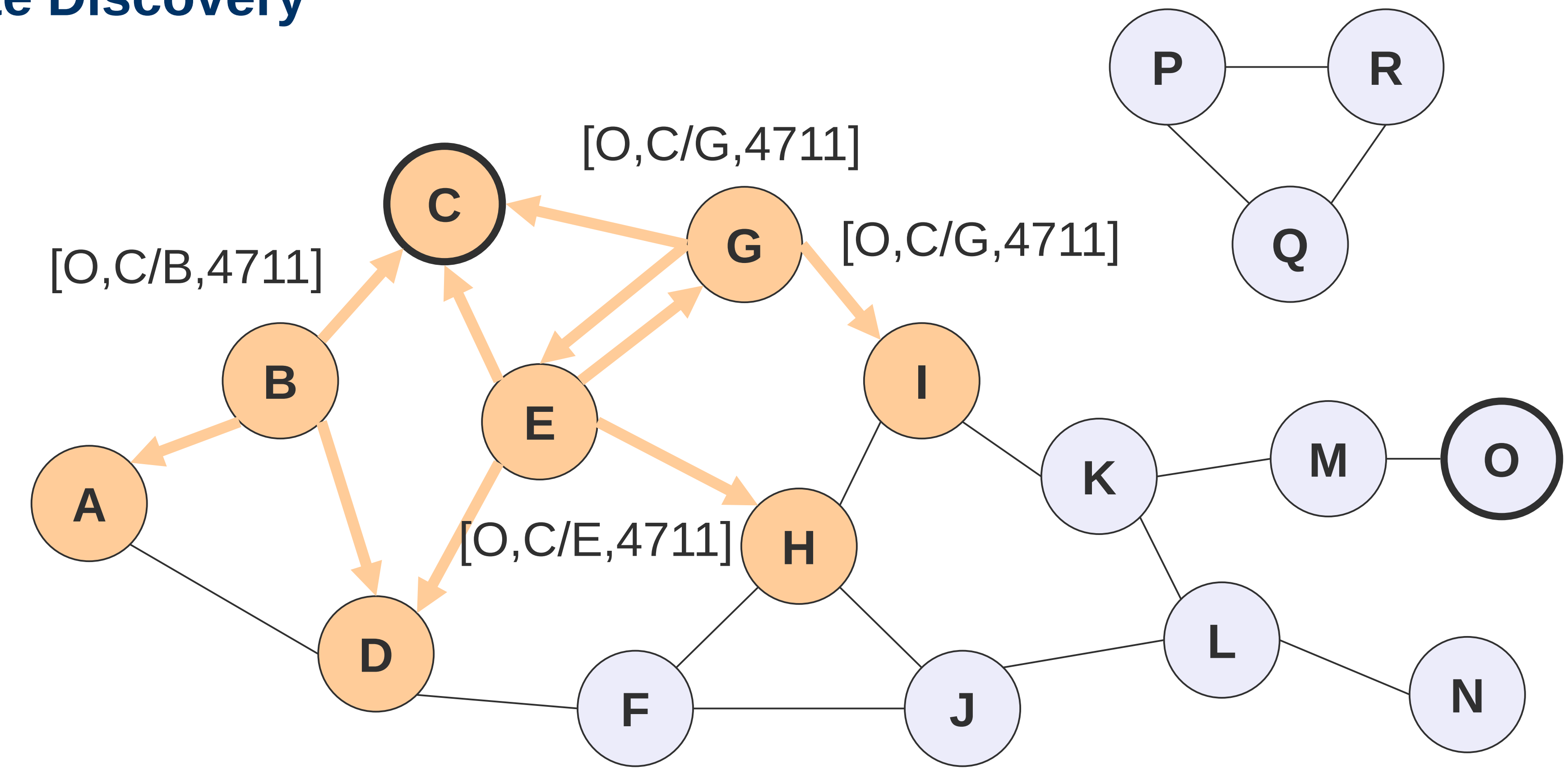
Sending from C to O



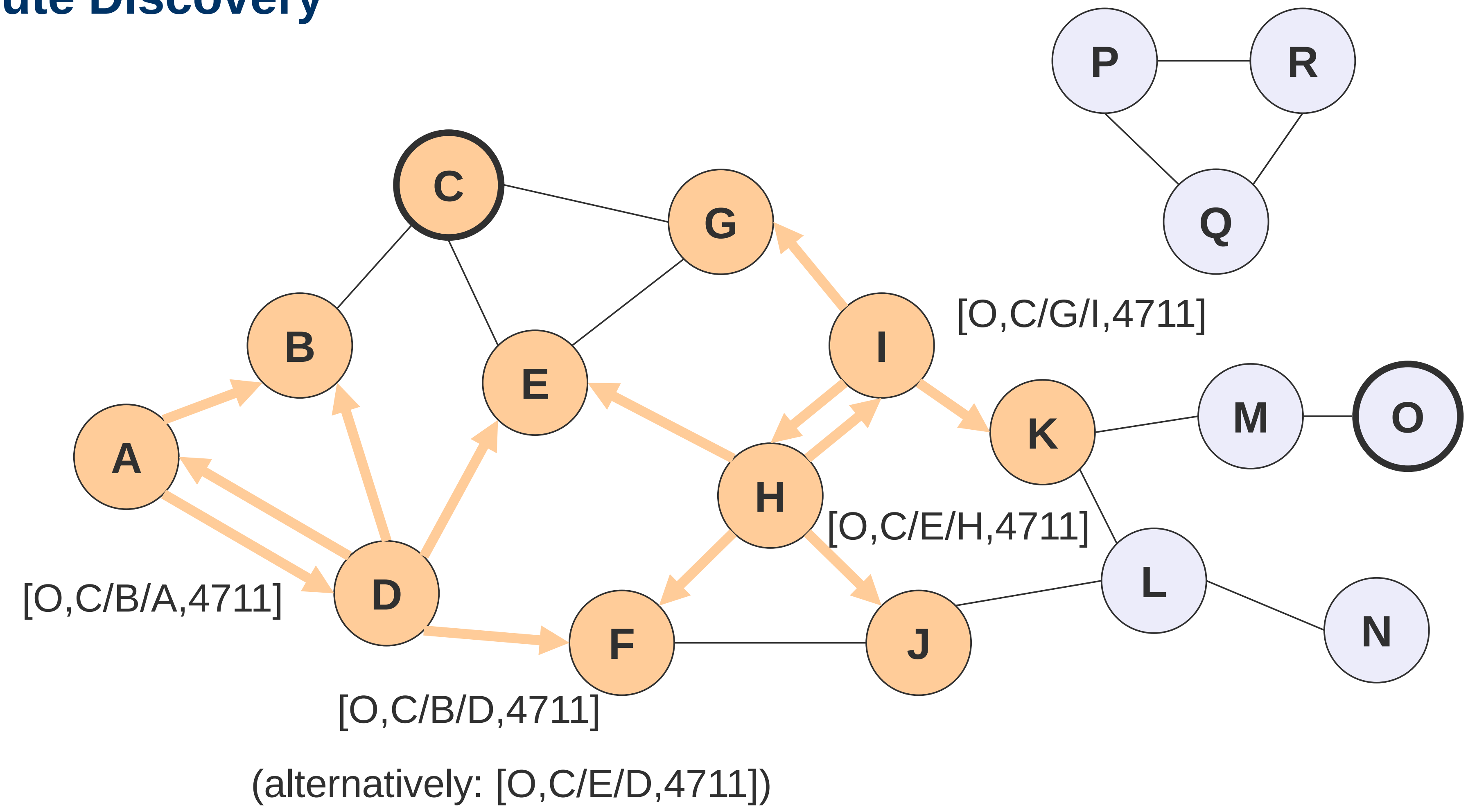
DSR: Route Discovery



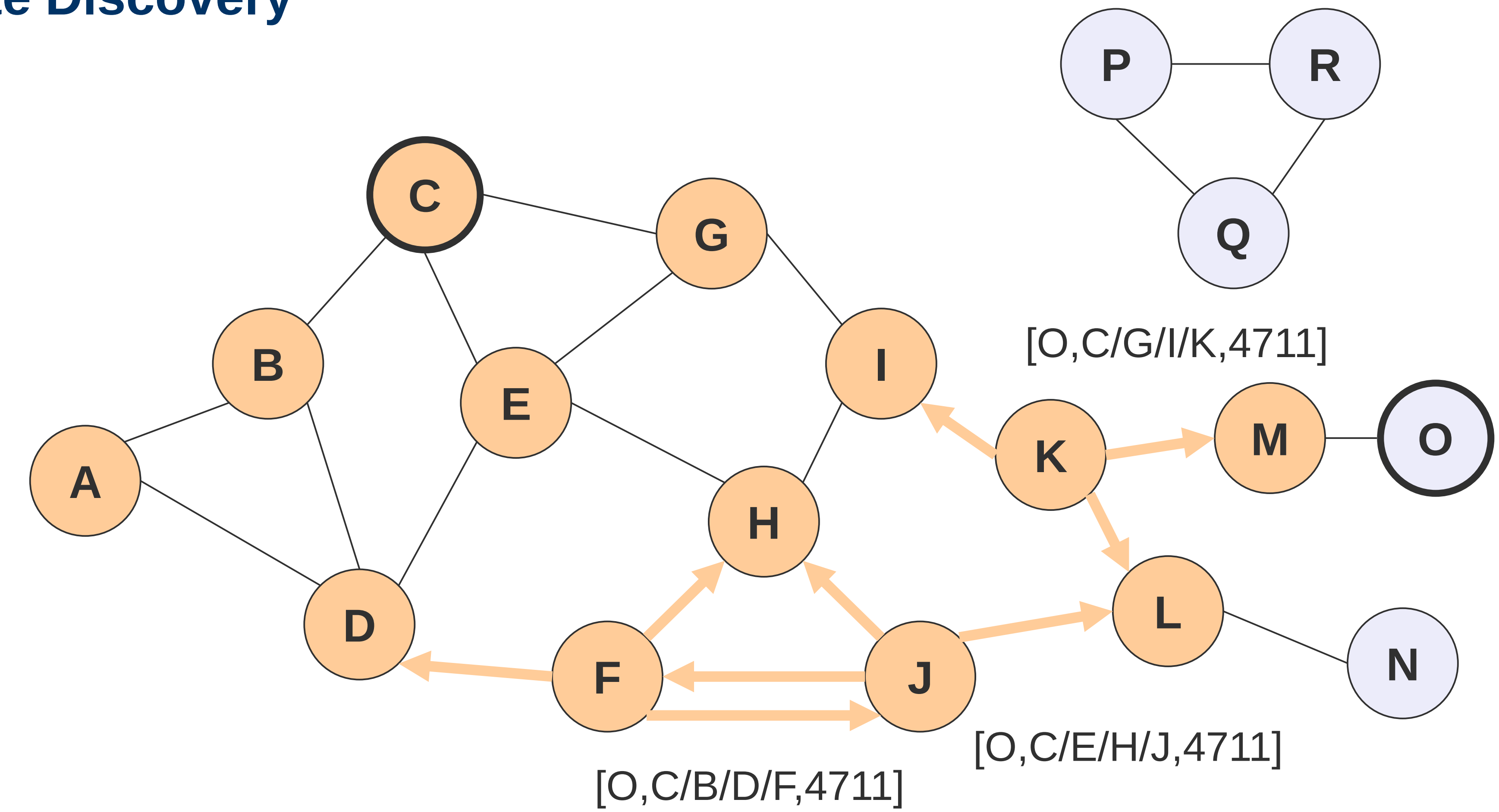
DSR: Route Discovery



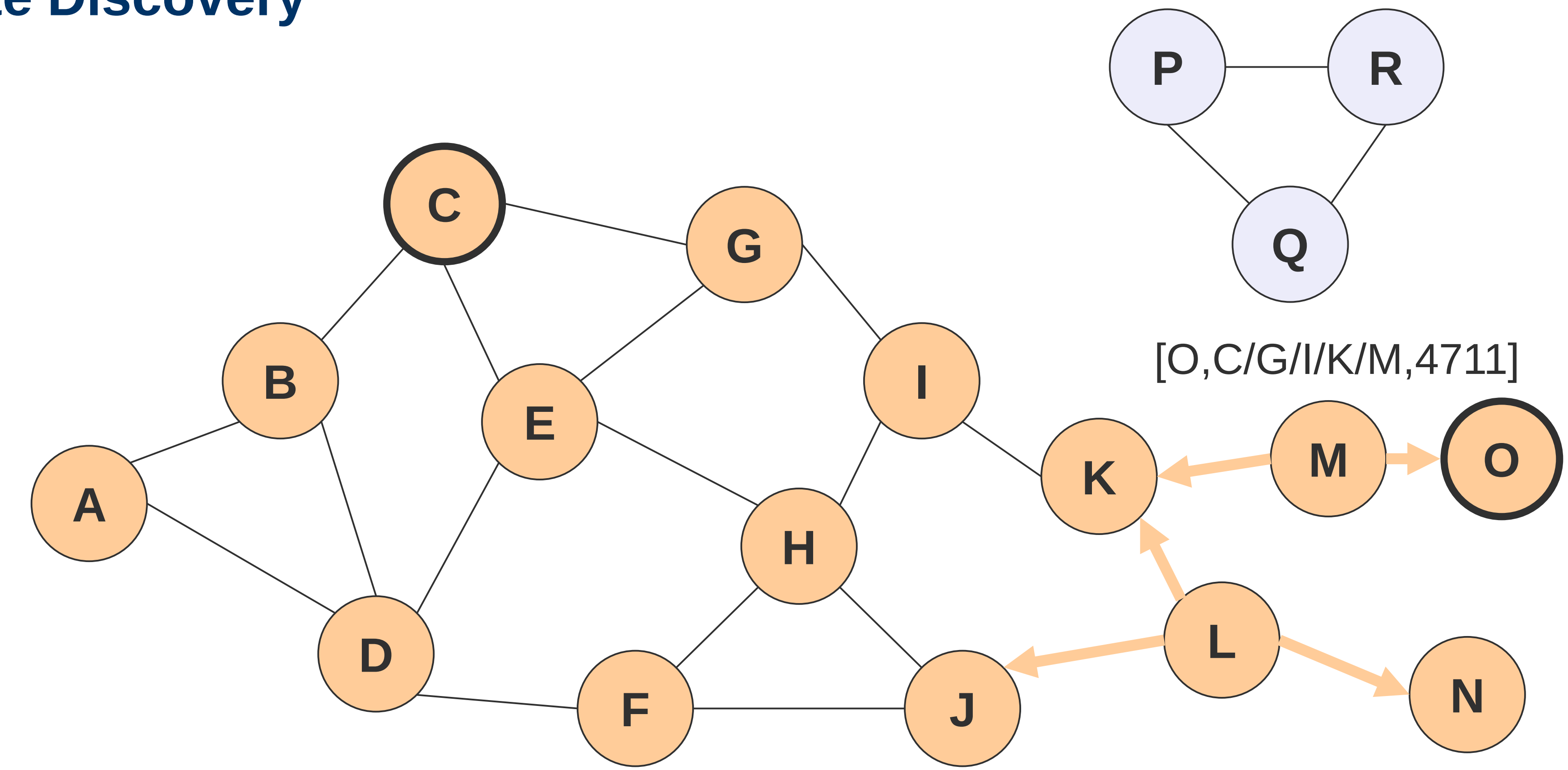
DSR: Route Discovery



DSR: Route Discovery



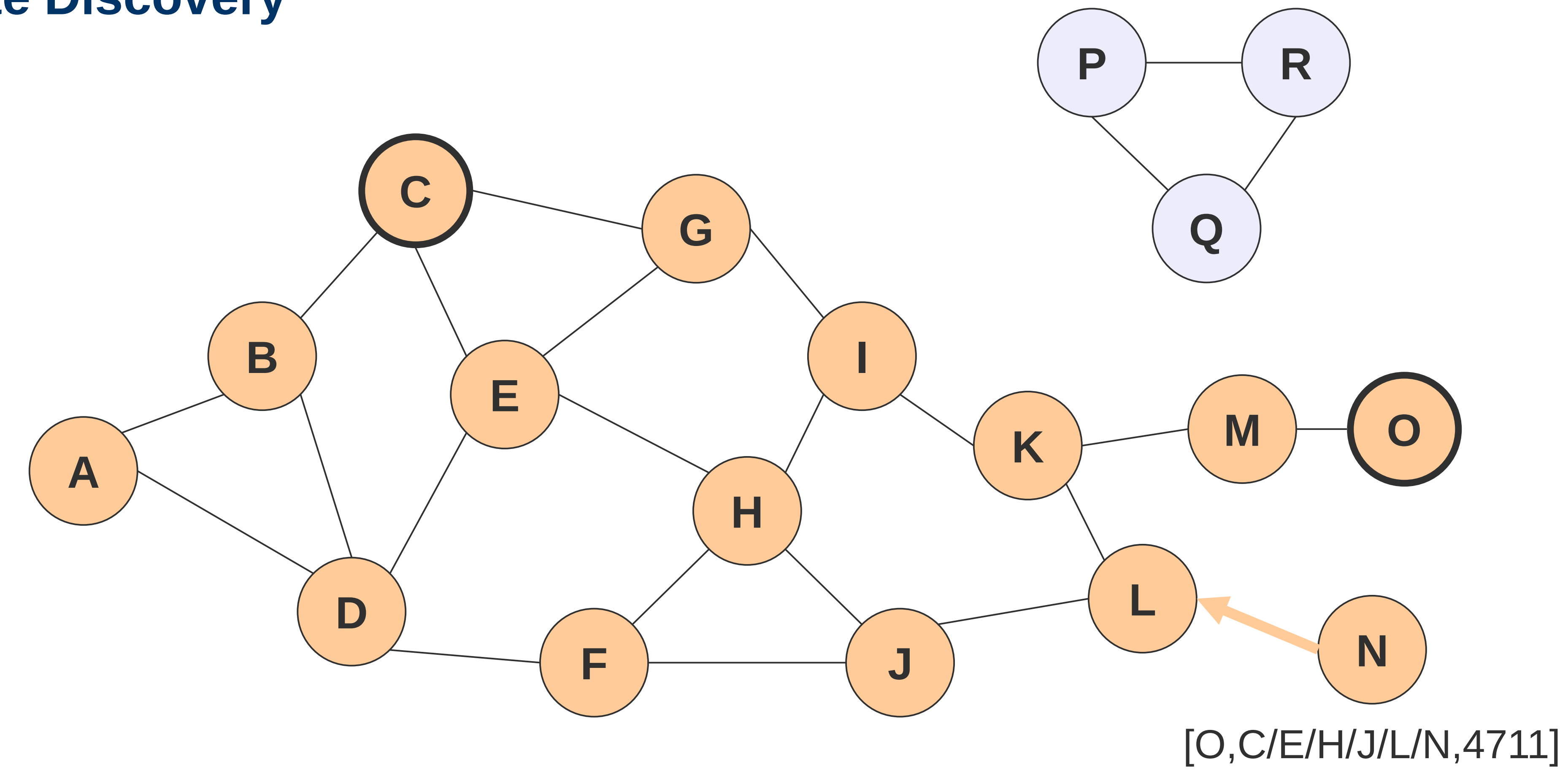
DSR: Route Discovery



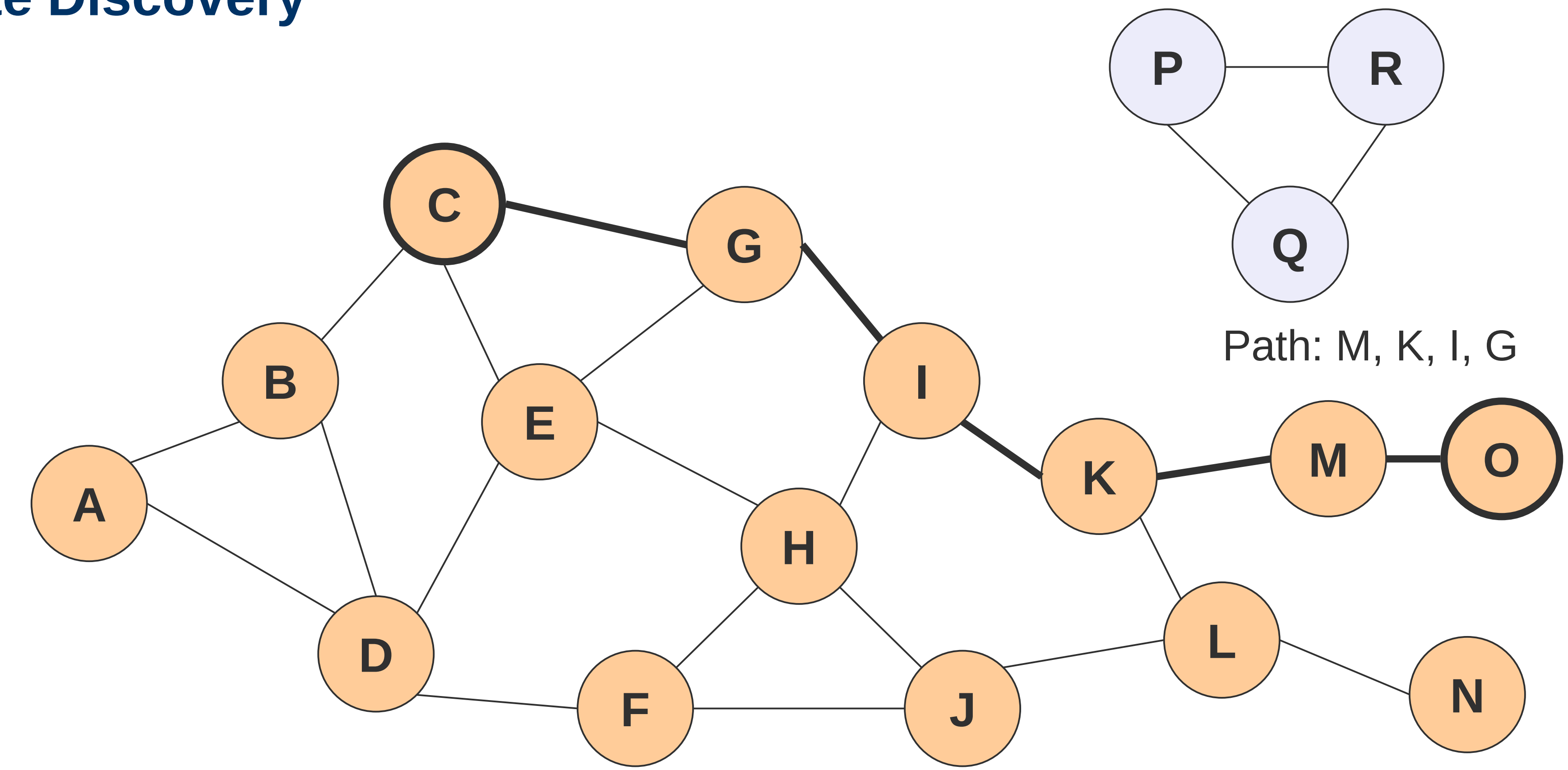
[O,C/E/H/J/L,4711]

(alternatively: [O,C/G/I/K/L,4711])

DSR: Route Discovery



DSR: Route Discovery



Path: M, K, I, G

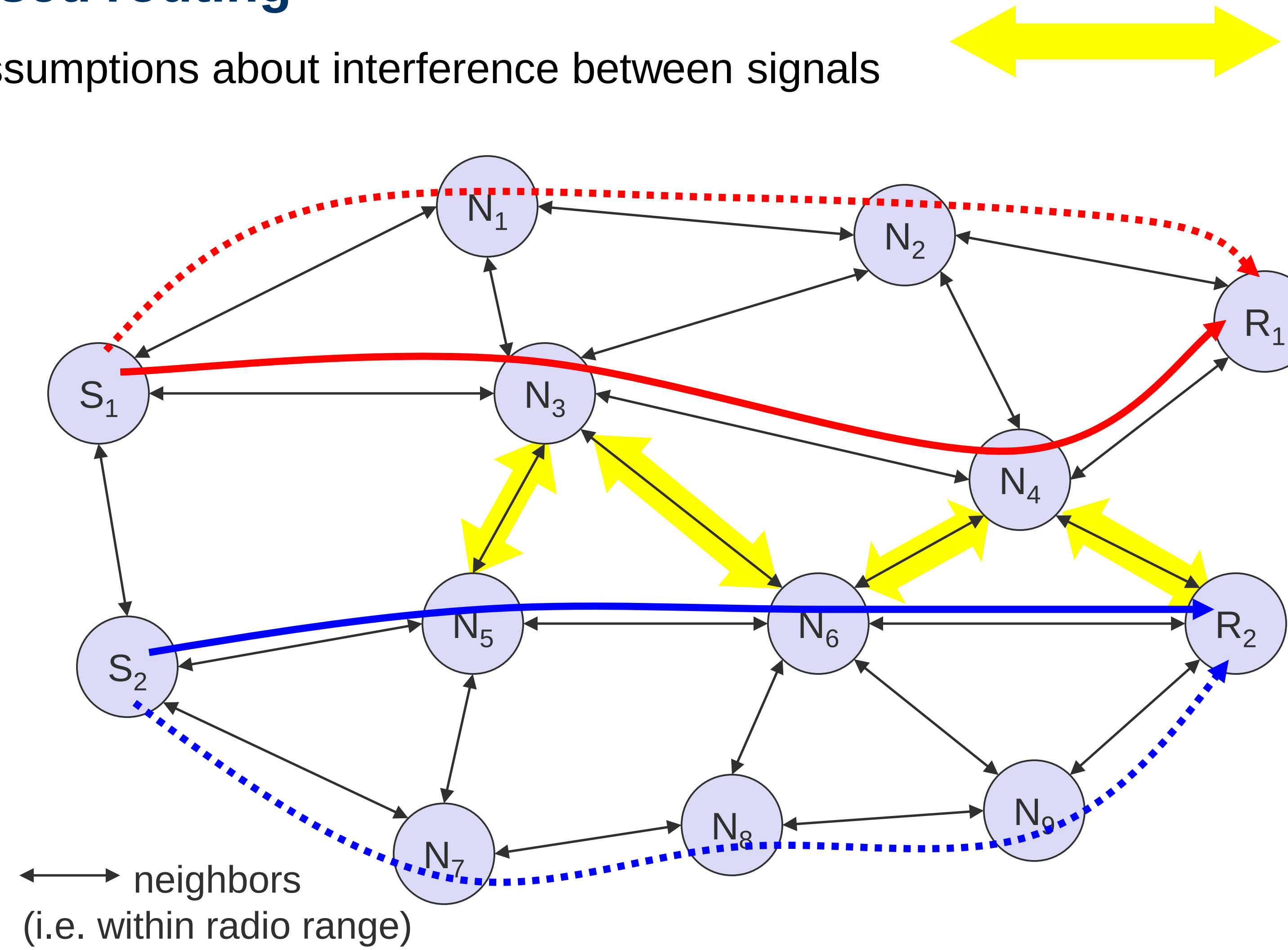
Dynamic Source Routing III

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

A plethora of 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

Further difficulties and 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

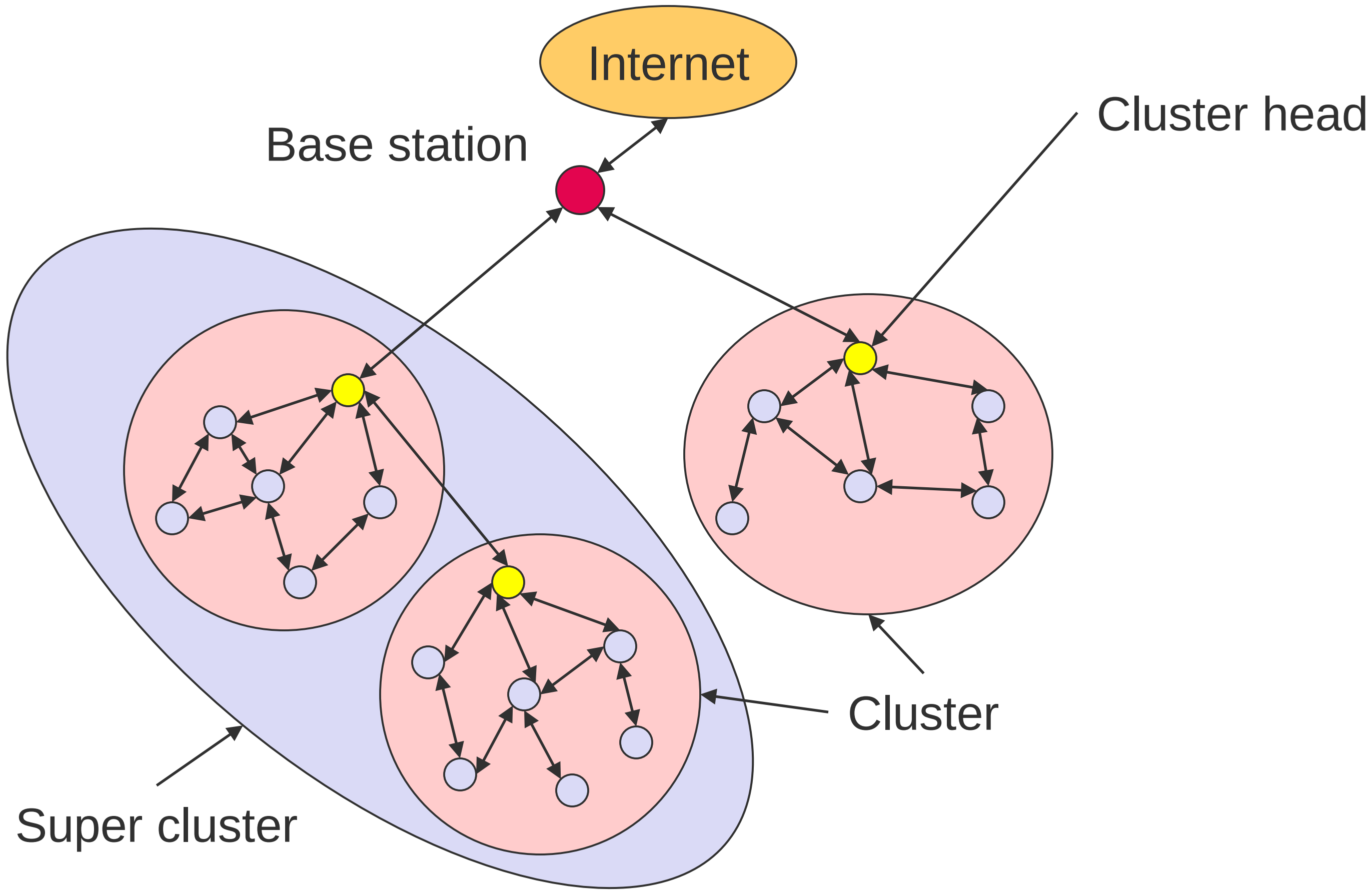
- Data integrity, protection from attacks (e.g. Denial of Service)

Scalability

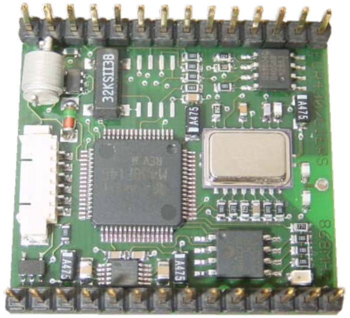
- 10 nodes? 100 nodes? 1000 nodes? 10000 nodes?

Integration with fixed networks

Clustering of ad-hoc networks



The next step: Wireless Sensor Networks (WSN)



Commonalities with MANETs

- Self-organization, multi-hop
- Typically wireless, should be energy efficient

Differences to MANETs

- *Applications:* MANET more powerful, more general ↔ WSN more specific
- *Devices:* MANET more powerful, higher data rates, more resources ↔ WSN rather limited, embedded, interacting with environment
- *Scale:* MANET rather small (some dozen devices) ↔ WSN can be large (thousands)
- *Basic paradigms:* MANET individual node important, ID centric ↔ WSN network important, individual node may be dispensable, data centric
- Mobility patterns, Quality-of Service, Energy, **Cost per node** …

Properties of wireless sensor networks

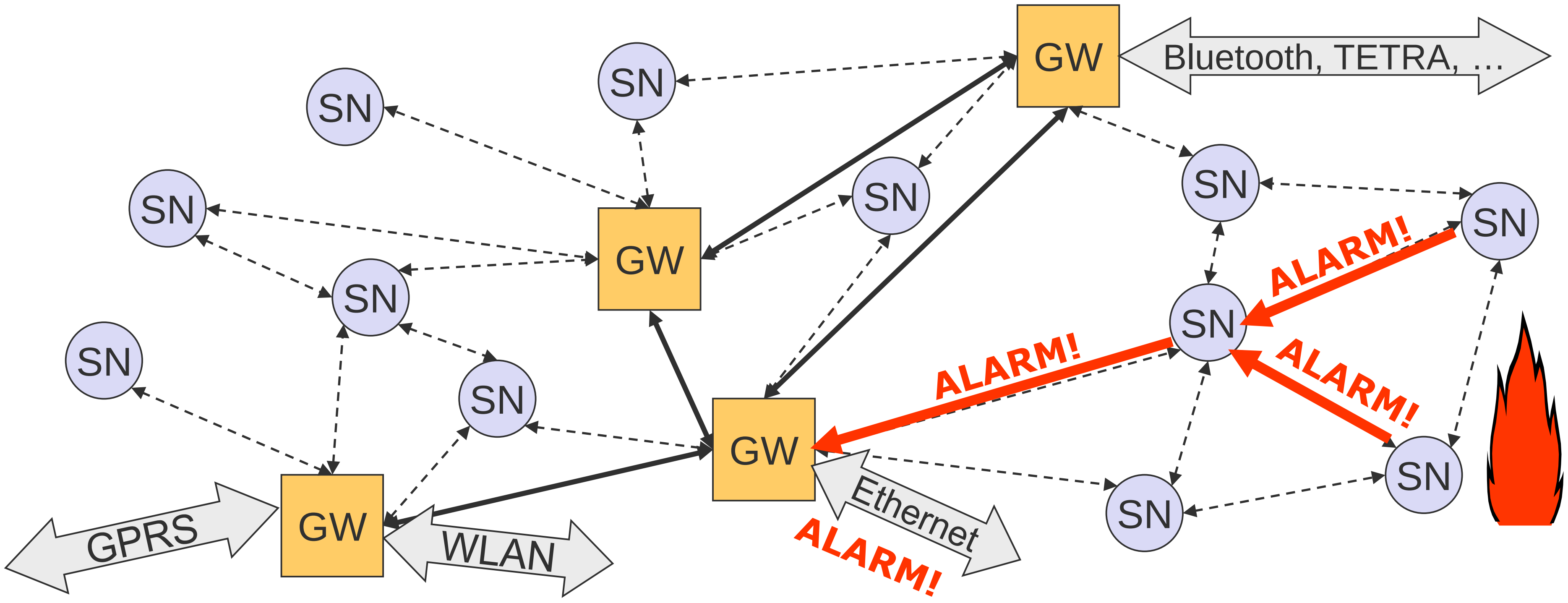
Sensor nodes (SN) monitor and control the environment

Nodes process data and forward data via radio

Integration into the environment, typically attached to other networks over a gateway (GW)

Network is self-organizing and energy efficient

Potentially high number of nodes at very low cost per node



Promising applications for WSNs

Machine and vehicle monitoring
- Sensor nodes in moveable parts
- Monitoring of hub temperatures, fluid levels …

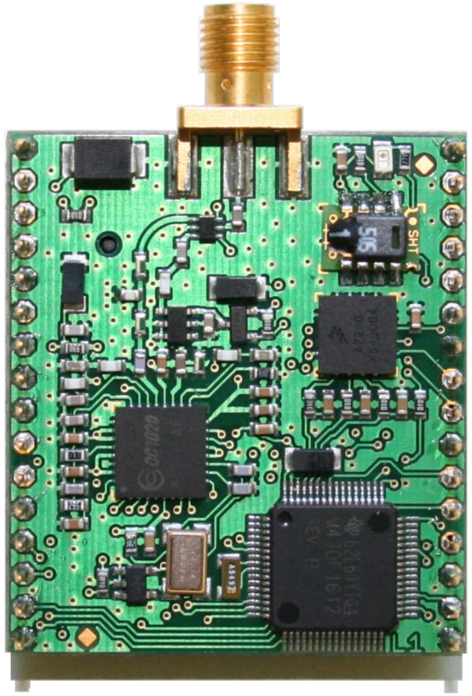
Health & medicine
- Long-term monitoring of patients with minimal restrictions
- Intensive care with relative great freedom of movement

Intelligent buildings, building monitoring
- Intrusion detection, mechanical stress detection
- Precision HVAC with individual climate

Environmental monitoring, person tracking
- Monitoring of wildlife and national parks
- Cheap and (almost) invisible person monitoring
- Monitoring waste dumps, demilitarized zones

… and many more: logistics (total asset management, RFID), telematics …
- WSNs are quite often complimentary to fixed networks!

Robust HW needed - example: Modular Sensor Board



Modular design

- Core module with controller, transceiver, SD-card slot
- Charging/programming/GPS/GPRS module
- Sensor carrier module

Software

- Firmware (C interface)
- RIOT, TinyOS, Contiki …
- Routing, management, flashing …
- ns-2 simulation models
- Integration into Visual Studio, Eclipse, LabVIEW, Robotics Studio …

Sensors attached on demand

- Acceleration, humidity, temperature, luminosity, noise detection, vibration, PIR movement detection…

Example: Evolution of different sensor nodes

Certified nodes

- Fully certified according to international regulations
- Range > 1.5 km (LOS), > 500m in buildings
- < 100µA while still running (no sensors, no RF)
- Can drive external sensors up to 500mA (analog/digital)
- SPI, serial, I²C, display, camera, joystick interfaces

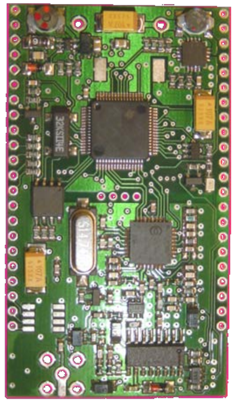
Gateways

- Bluetooth, WLAN, Ethernet, serial, USB,
  RS485, GSM/GPRS

Software

- Auto-configuration, GPS tracking,
  over-the-air programming, building monitoring, …

Evaluation boards



Current developments

RiotOS

- The friendly Operating System for the Internet of Things
- microkernel architecture and a tickless scheduler for very lightweight devices, real-time, multi-threading
- http://www.riot-os.org

VIVE

- Distributed event detection
- Examples: bridge monitoring, rehabilitation
- http://www.mi.fu-berlin.de/inf/groups/ag-tech/projects/VIVE/index.html

Example Application: Habitat Monitoring/Skomer Island UK

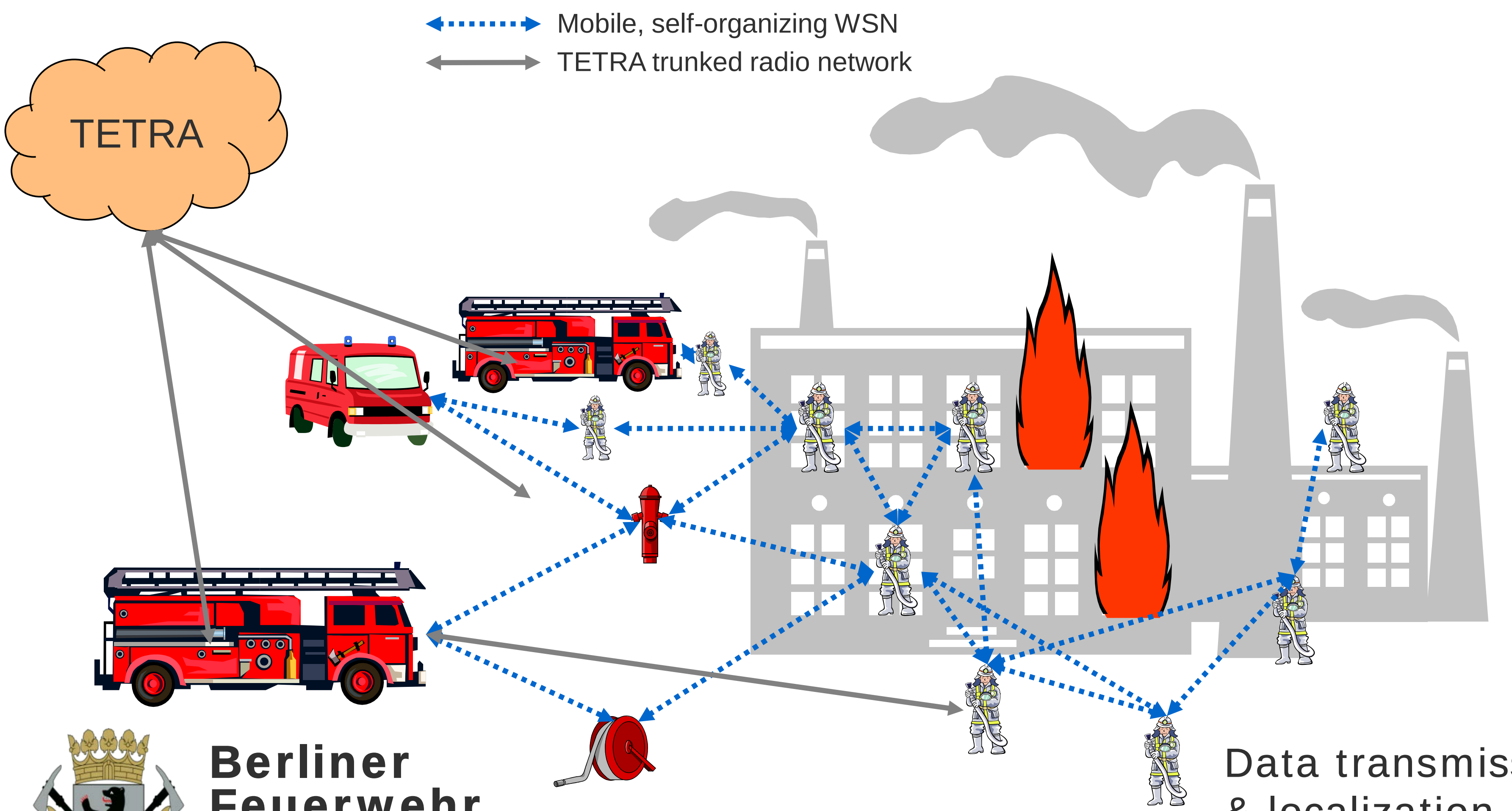
Manx Shearwater

Combination of RFID and ScatterWeb

Main challenge: robustness, reliability, easy-to-use

Joint project with Oxford University and MSRC

Project FeuerWhere – the extreme challenge



Berliner Feuerwehr
4450 fire fighters
300000 incidents/year (8000 fires)

Data transmission & localization