Mobile Communications
Network Protocols/Mobile IP

- Motivation
- Data transfer , Encapsulation
- Security, IPv6, Problems
- Micro mobility support
- DHCP
- Ad-hoc networks, Routing protocols

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

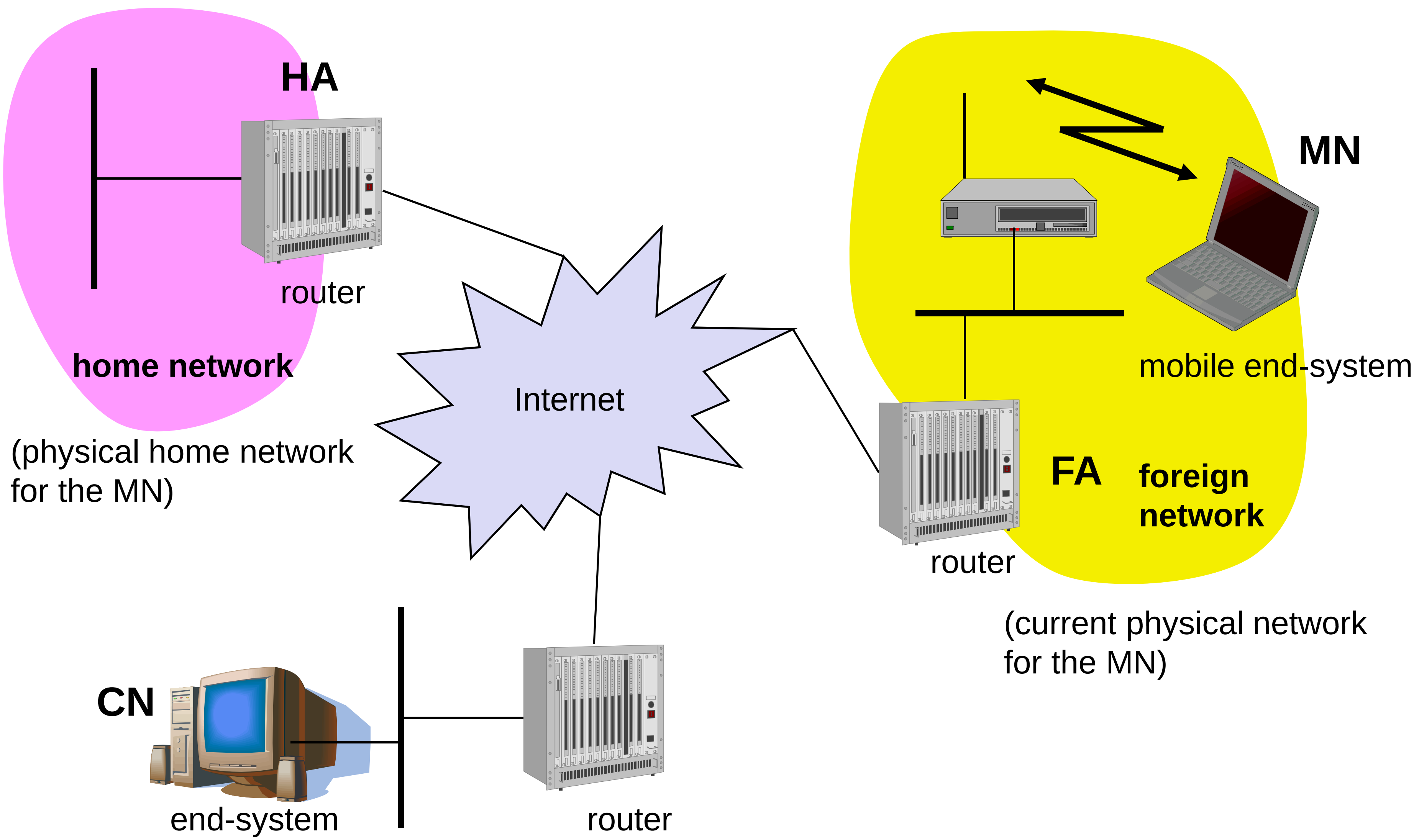
Requirements for Mobile IPv4 (RFC 3344, was: 3220, was: 2002 , updated by: 4721)

- 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

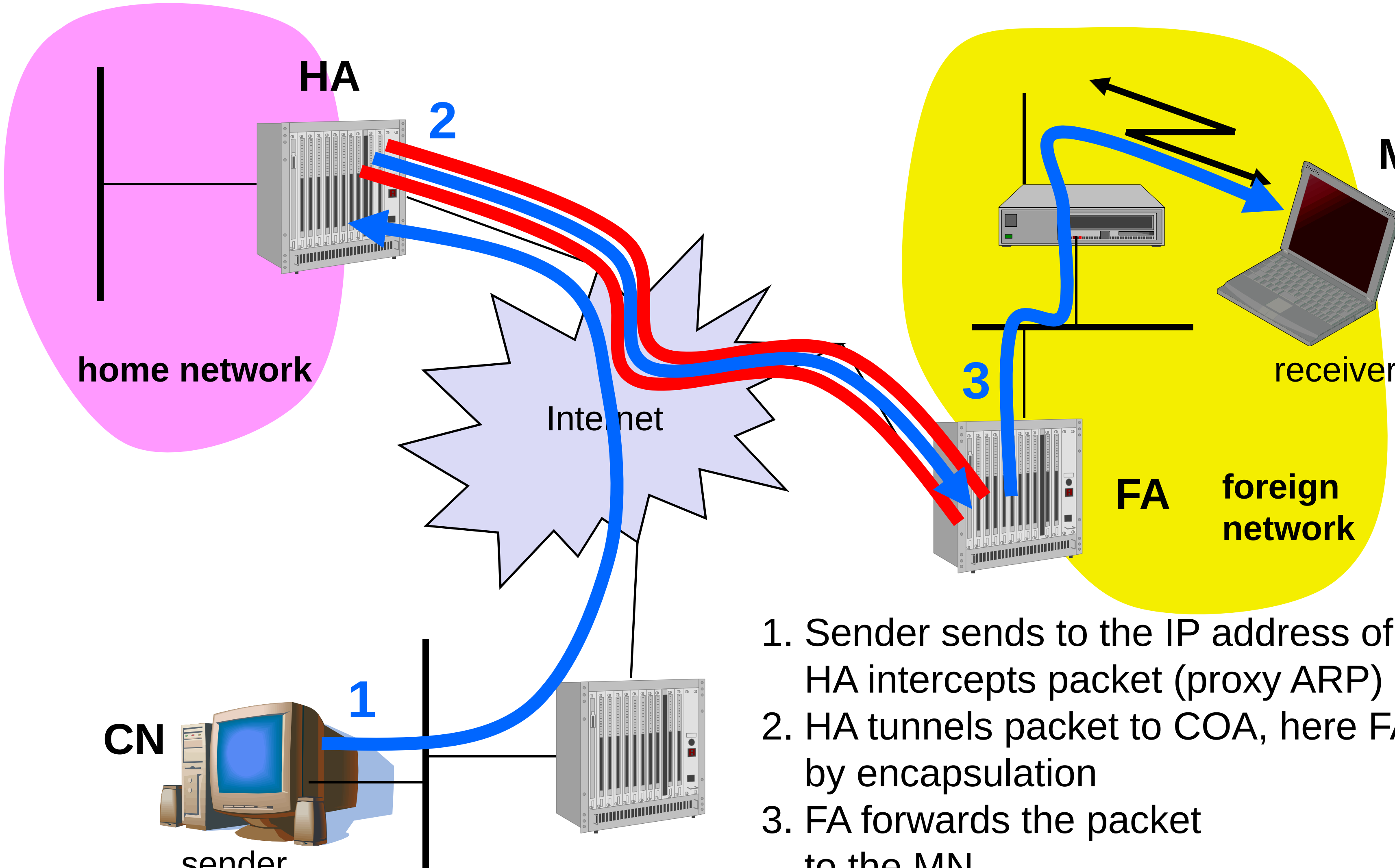
Terminology

- 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

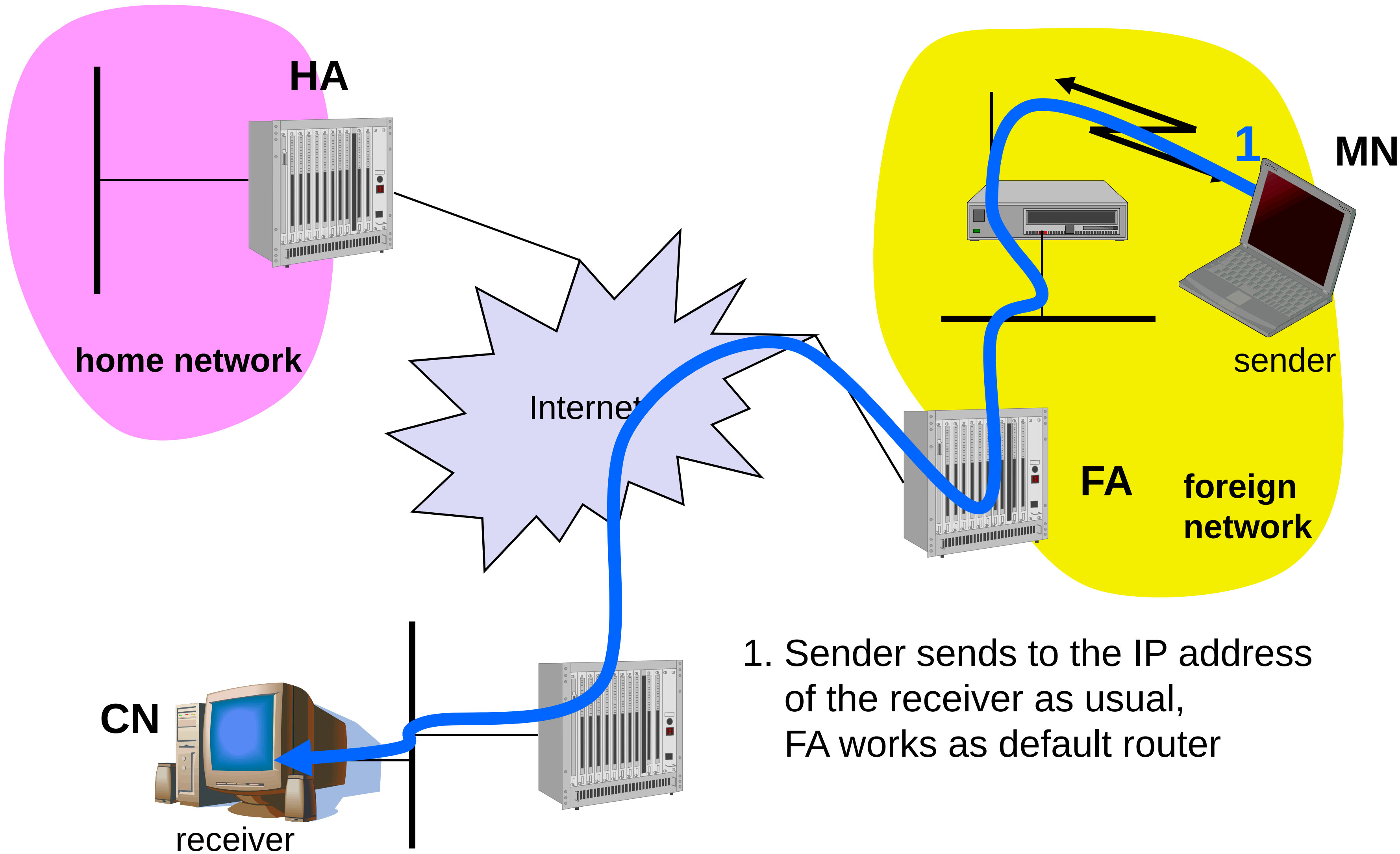


Data transfer to the mobile system



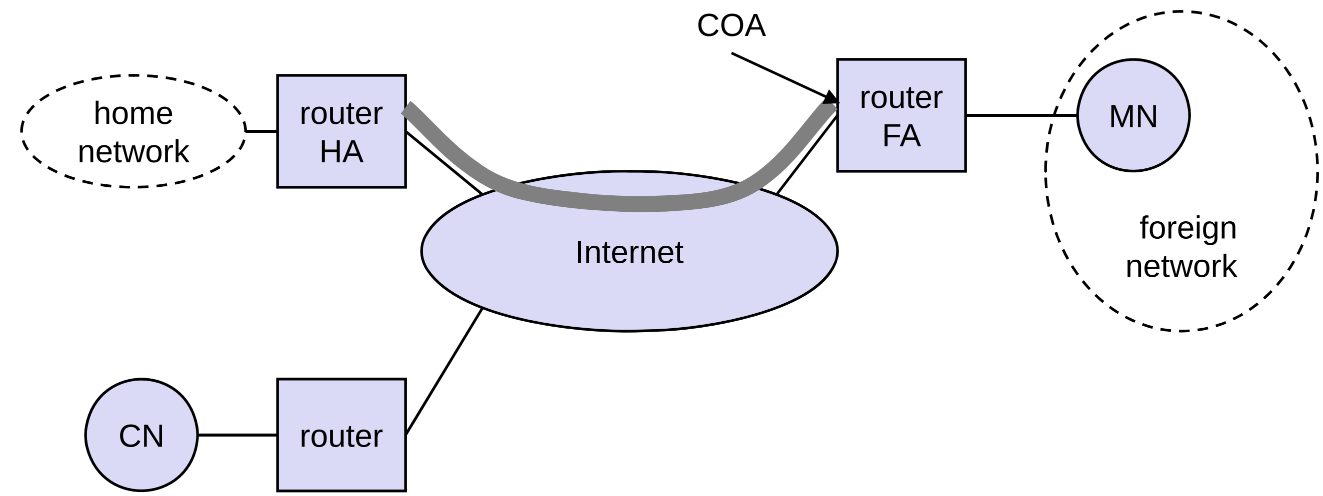
1. Sender sends to the IP address of MN, HA intercepts packet (proxy ARP)
2. HA tunnels packet to COA, here FA, by encapsulation
3. FA forwards the packet to the MN

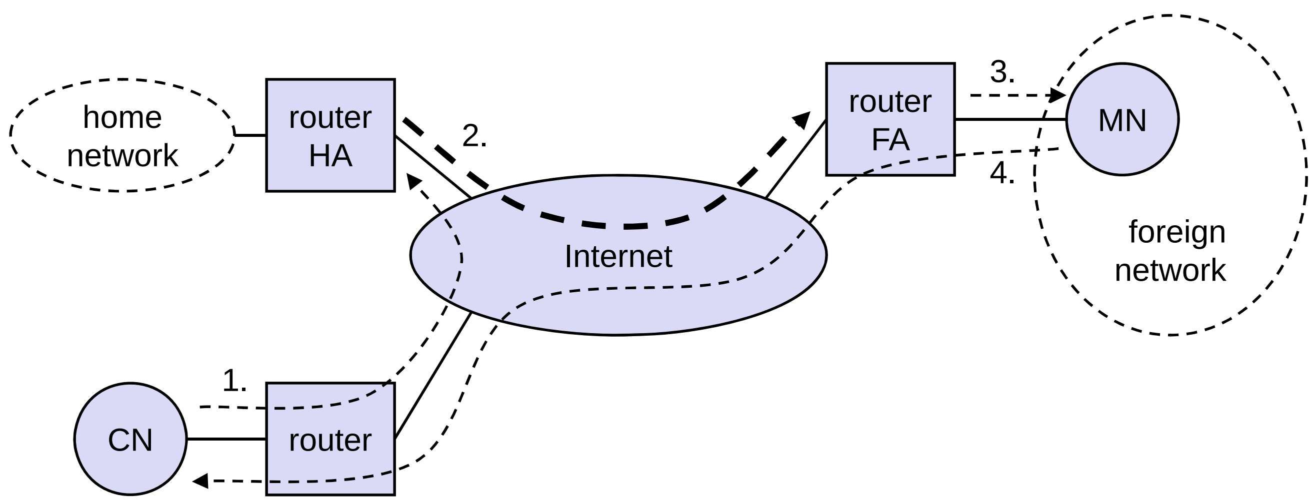
Data transfer from the mobile system



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

Overview

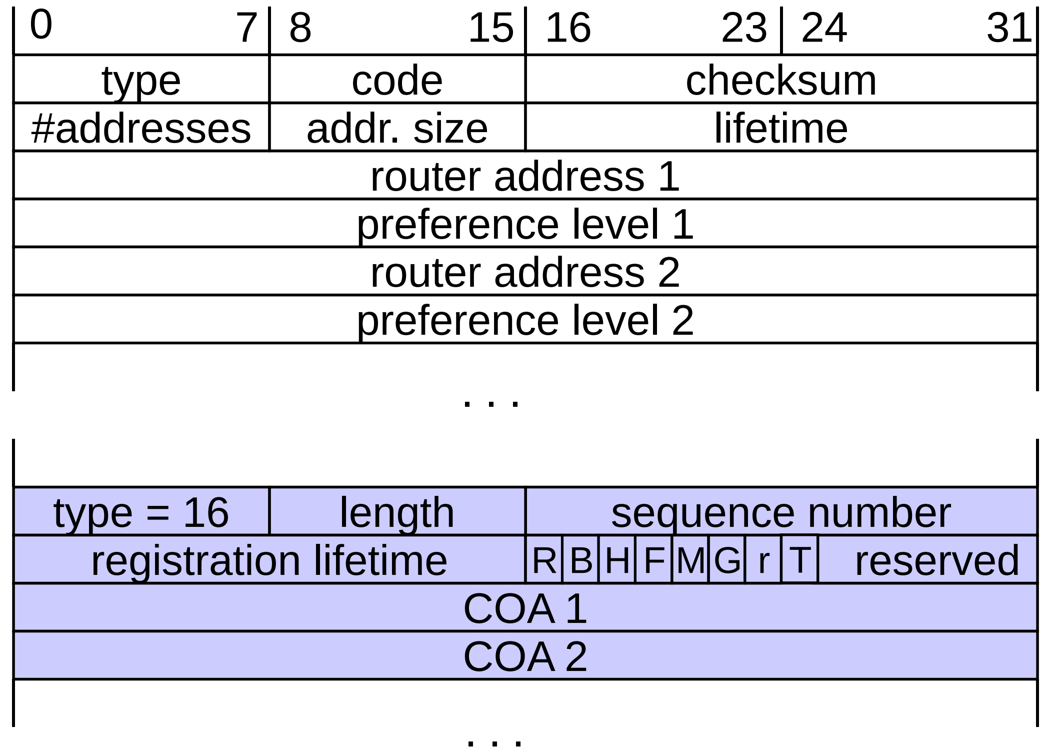

COA
home
network
router
HA
router
FA
MN
Internet
foreign
network
CN
router


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

Network integration

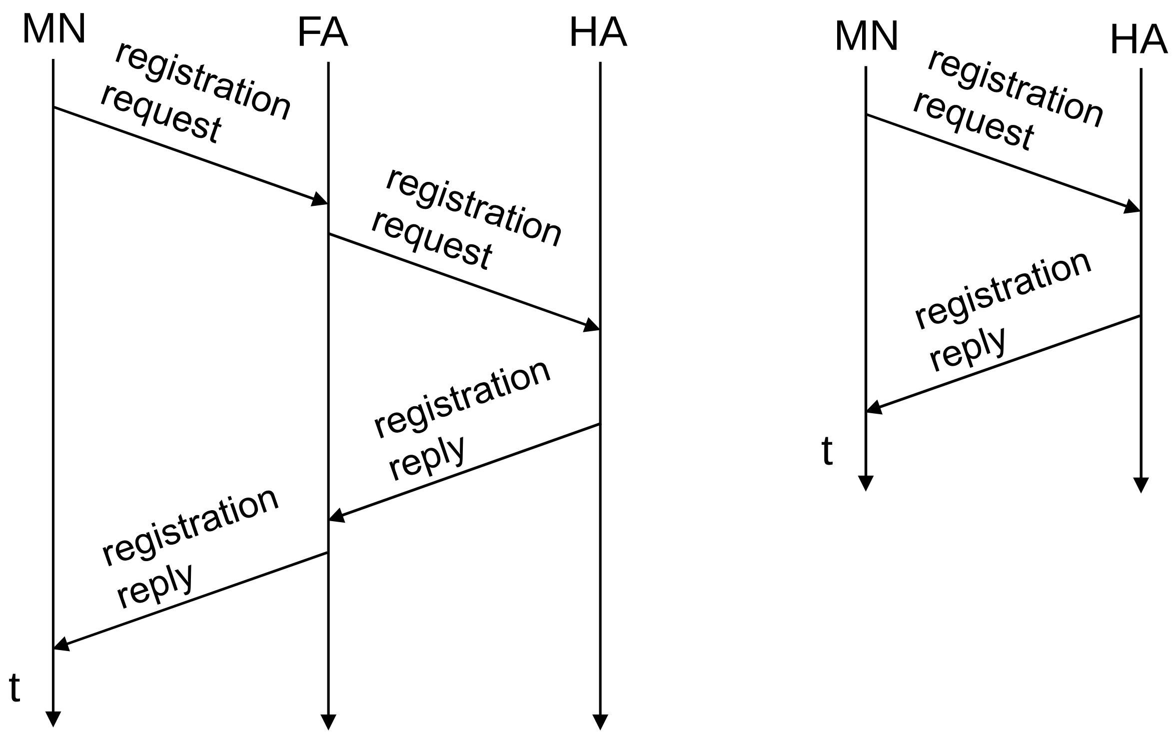
- Agent Advertisement
  - HA and FA periodically send advertisement messages into their physical subnets
  - MN listens to these messages and detects, if it is in the home or a foreign network (standard case for home network)
  - MN reads a COA from the FA advertisement messages
- Registration (always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

Agent advertisement

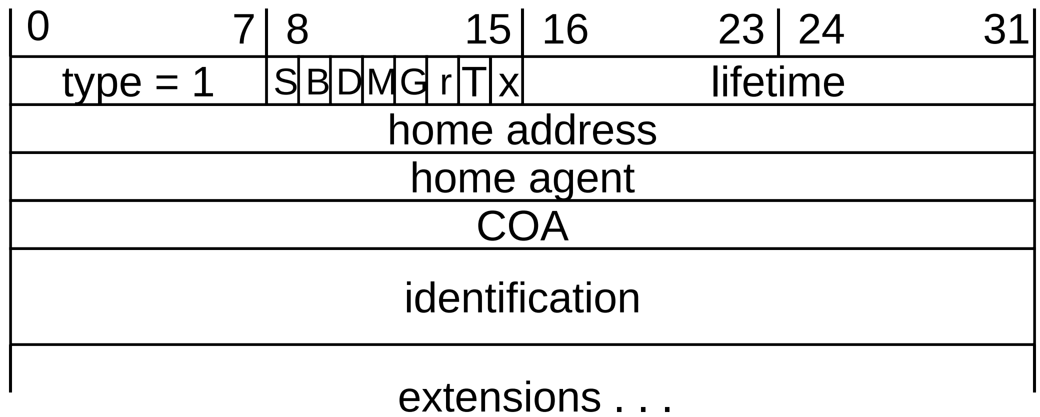


type = 16
length = 6 + 4 * #COAs
R: registration required
B: busy, no more registrations
H: home agent
F: foreign agent
M: minimal encapsulation
G: GRE encapsulation
r: =0, ignored (former Van Jacobson compression)
T: FA supports reverse tunneling
reserved: =0, ignored

Registration



Mobile IP registration request



S: simultaneous bindings
B: broadcast datagrams
D: decapsulation by MN
M mininal encapsulation
G: GRE encapsulation
r: =0, ignored
T: reverse tunneling requested
x: =0, ignored

Mobile IP registration reply

0 – 7	8 – 15	16 – 31
type = 3	code	lifetime
home address		
home agent		
identification		
extensions . . .		

Example codes:

registration successful

- 0 registration accepted
- 1 registration accepted, but simultaneous mobility bindings unsupported

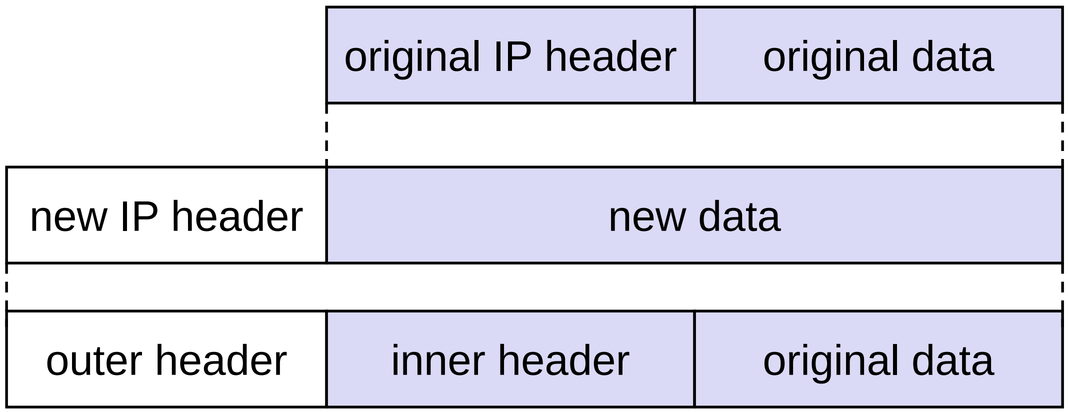
registration denied by FA

- 65 administratively prohibited
- 66 insufficient resources
- 67 mobile node failed authentication
- 68 home agent failed authentication
- 69 requested Lifetime too long

registration denied by HA

- 129 administratively prohibited
- 131 mobile node failed authentication
- 133 registration Identification mismatch
- 135 too many simultaneous mobility bindings

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

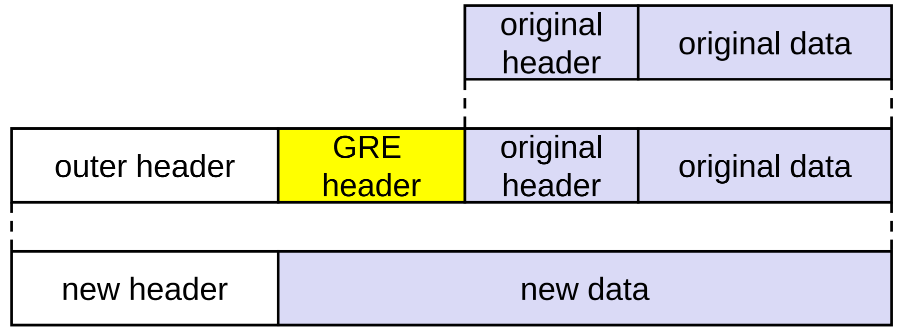
<table>
<tr><td>ver.</td><td>IHL</td><td>DS (TOS)</td><td colspan="2">length</td></tr>
<tr><td colspan="3">IP identification</td><td>flags</td><td>fragment offset</td></tr>
<tr><td colspan="2">TTL</td><td>IP-in-IP</td><td colspan="2">IP checksum</td></tr>
<tr><td colspan="5">IP address of HA</td></tr>
<tr><td colspan="5">Care-of address COA</td></tr>
<tr><td>ver.</td><td>IHL</td><td>DS (TOS)</td><td colspan="2">length</td></tr>
<tr><td colspan="3">IP identification</td><td>flags</td><td>fragment offset</td></tr>
<tr><td colspan="2">TTL</td><td>lay. 4 prot.</td><td colspan="2">IP checksum</td></tr>
<tr><td colspan="5">IP address of CN</td></tr>
<tr><td colspan="5">IP address of MN</td></tr>
<tr><td colspan="5">TCP/UDP/ ... payload</td></tr>
</table>

Encapsulation II

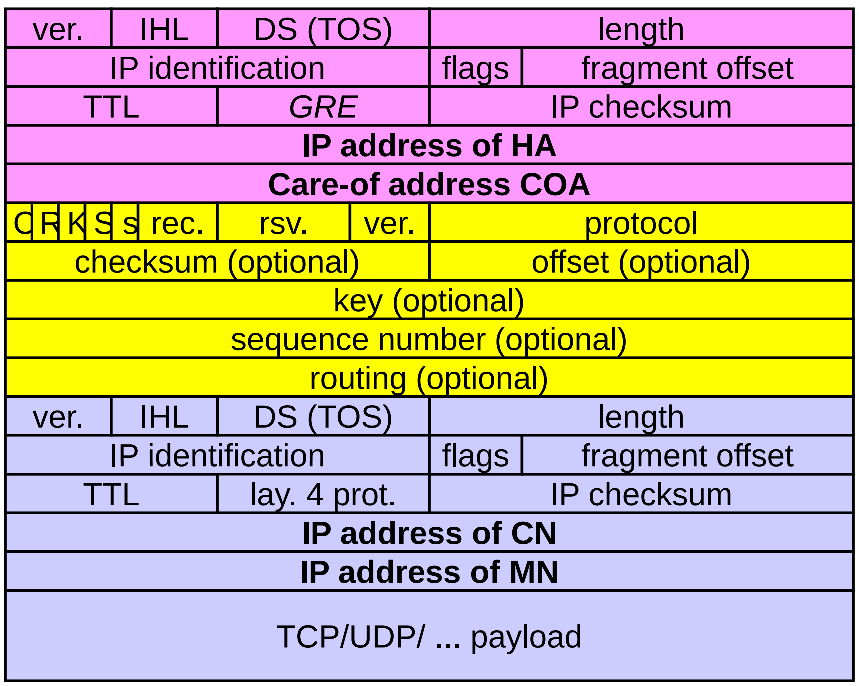
- Minimal encapsulation (optional)
  - avoids repetition of identical fields
  - e.g. TTL, IHL, version, DS (RFC 2474, old: TOS)
  - only applicable for non fragmented packets, no space left for fragment identification

<table>
<tr><td>ver.</td><td>IHL</td><td colspan="2">DS (TOS)</td><td colspan="2">length</td></tr>
<tr><td colspan="4">IP identification</td><td>flags</td><td>fragment offset</td></tr>
<tr><td colspan="2">TTL</td><td colspan="2">min. encap.</td><td colspan="2">IP checksum</td></tr>
<tr><td colspan="6">IP address of HA</td></tr>
<tr><td colspan="6">care-of address COA</td></tr>
<tr><td colspan="2">lay. 4 protoc.</td><td>S</td><td>reserved</td><td colspan="2">IP checksum</td></tr>
<tr><td colspan="6">IP address of MN</td></tr>
<tr><td colspan="6">original sender IP address (if S=1)</td></tr>
<tr><td colspan="6">TCP/UDP/ ... payload</td></tr>
</table>

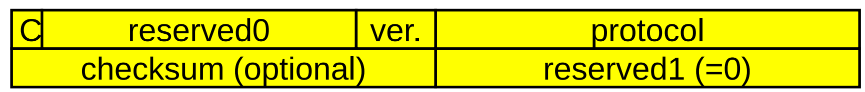
Generic Routing Encapsulation



RFC 1701



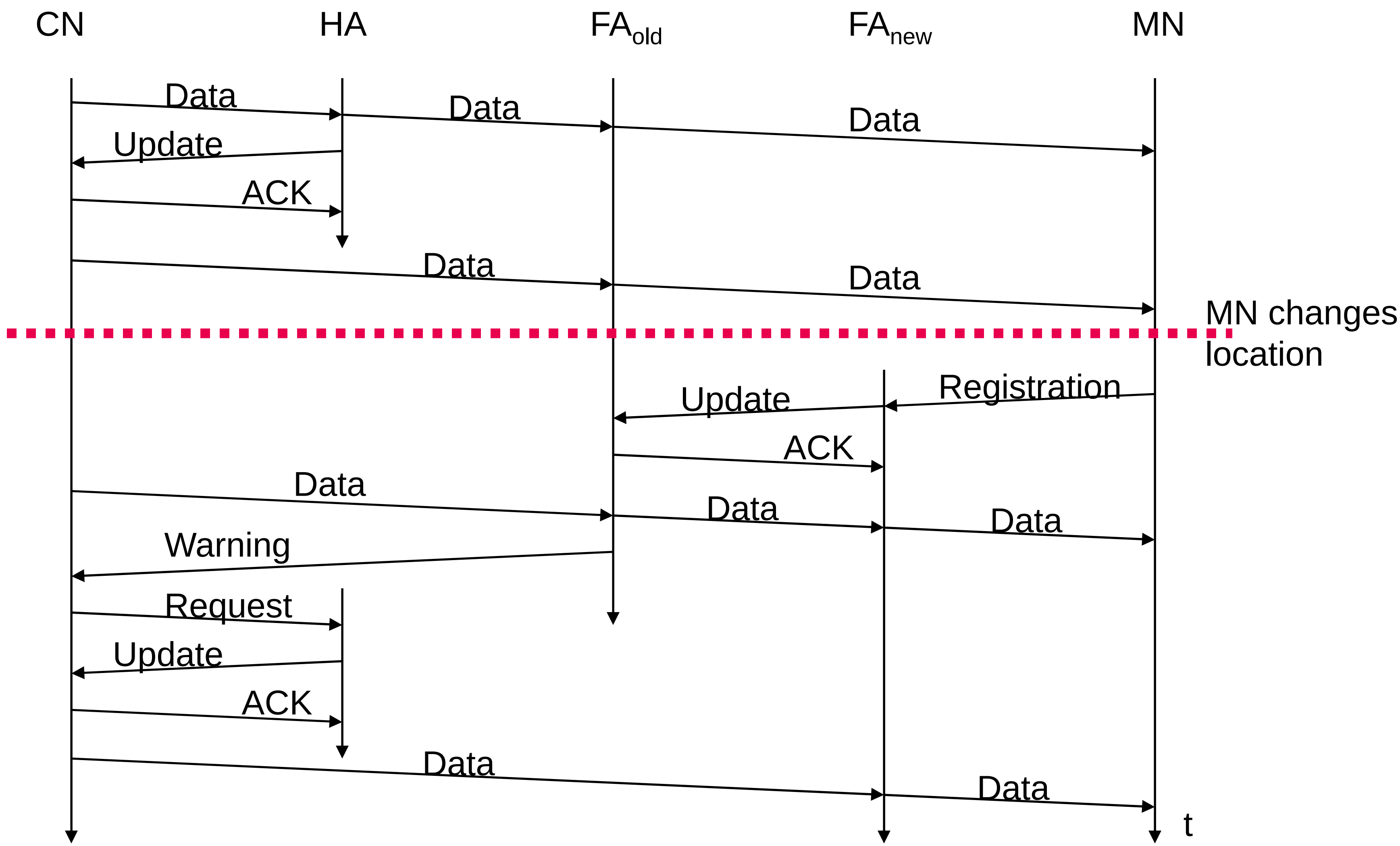
RFC 2784 (updated by 2890)



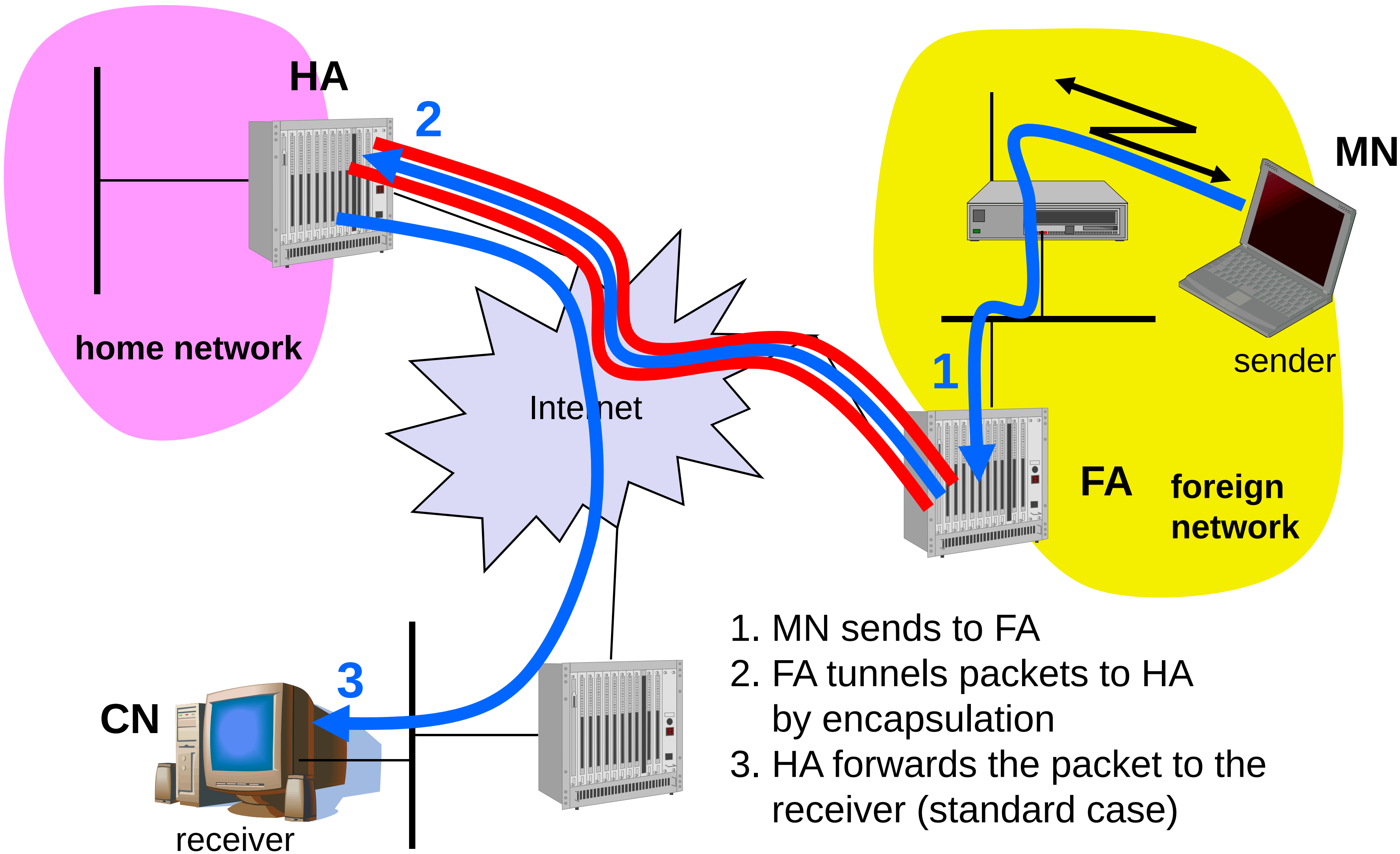
Optimization of packet forwarding

- 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 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

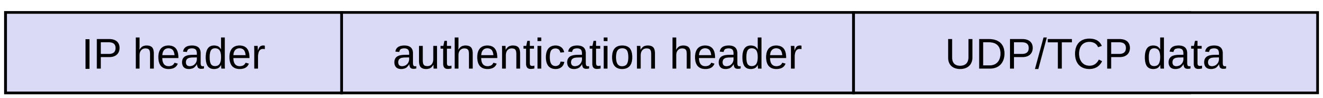
- Security
  - authentication with FA problematic, for the FA typically belongs to another organization
  - no protocol for key management and key distribution has been standardized in the Internet
  - patent and export restrictions
- Firewalls
  - typically mobile IP cannot be used together with firewalls, 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

Security in Mobile IP

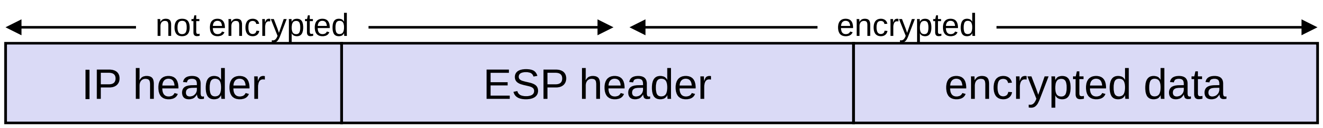
- Security requirements (Security Architecture for the Internet Protocol, RFC 4301, was: 1825, 2401)
  - Integrity
    any changes to data between sender and receiver can be detected by the receiver
  - Authentication
    sender address is really the address of the sender and all data received is really data sent by this sender
  - Confidentiality
    only sender and receiver can read the data
  - Non-Repudiation
    sender cannot deny sending of data
  - Traffic Analysis
    creation of traffic and user profiles should not be possible
  - Replay Protection
    receivers can detect replay of messages

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

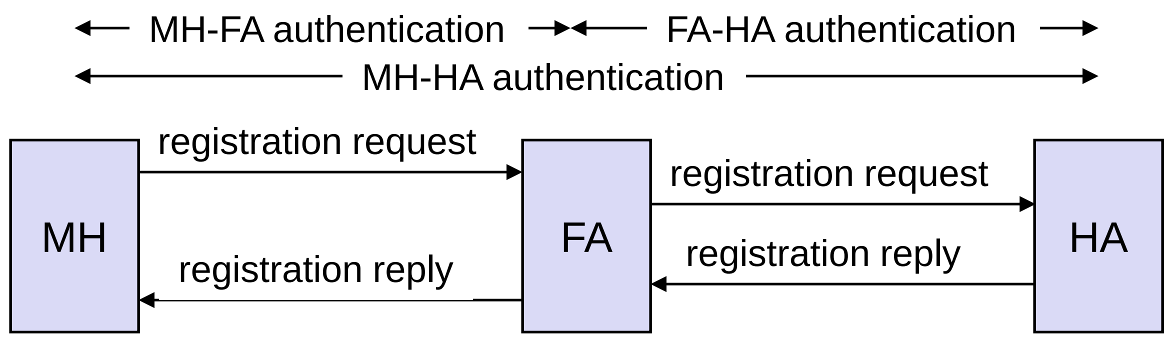


  - Encapsulation Security Payload
    - protects confidentiality between communication partners



IP security architecture II

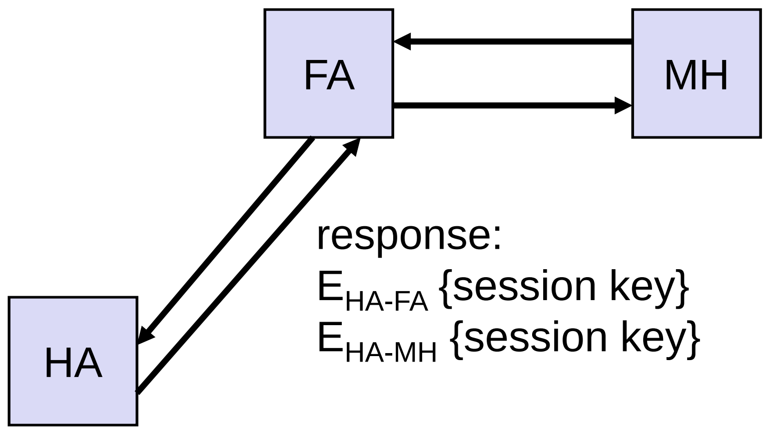
- Mobile Security Association for registrations
  - parameters for the mobile host (MH), home agent (HA), and foreign agent (FA)
- Extensions of the IP security architecture
  - extended authentication of registration



  - 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

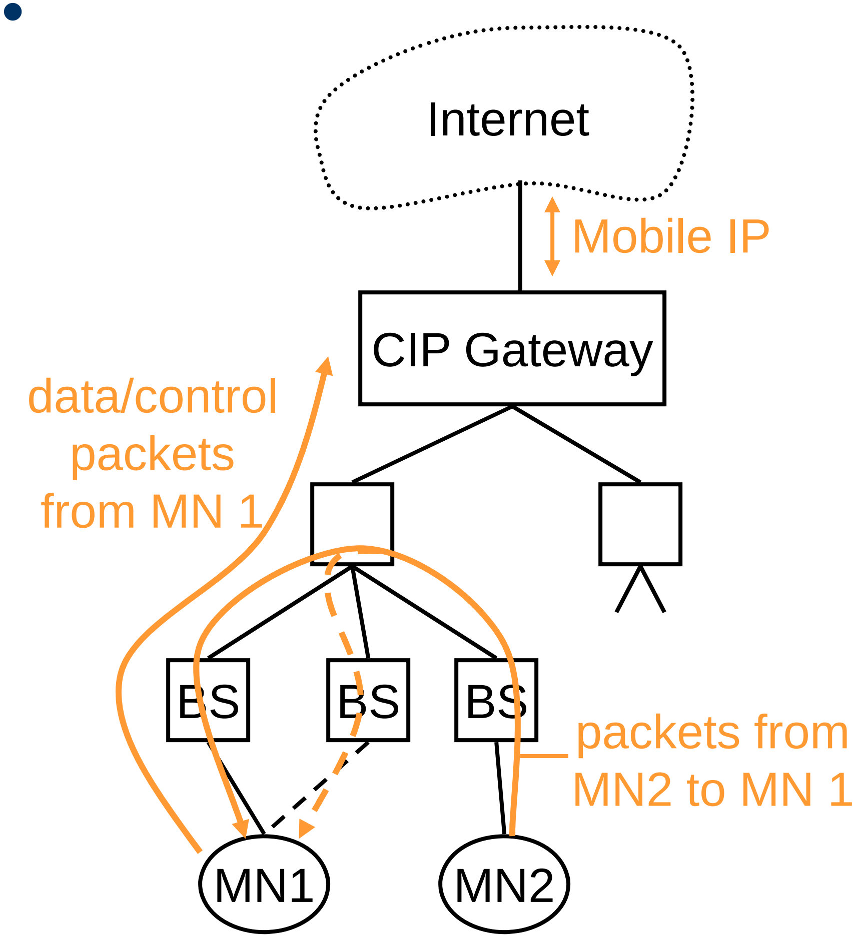
- Micro-mobility support:
  - Efficient local handover inside a foreign domain without involving a home agent
  - Reduces control traffic on backbone
  - Especially needed in case of route optimization

- 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 MNs are authenticated
  - Replay-protection (using timestamps)

- Potential problems:
  - MNs 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

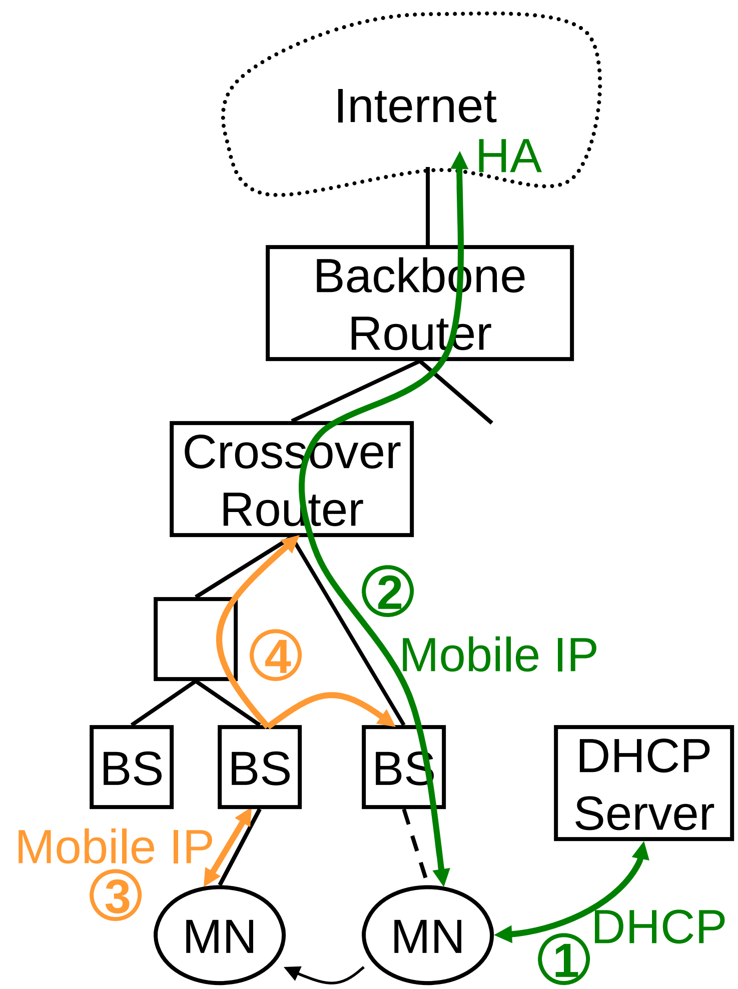
- Advantages:
  - Simple and elegant architecture
  - Mostly self-configuring (little management needed)
  - Integration with firewalls / private address support possible

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

HAWAII

- Operation:
  - MN obtains co-located COA ① and registers with HA ②
  - Handover: MN keeps COA, ③ new BS answers Reg. Request ④ and updates routers
  - MN views BS as foreign agent

- Security provisions:
  - MN-FA authentication mandatory
  - Challenge/Response Extensions mandatory



HAWAII: Security

- Advantages:
  - Mutual authentication and C/R extensions mandatory
  - Only infrastructure components can influence routing entries

- Potential problems:
  - Co-located COA raises DHCP security issues
    (DHCP has no strong authentication)
  - Decentralized security-critical functionality
    (Mobile IP registration processing during handover)
    in base stations
  - Authentication of HAWAII protocol messages unspecified
    (potential attackers: stationary nodes in foreign network)
  - MN authentication requires PKI or AAA infrastructure

HAWAII: Other issues

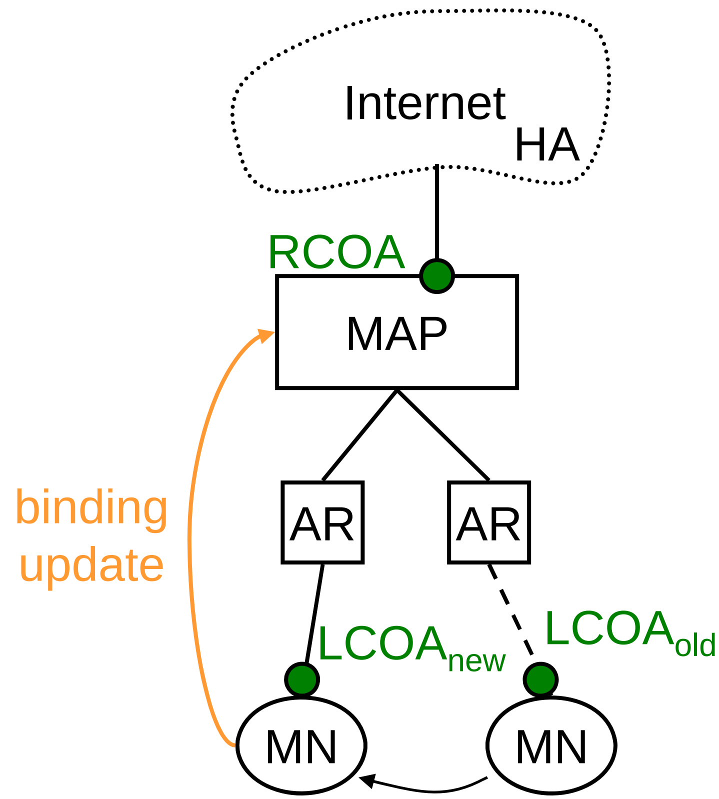
- Advantages:
  - Mostly transparent to MNs
    (MN sends/receives standard Mobile IP messages)
  - Explicit support for dynamically assigned home addresses

- Potential problems:
  - Mixture of co-located COA and FA concepts may not be supported by some MN implementations
  - No private address support possible
    because of co-located COA

Hierarchical Mobile IPv6 (RFC 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



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)

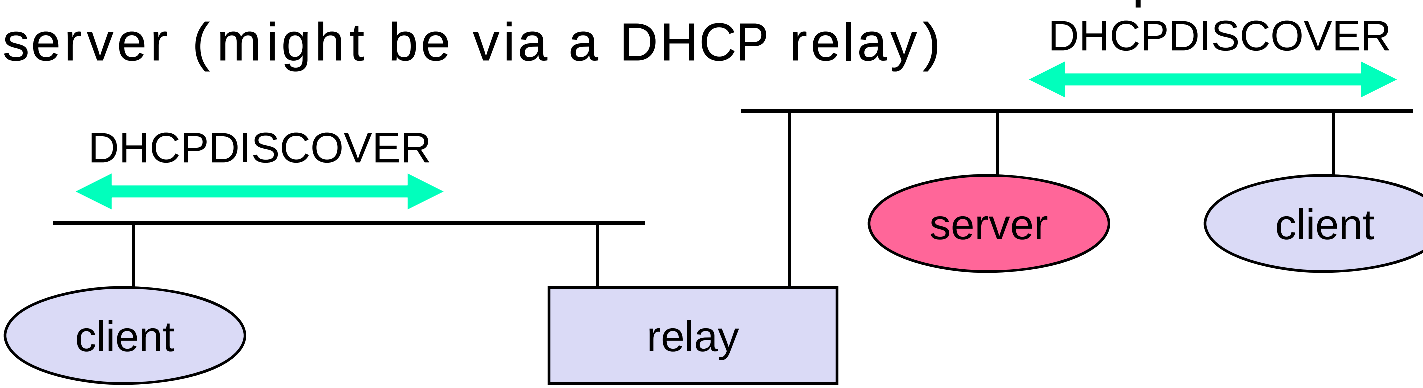
Hierarchical Mobile IP: Other issues

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

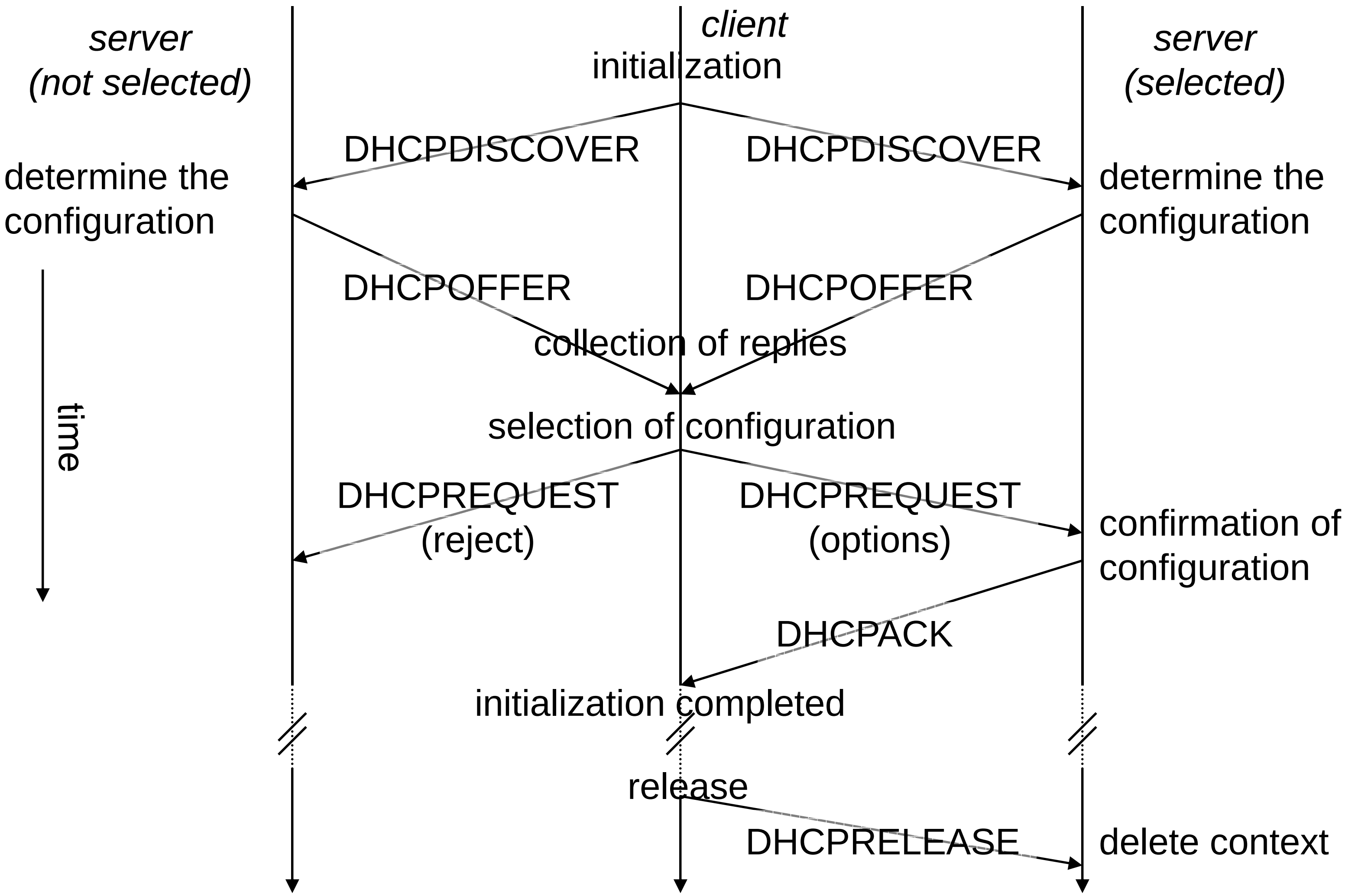
- Potential problems:
  - Not transparent to MNs
  - Handover efficiency in wireless mobile scenarios:
    - Complex MN operations
    - All routing reconfiguration messages sent over wireless link

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

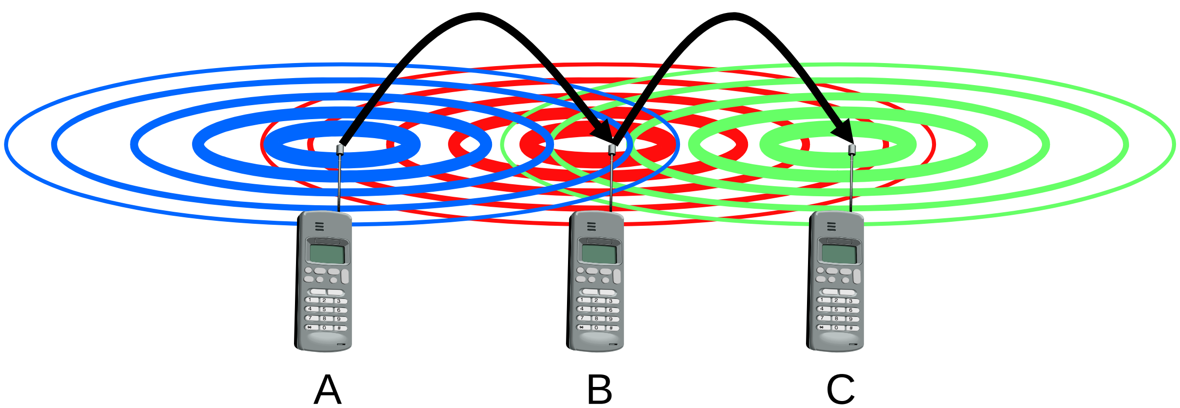


DHCP characteristics

- 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

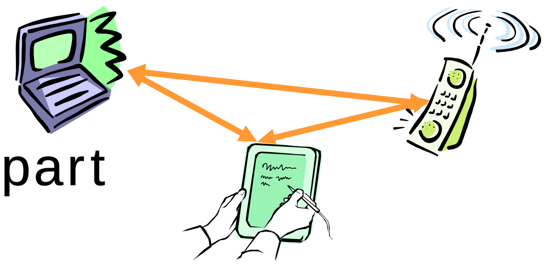
- Standard Mobile IP needs an infrastructure
  - Home Agent/Foreign Agent in the fixed network
  - DNS, routing etc. are not designed for mobility
- Sometimes there is no infrastructure!
  - remote areas, ad-hoc meetings, disaster areas
  - cost can also be an argument against an infrastructure!
- Main 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

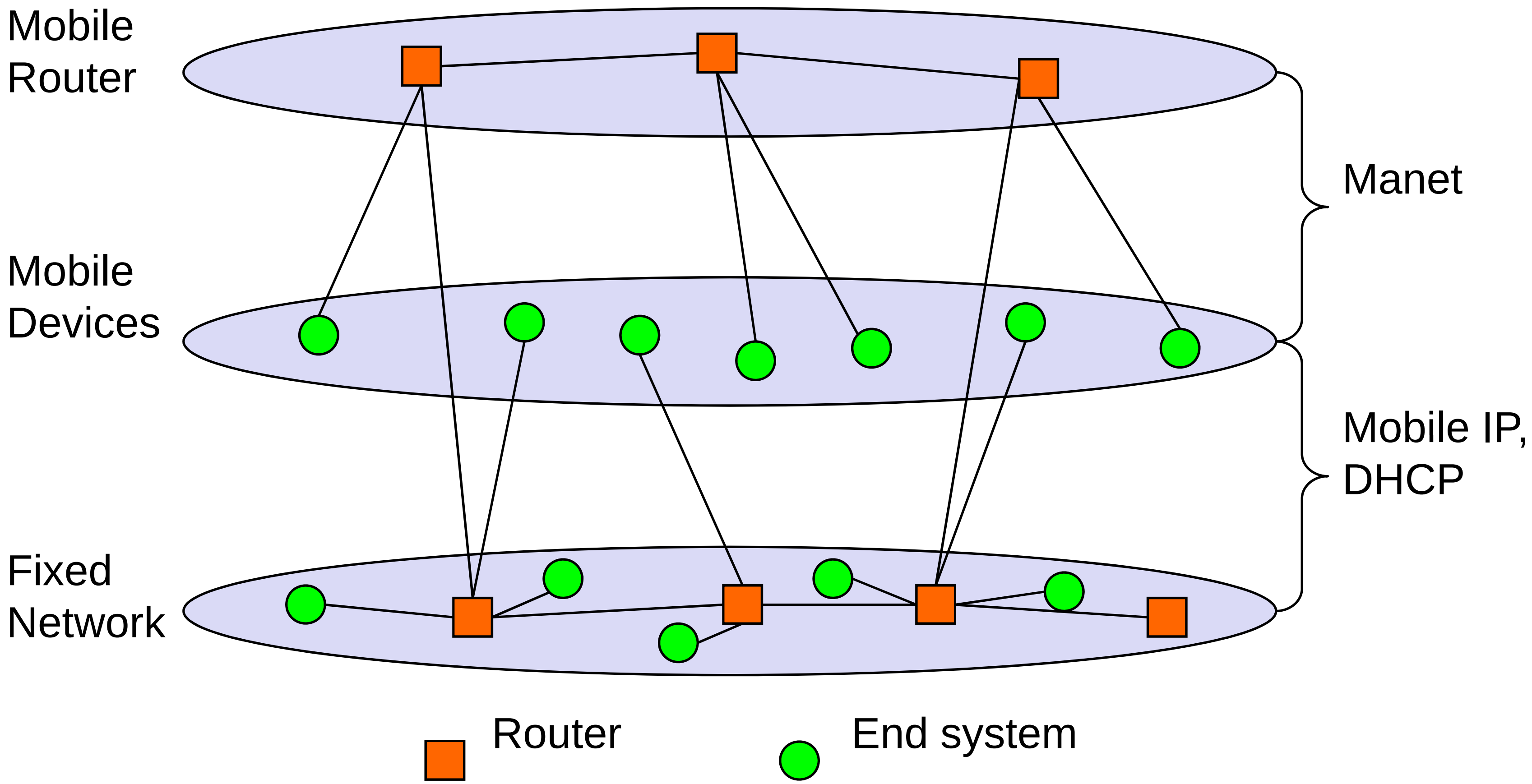
- Examples
  - Single-hop: All partners max. one hop apart
    - Bluetooth piconet, PDAs in a room, gaming devices…



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

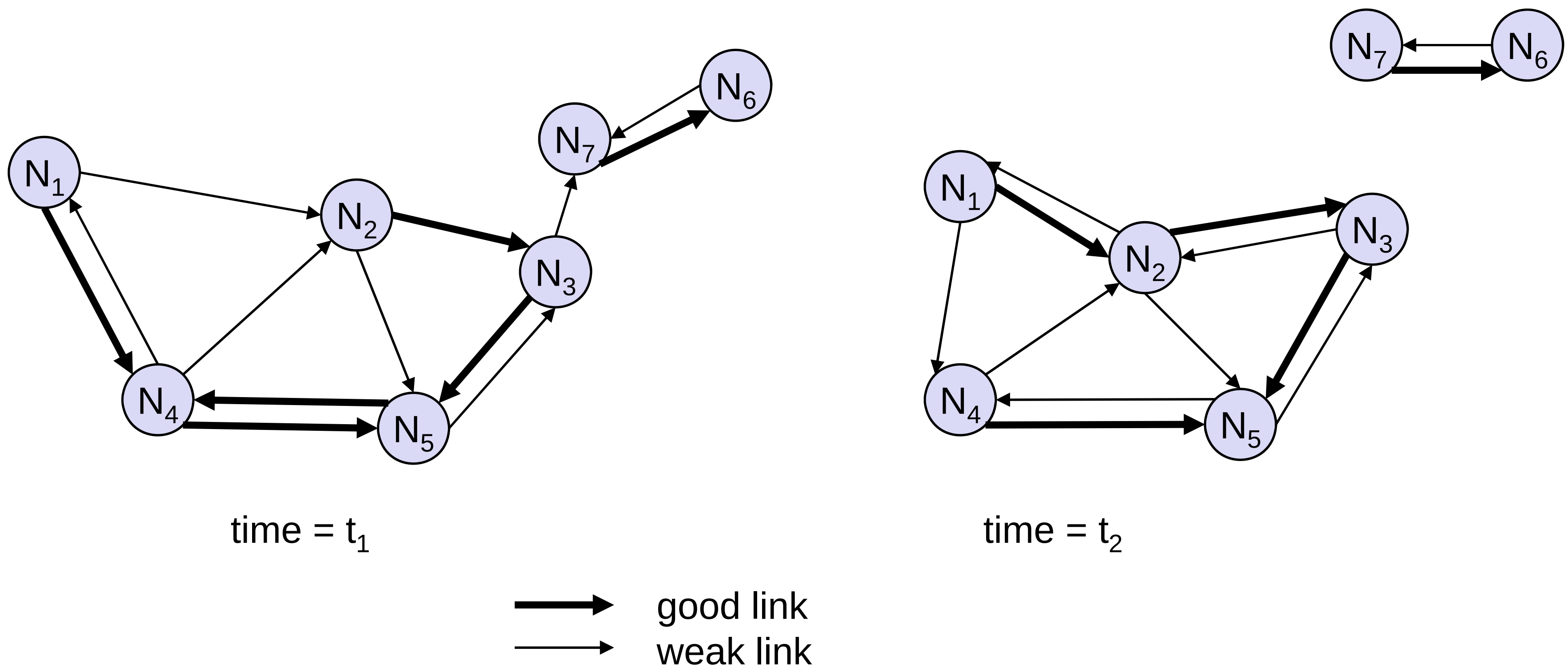
- Internet: MANET (Mobile Ad-hoc Networking) group

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 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

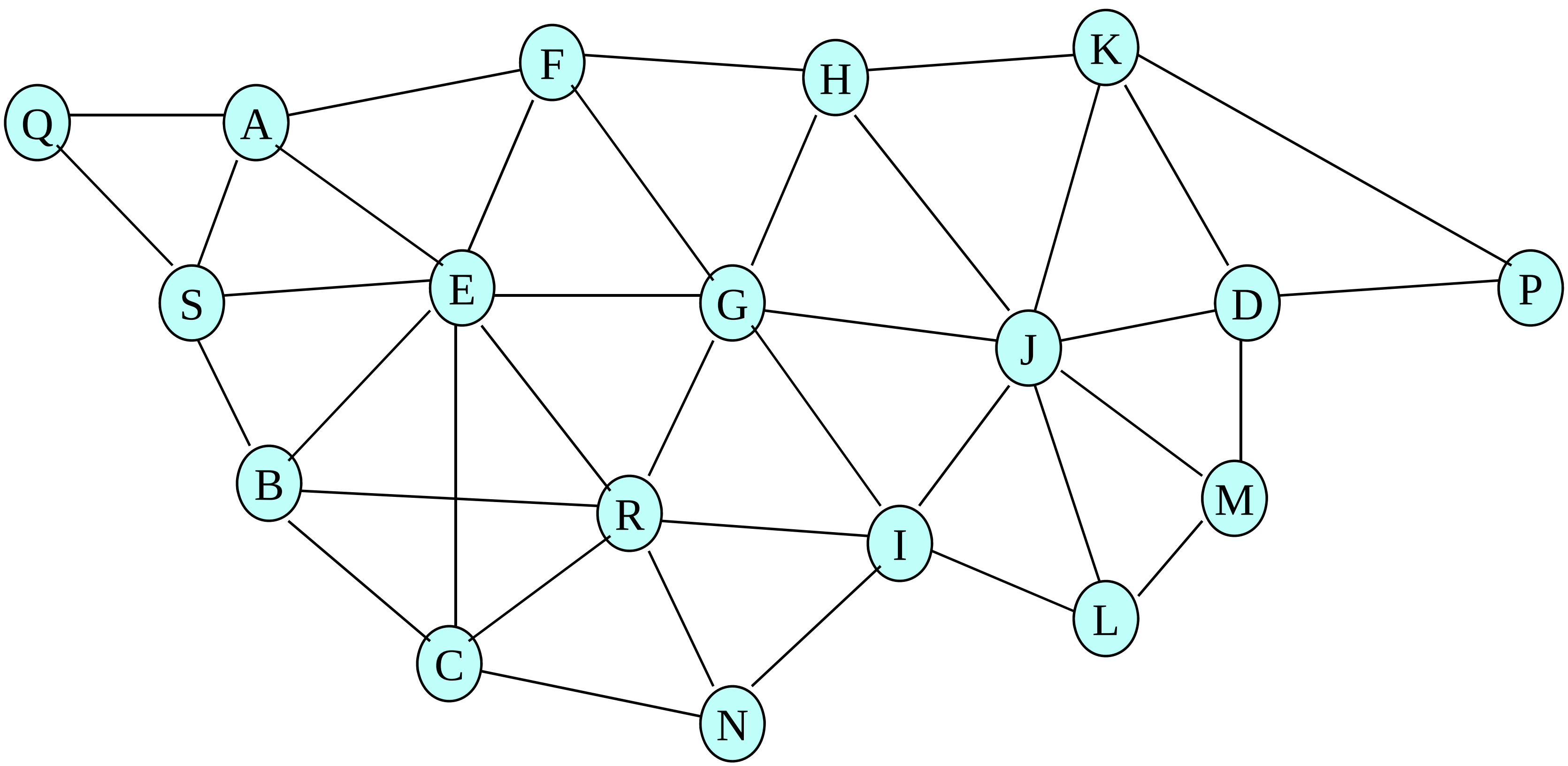
- Sequence numbers for all routing updates
  - assures in-order execution of all updates
  - avoids loops and inconsistencies

- 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)

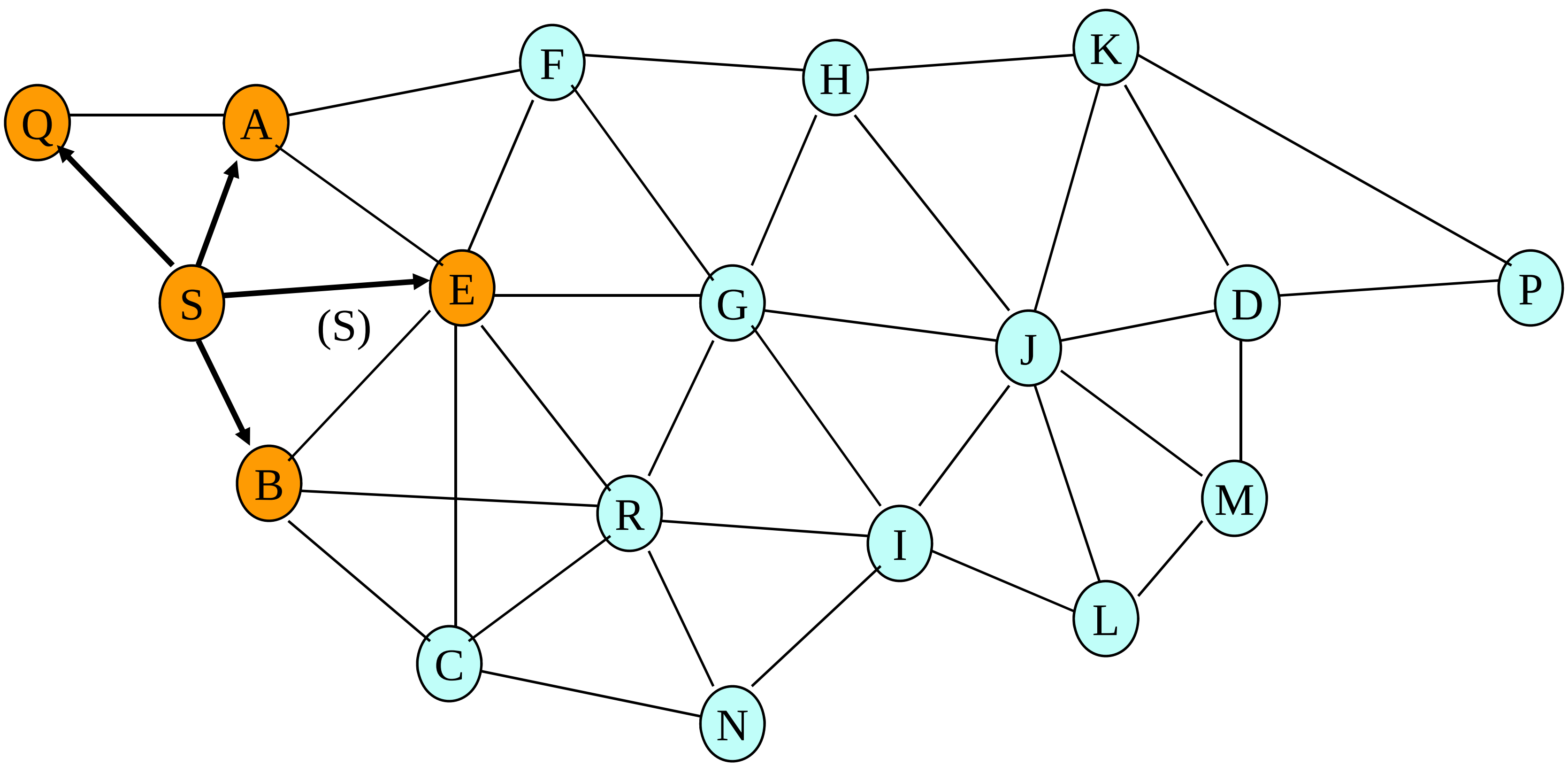
Dynamic source routing (DSR)

- Reactive routing protocol
- 2 phases, operating both **on demand**:
  - **Route discovery**
    - Used only when source S attempts to to send a packet to destination D
    - Based on flooding of Route Requests (RREQ)
  - **Route maintenance**
    - makes S able to detect, while using a source route to D, if it can no longer use its route (because a link along that route no longer works)

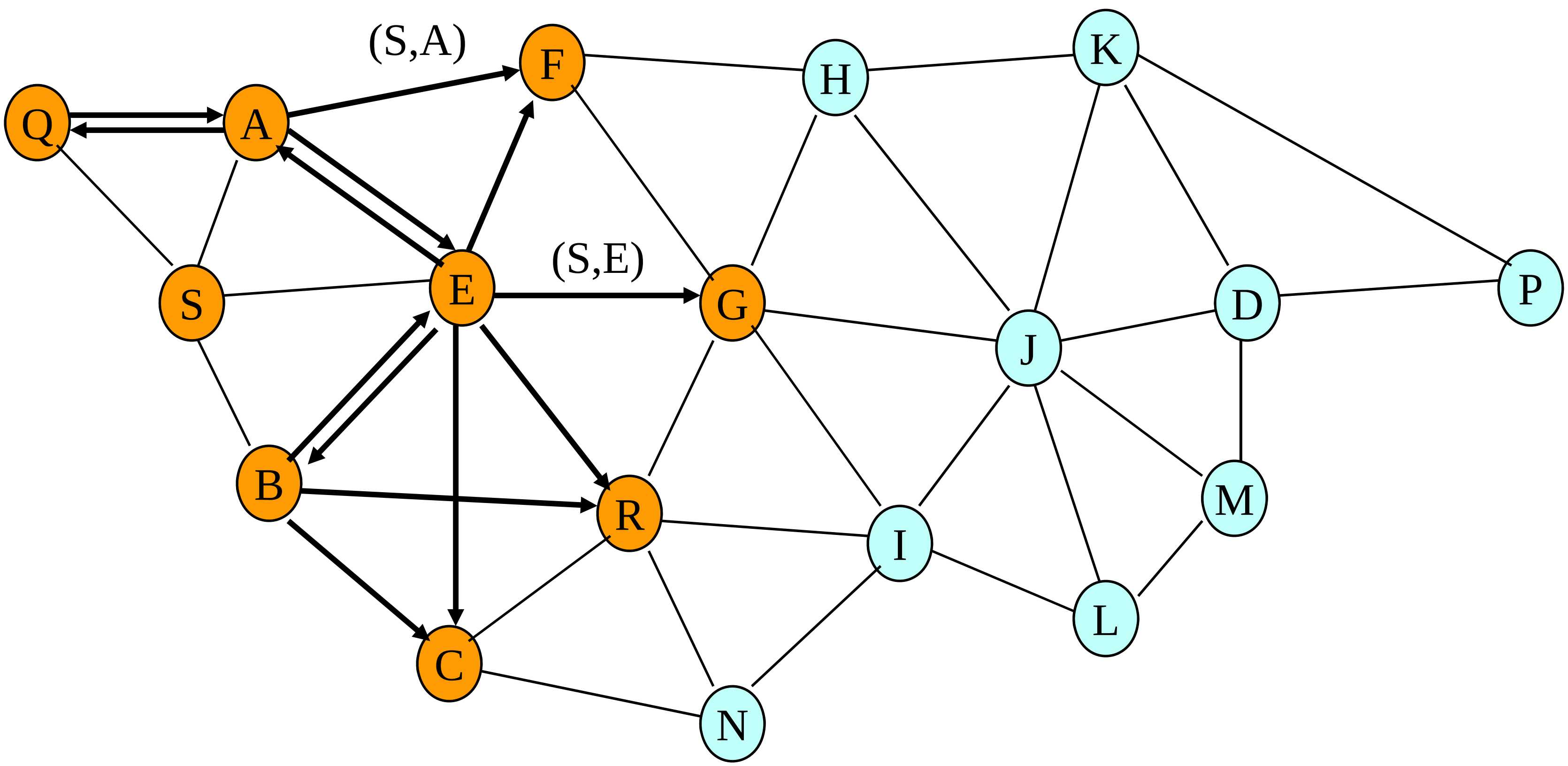
DSR: Route discovery (1)



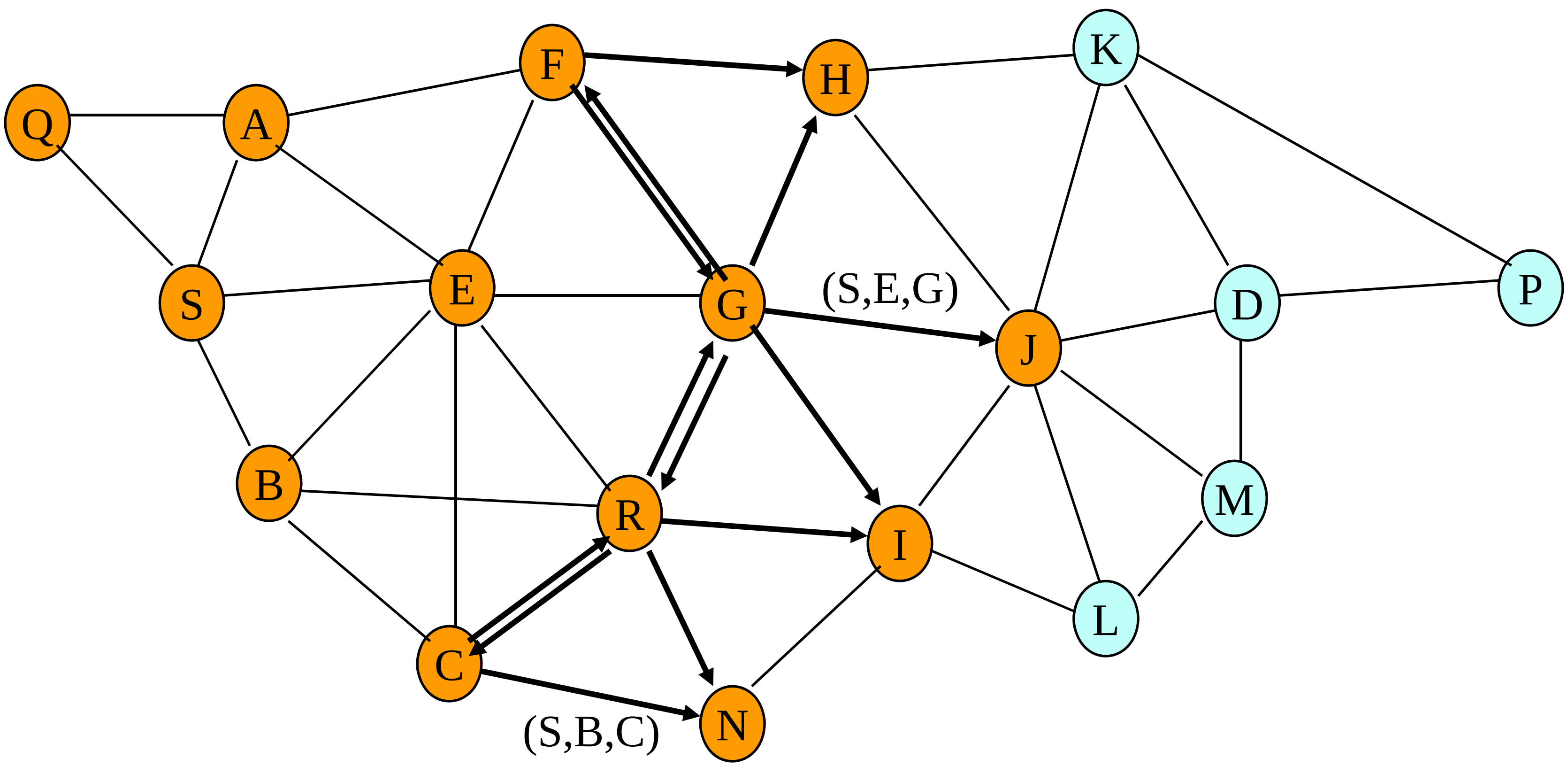
DSR: Route discovery (2)



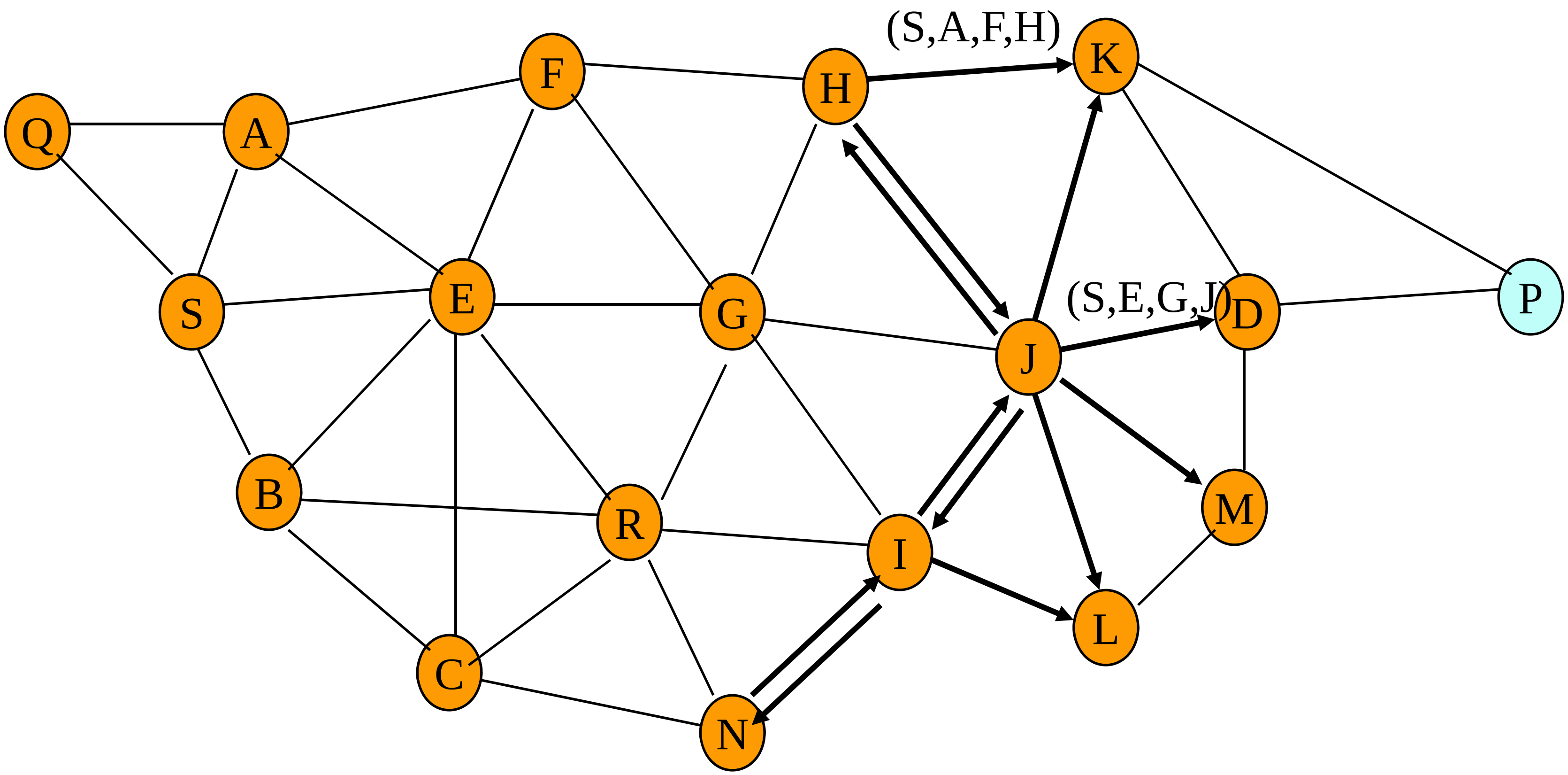
DSR: Route discovery (3)



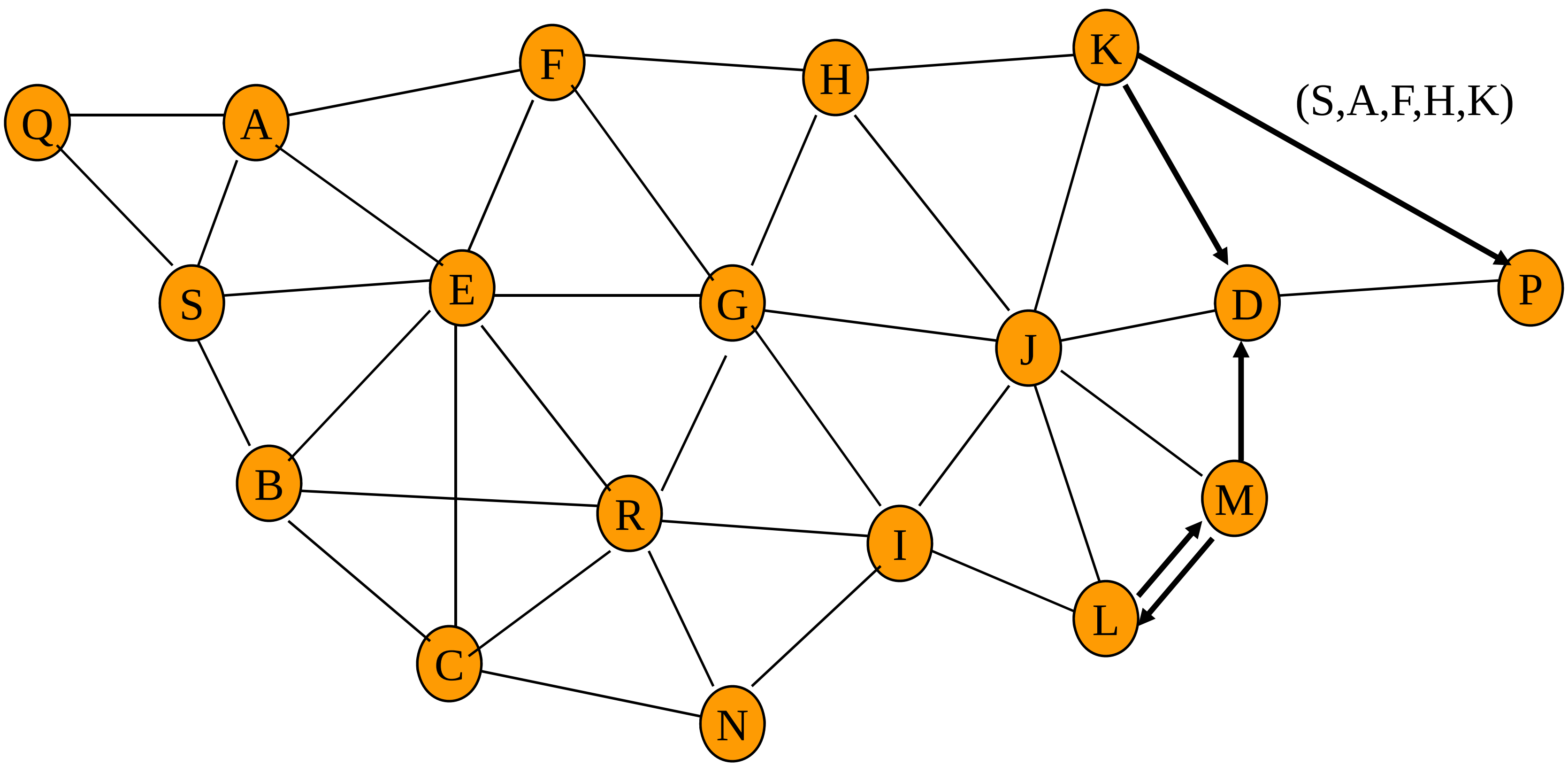
DSR: Route discovery (4)



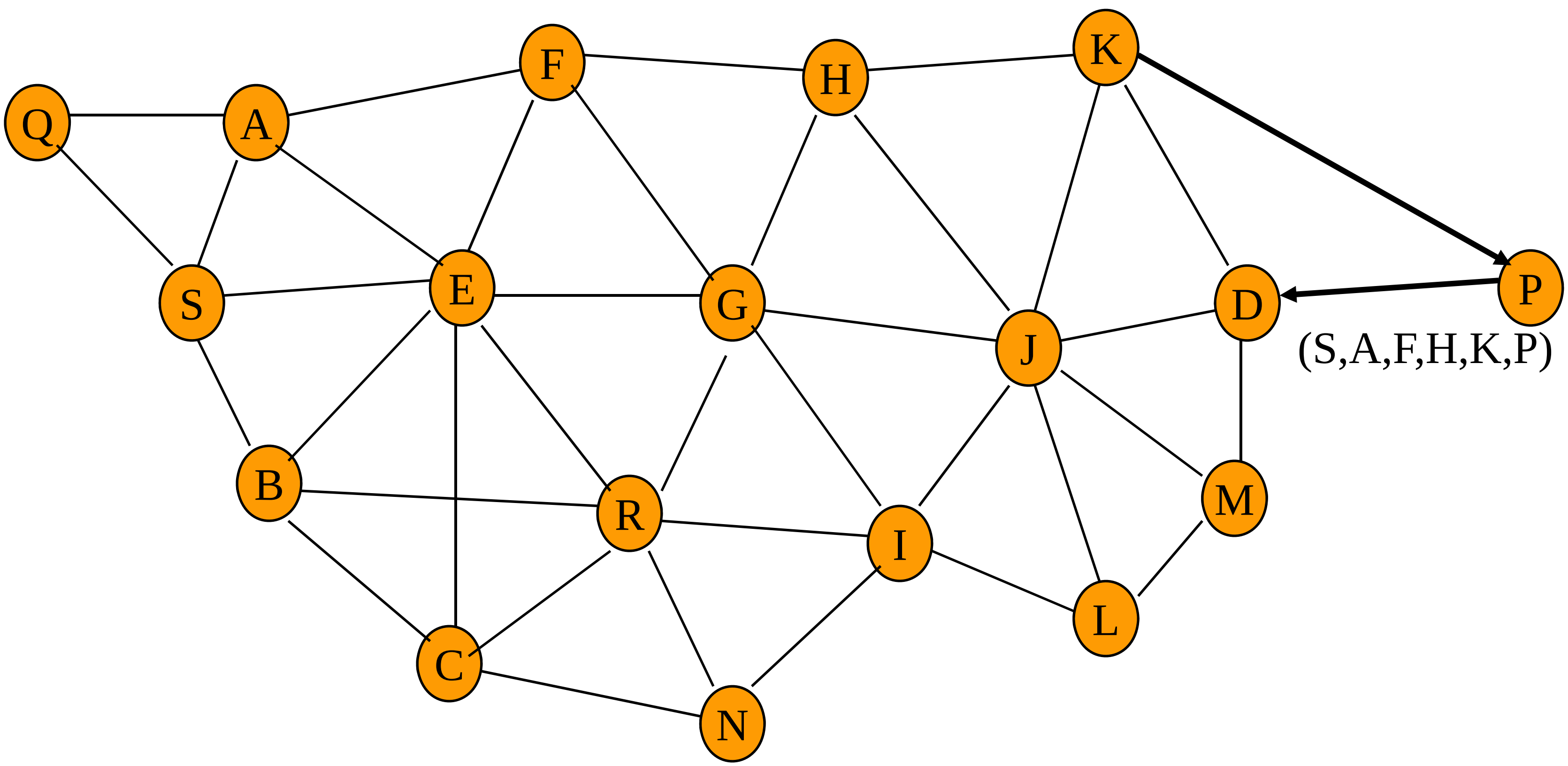
DSR: Route discovery (5)



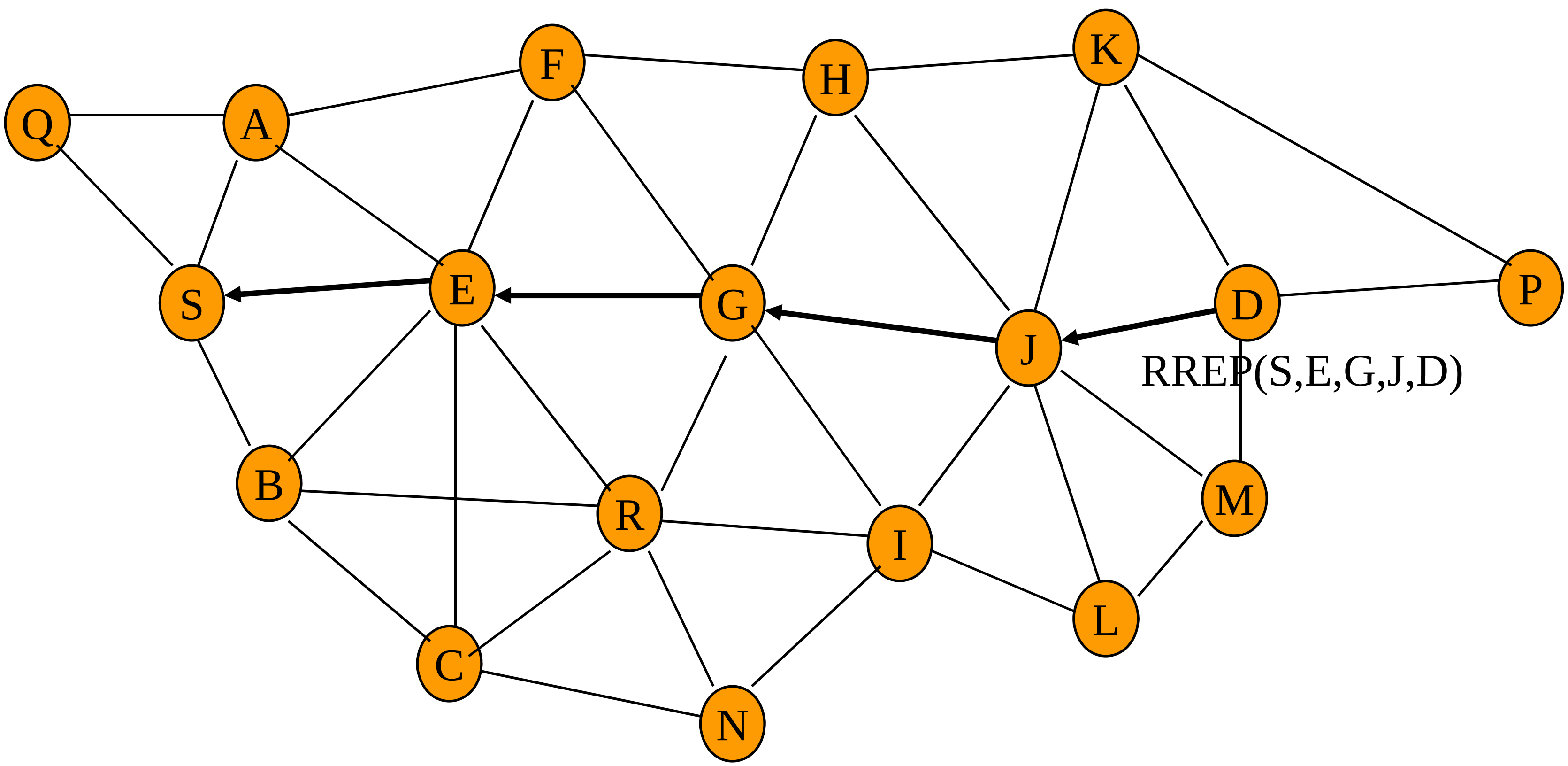
DSR: Route discovery (6)



DSR: Route discovery (7)



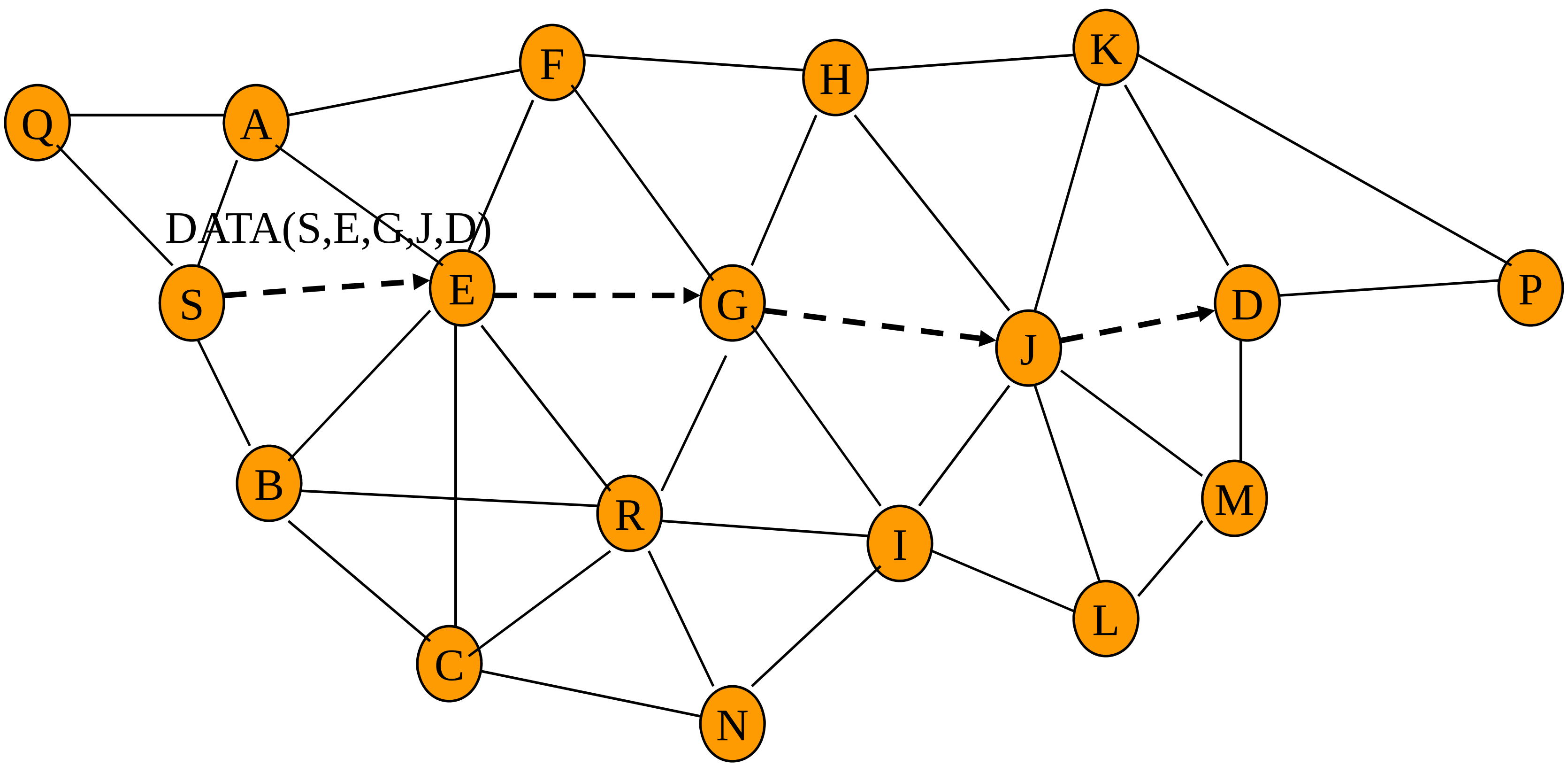
DSR: Route discovery (8)



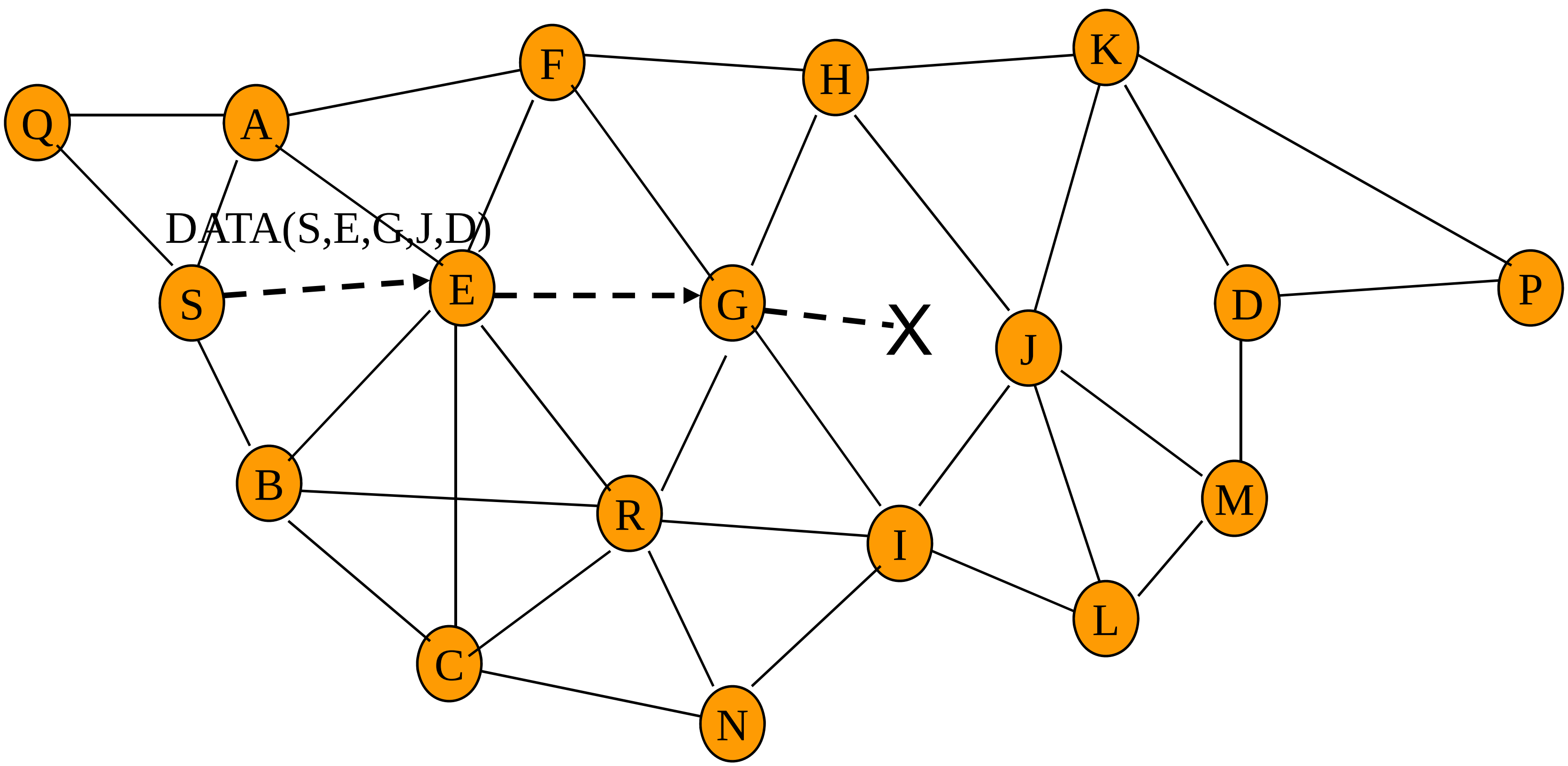
DSR: Route Discovery (9)

- Route reply by reversing the route (as illustrated) works only if all the links along the route are bidirectional
- If unidirectional links are allowed, then RREP may need a route discovery from D to S
- Note: IEEE 802.11 assumes that links are bidirectional

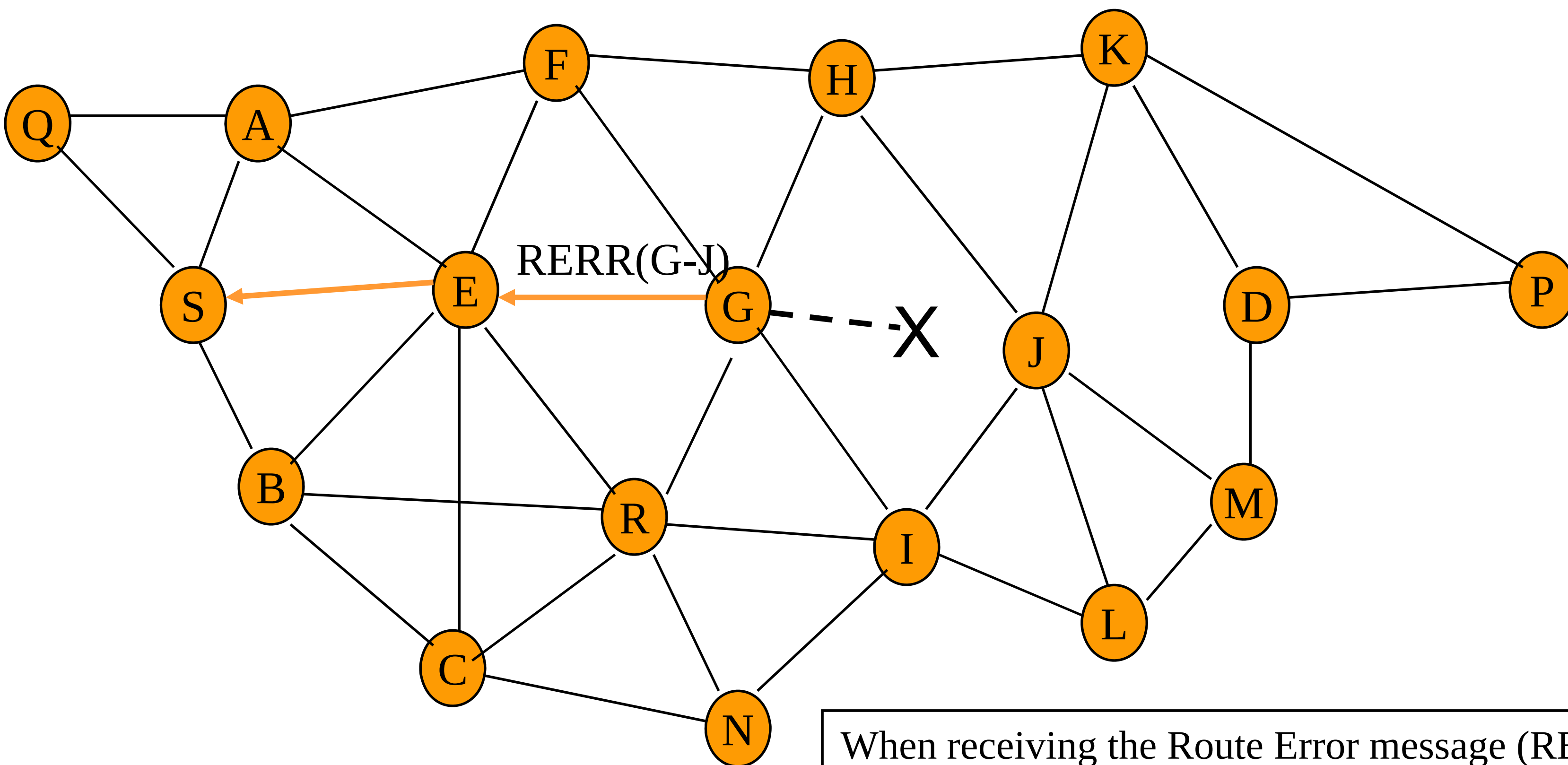
DSR: Data delivery



DSR: Route maintenance (1)



DSR: Route maintenance (2)



When receiving the Route Error message (RERR), S removes the broken link from its cache. It then tries another route stored in its cache; if none, it initializes a new route discovery

DSR: Optimization of route discovery: route caching

- Principle: each node caches a new route it learns by any means
- Examples
  - When node S finds route (S, E, G, J, D) to D, it also learns route (S, E, G) to node G
  - In the same way, node E learns the route to D
  - Same phenomenon when transmitting route replies
- Moreover, routes can be overheard by nodes in the neighbourhood
- However, route caching has its downside: stale caches can severely hamper the performance of the network

DSR: Strengths

- Routes are set up and maintained only between nodes who need to communicate
- Route caching *can* further reduce the effort of route discovery
- A single route discovery may provide several routes to the destination

DSR: Weaknesses

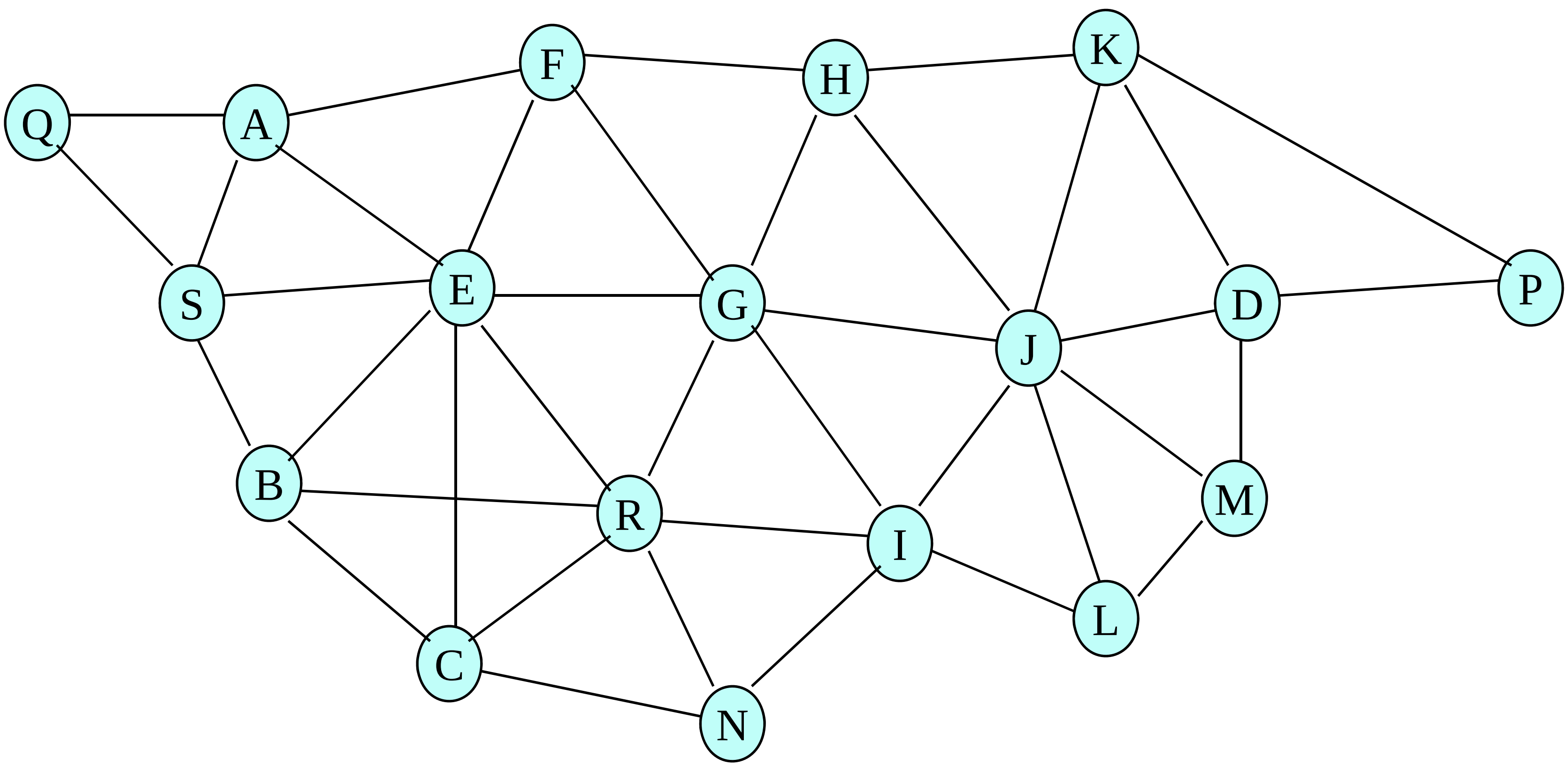
- Route requests tend to flood the network and generally reach all the nodes of the network
- Because of source routing, the packet header size grows with the route lengh
- Risk of many collisions between route requests by neighboring nodes ➔ need for random delays before forwarding RREQ
- Similar problem for the RREP (*Route Reply storm* problem), in case links are not bidirectional

Note: *Location-aided routing* may help reducing the number of useless control messages

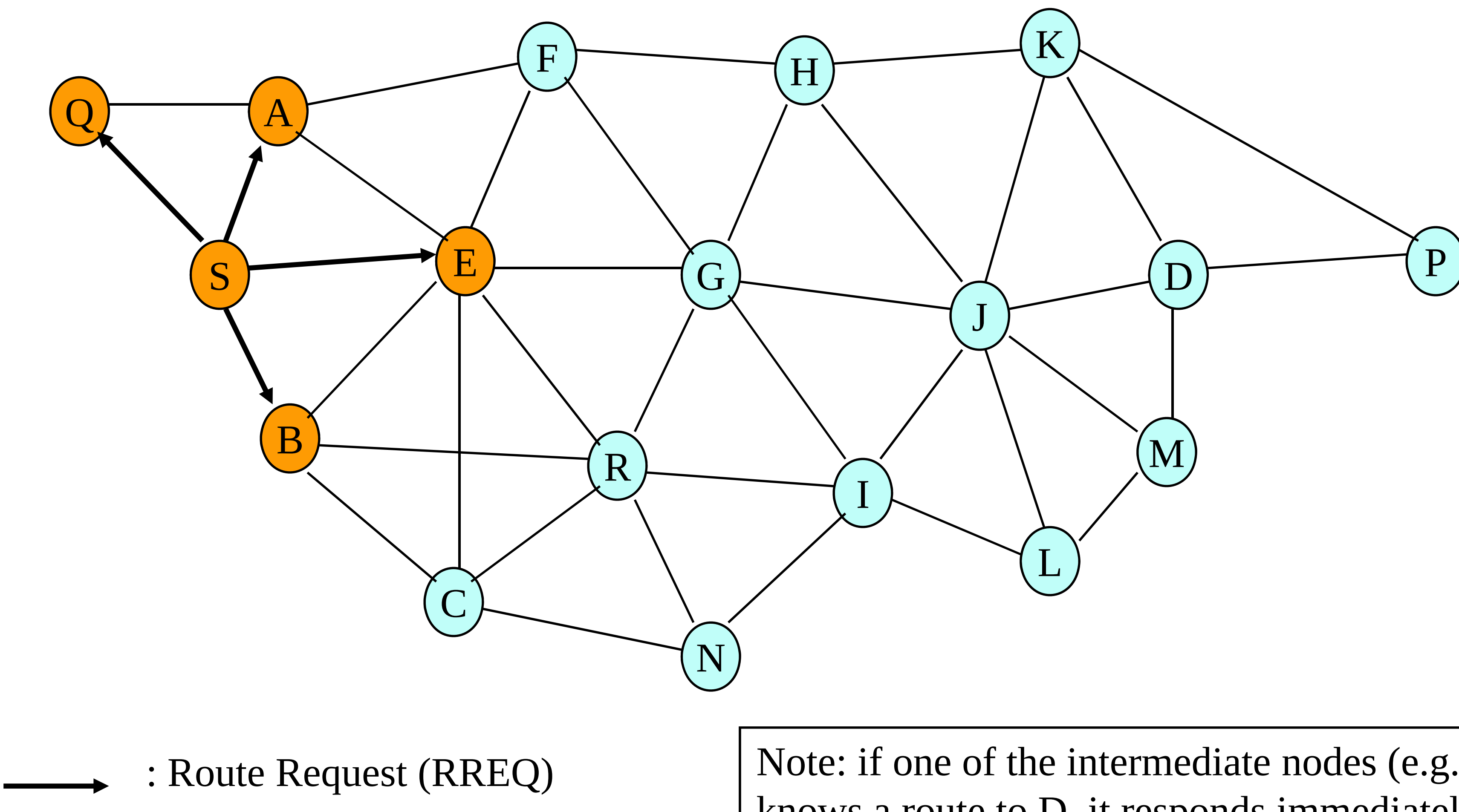
Ad Hoc On-Demand Distance Vector Routing (AODV)

- As it is based on source routing, DSR includes source routes in data packet headers
- Large packet headers in DSR → risk of poor performance if the number of hops is high
- AODV uses a route discovery mechanism similar to DSR, but it maintains routing tables at the nodes
- AODV *ages* the routes and maintains a hop count
- AODV assumes that all links are bi-directional

AODV : Route discovery (1)

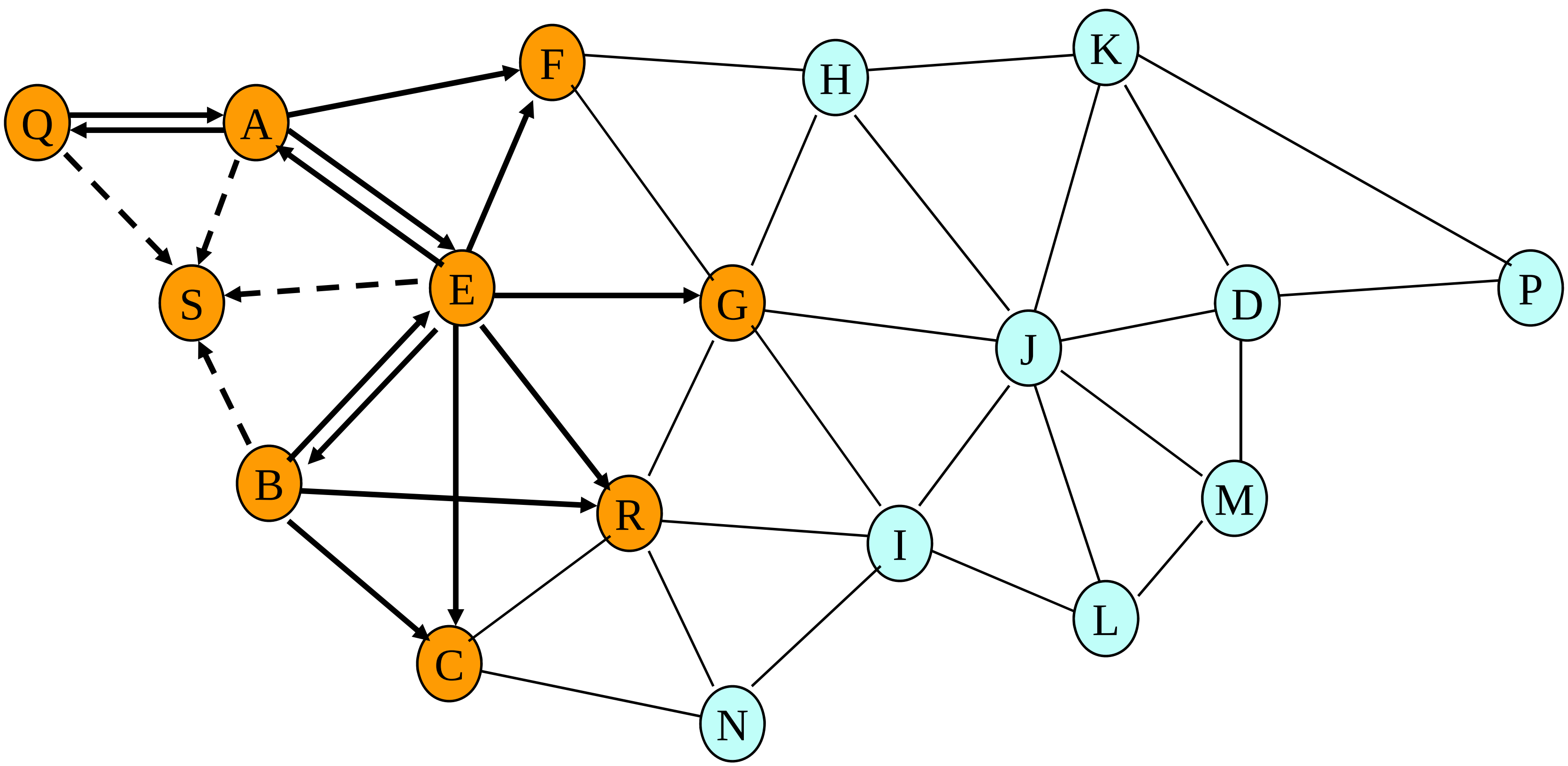


AODV : Route discovery (2)



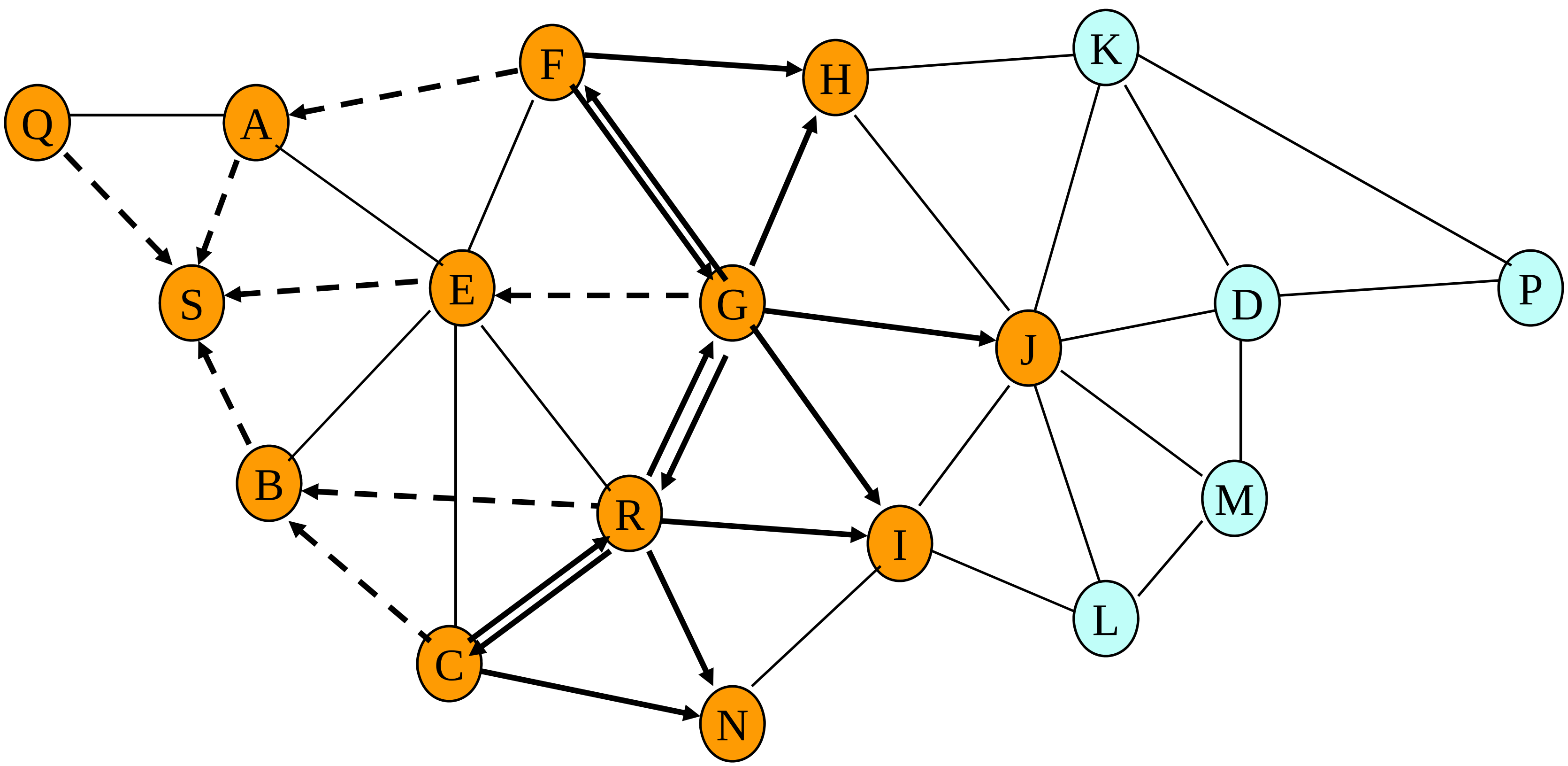
Note: if one of the intermediate nodes (e.g., A) knows a route to D, it responds immediately to S

AODV : Route discovery (3)

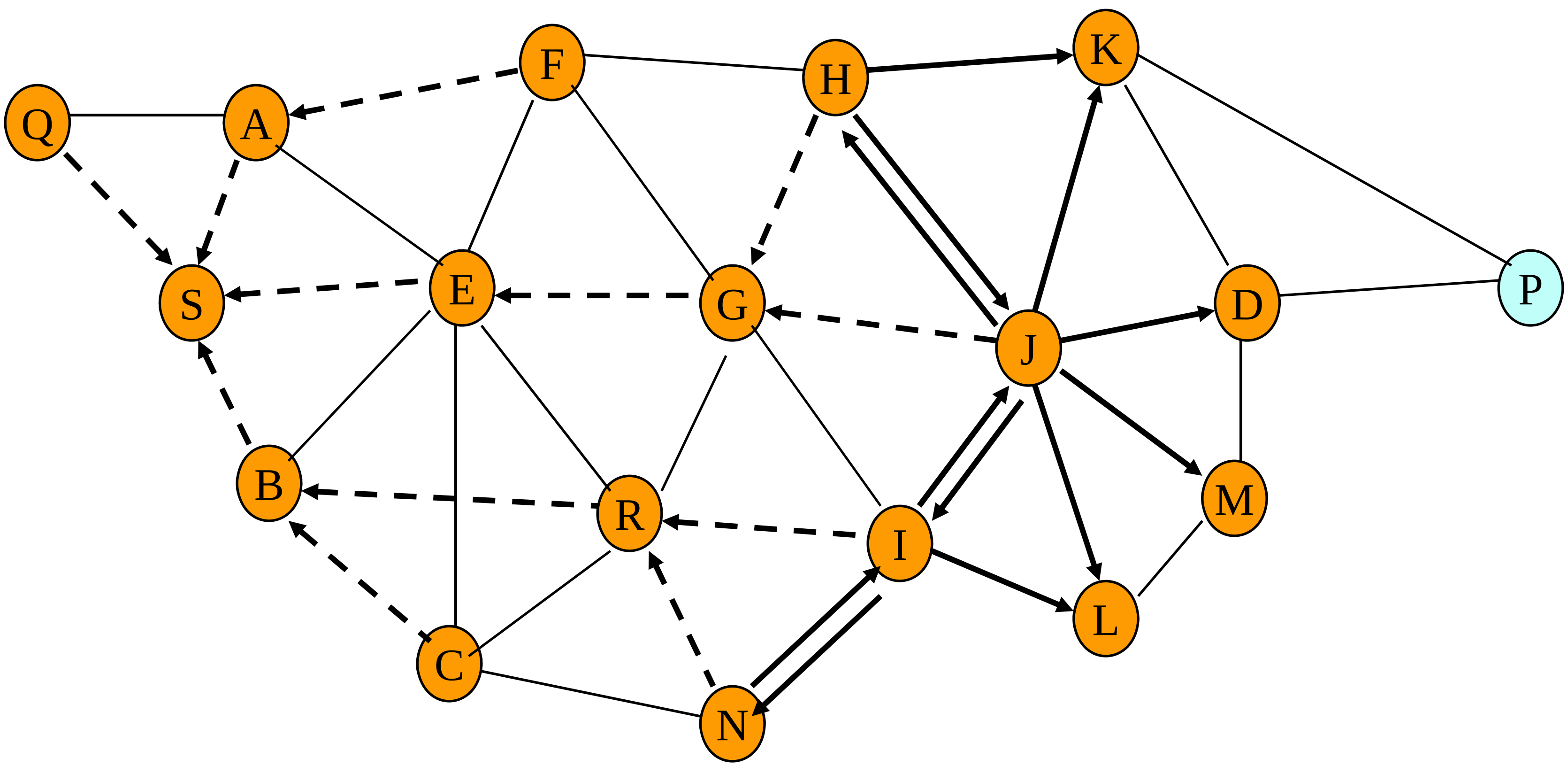


- - ➔ : represents a **link** on the **reverse path**

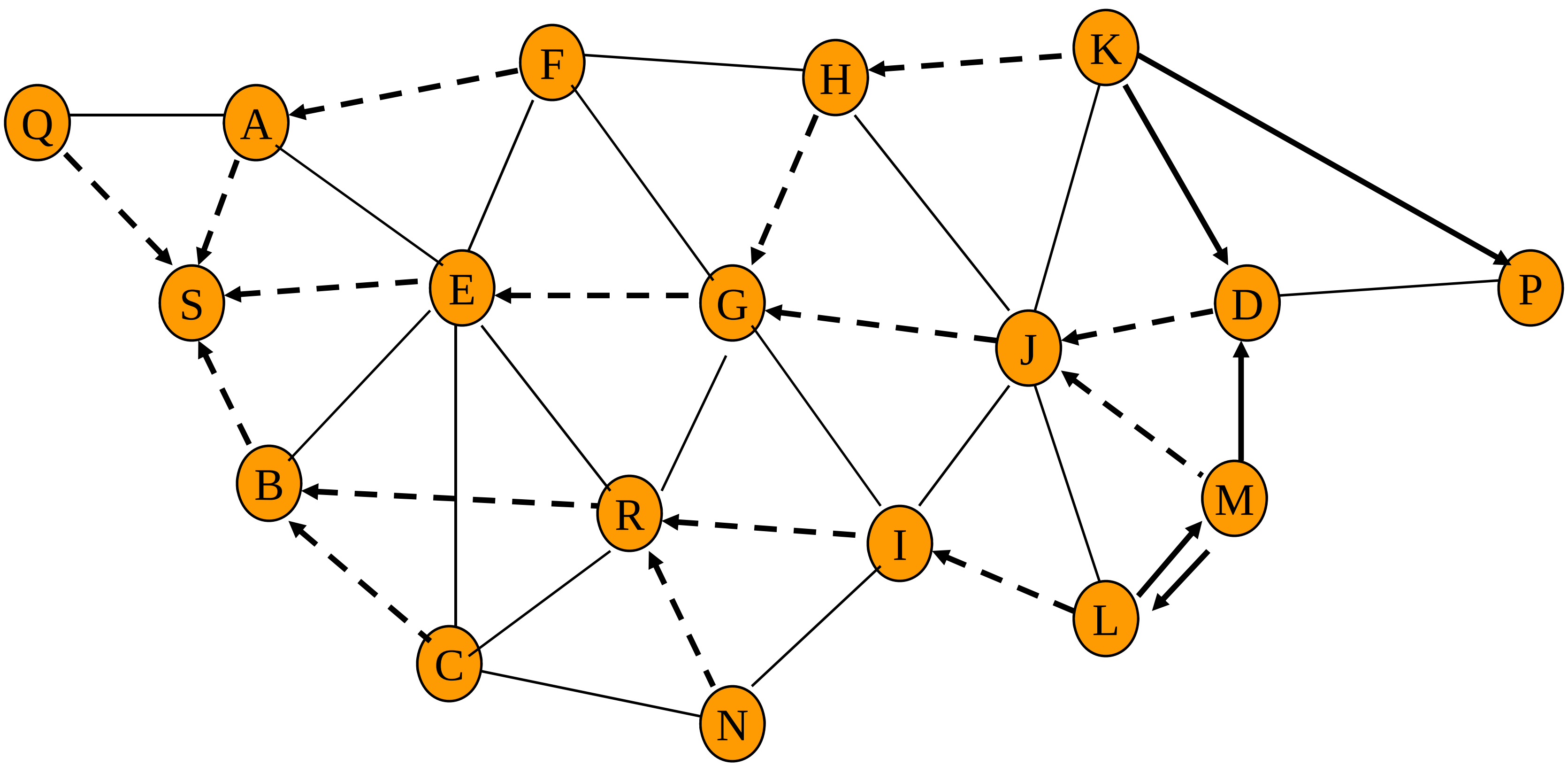
AODV : Route discovery (4)



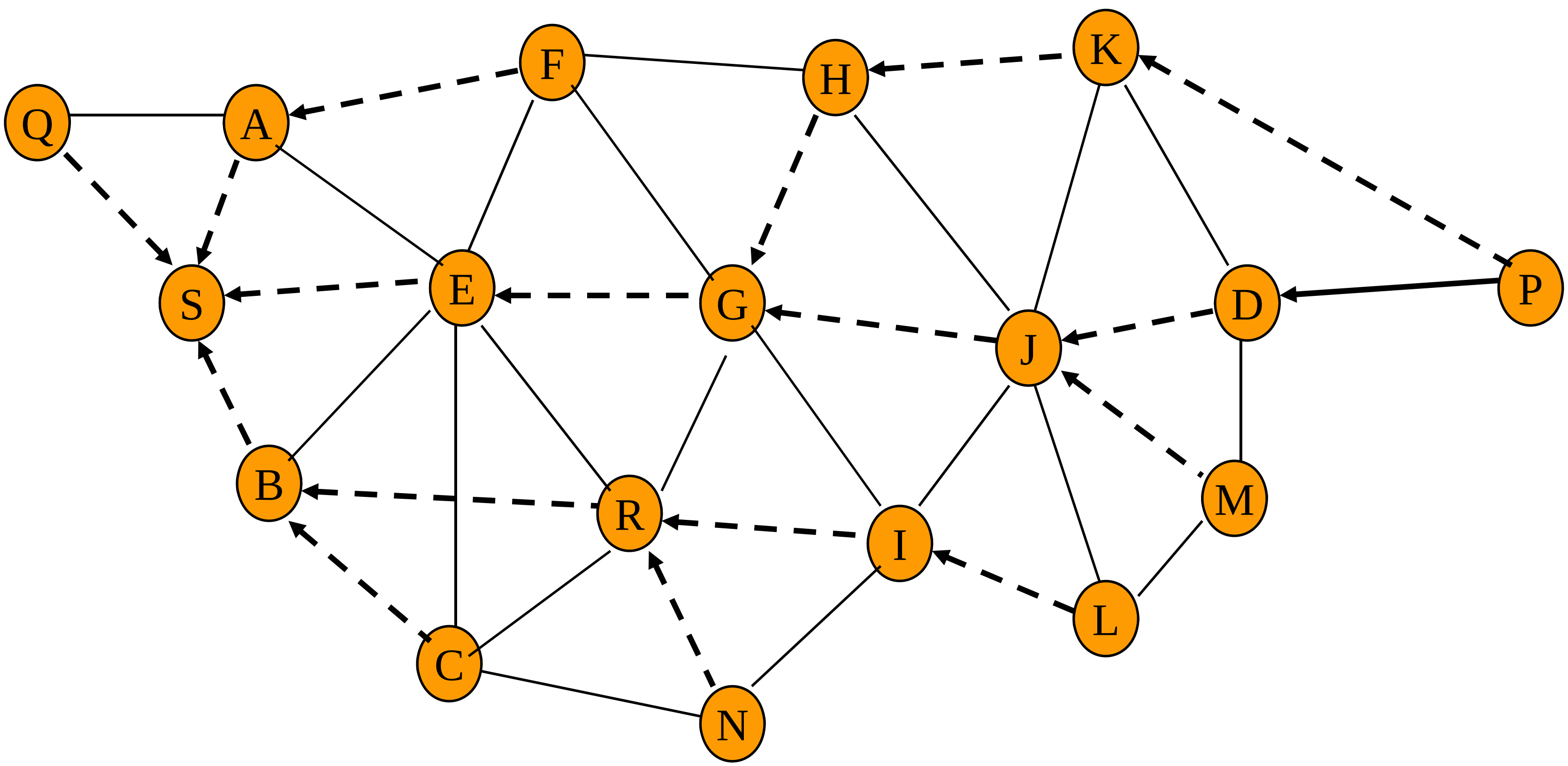
AODV : Route discovery (5)



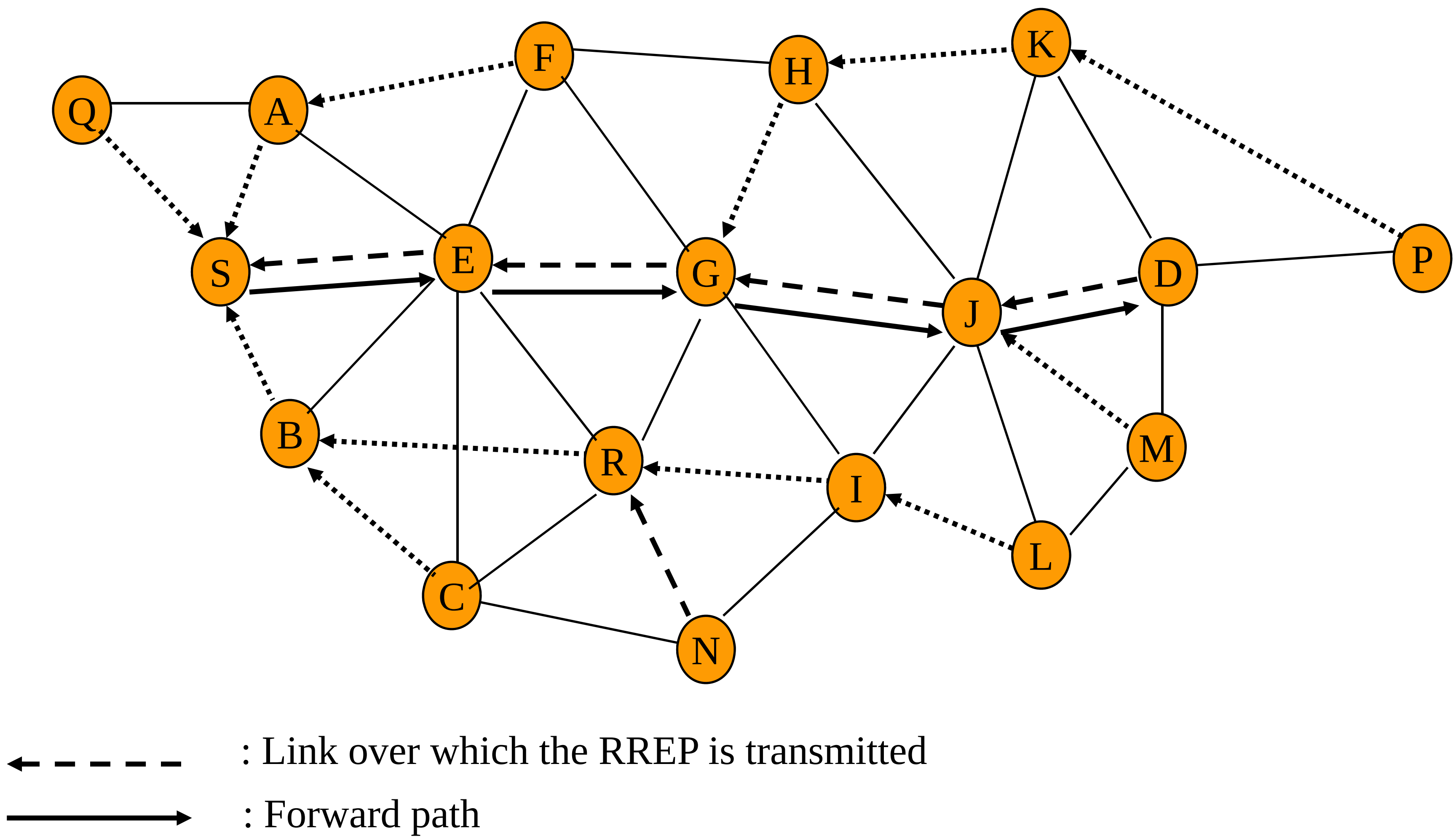
AODV : Route discovery (6)



AODV : Route discovery (7)



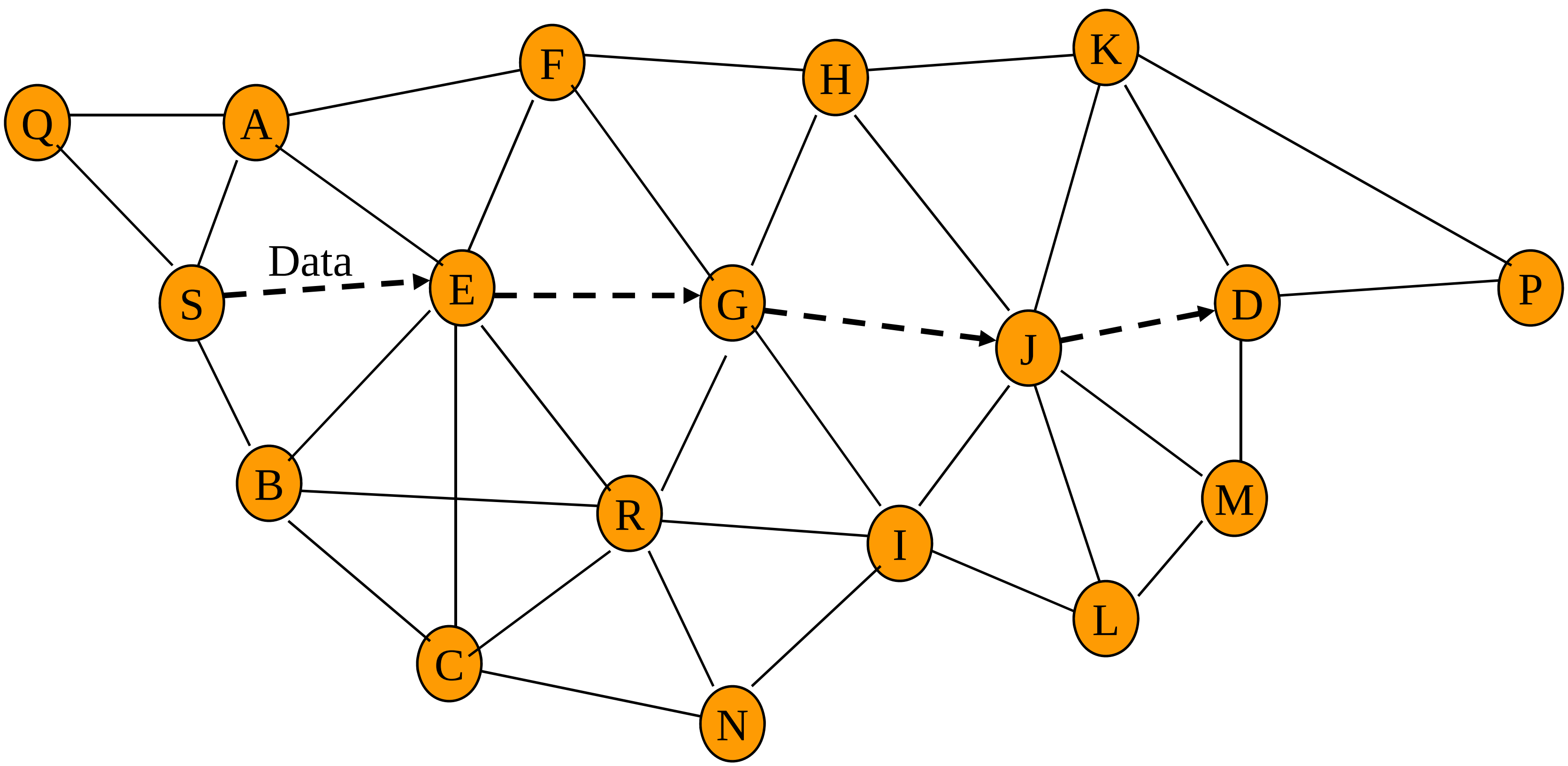
AODV : *Route reply* and setup of the *forward path*



Route reply in AODV

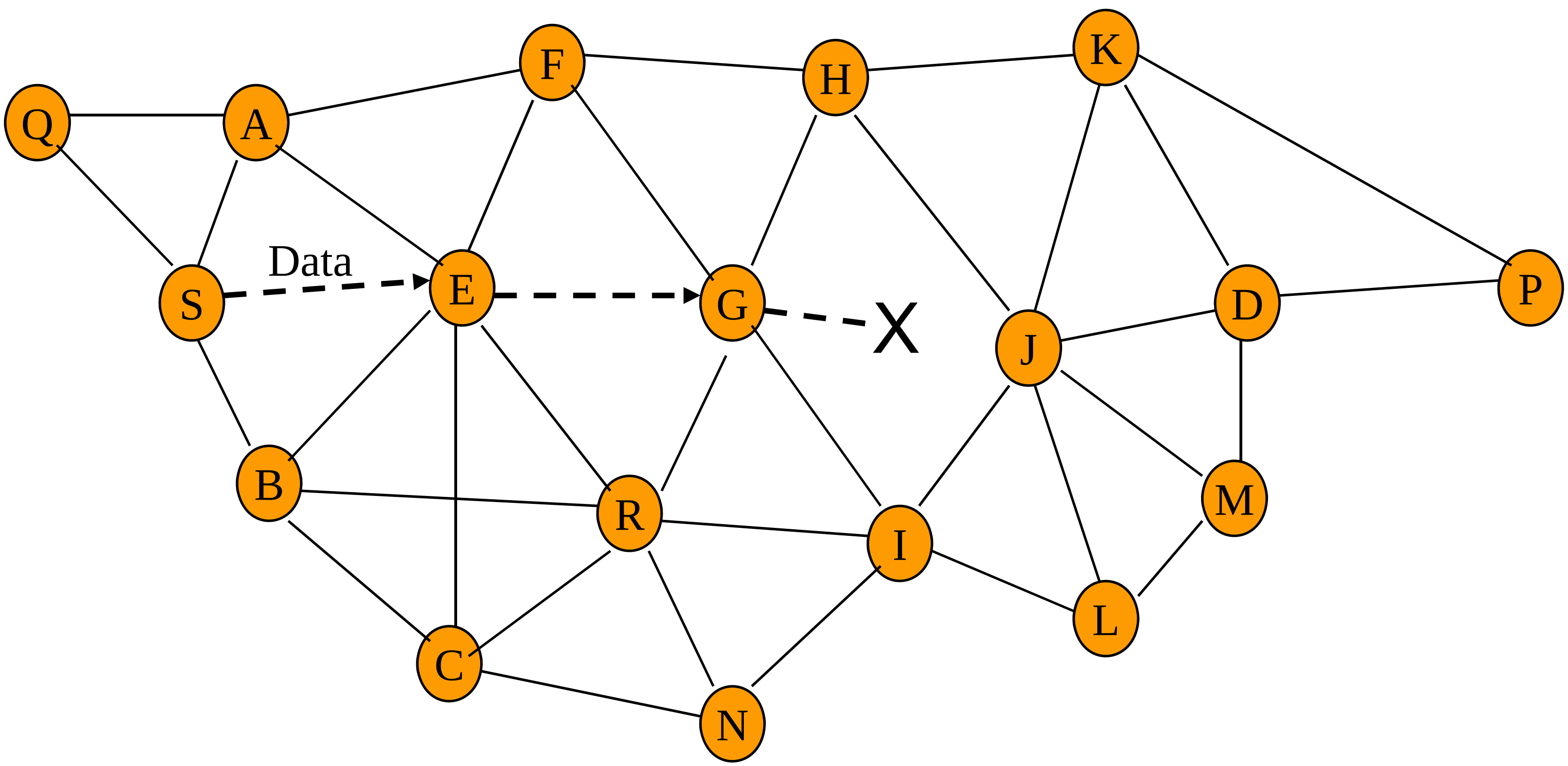
- In case it knows a path more recent than the one previously known to sender S, an *intermediate node* may also send a route reply (RREP)
- The freshness of a path is assessed by means of **destination sequence numbers**
- Both reverse and forward paths are purged at the expiration of appropriately chosen timeout intervals

AODV : Data delivery

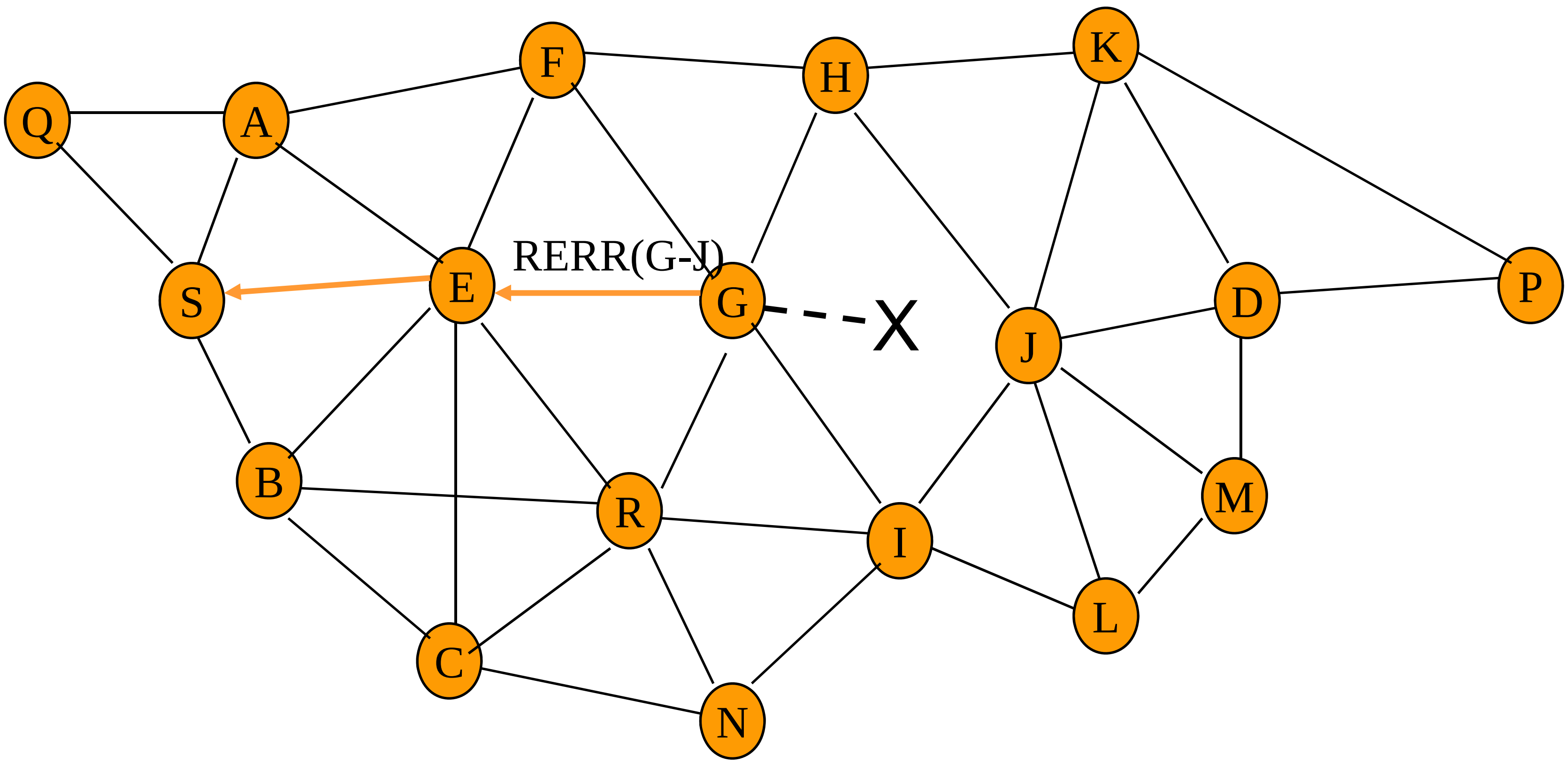


The route is not included in the packet header

AODV : Route maintenance (1)



AODV : Route maintenance (2)

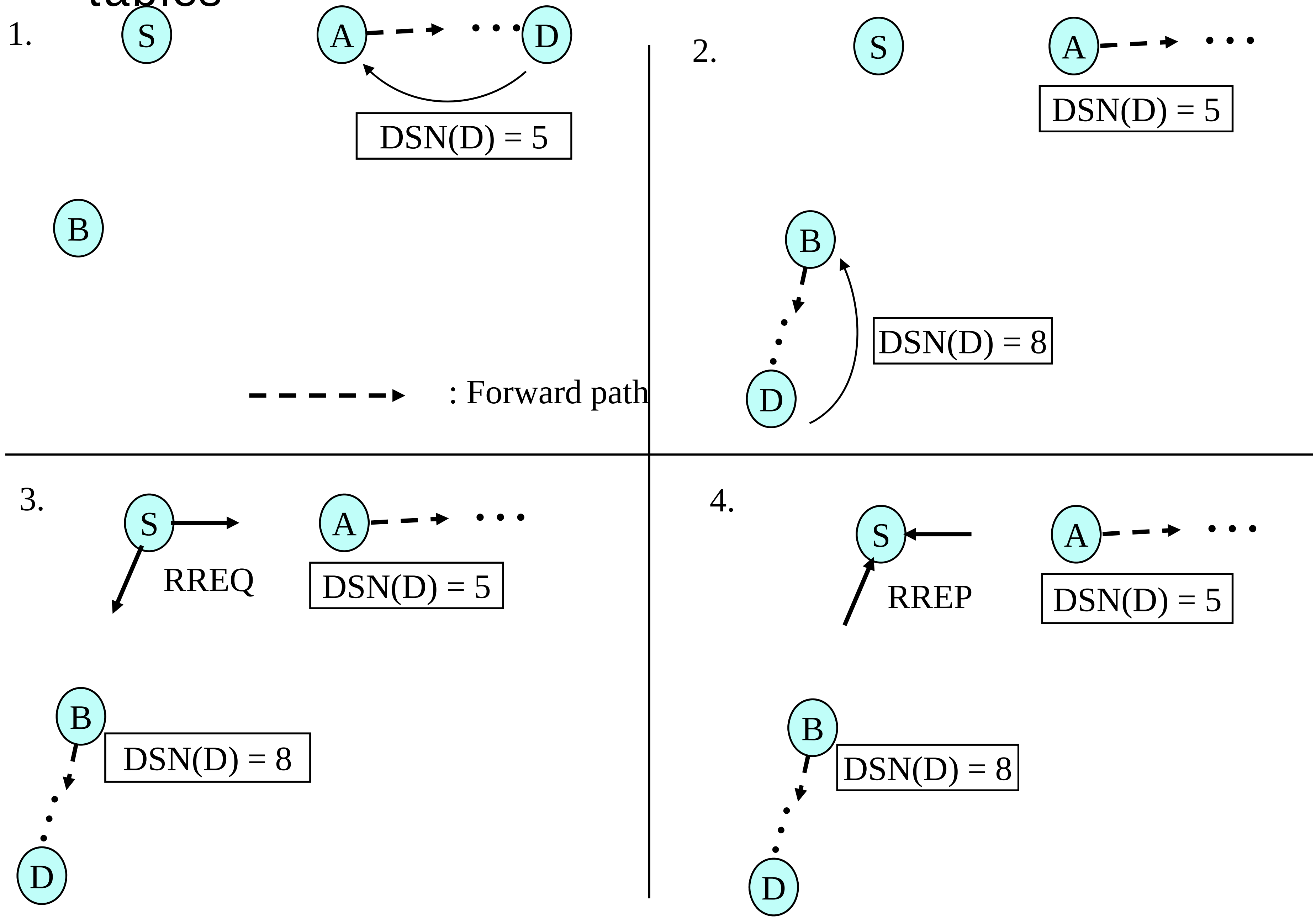


When receiving the Route Error message (RERR),
S removes the broken link from its cache.
It then initializes a new route discovery.

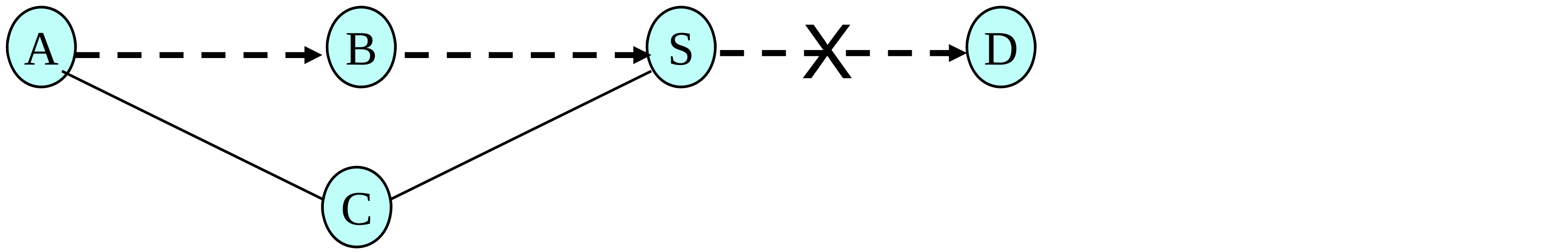
AODV: Destination sequence numbers

- If the destination responds to RREP, it places its current sequence number in the packet
- If an *intermediate* node responds, it places its record of the destination’s sequence number in the packet
- Purpose of sequence numbers:
  - Avoid using stale information about routes
  - Avoid loops (no source routing!)

AODV : Avoiding the usage of stale routing tables



AODV : Avoiding loops



- Assume there is a route between A and D; link S-D breaks; assume A is not aware of this, e.g. because RERR sent by S is lost
- Assume now S wants to send to D. It performs a RREQ, which can be received by A via path S-C-A
- Node A will reply since it knows a route to D via node B
- This would result in a loop (S-C-A-B-S)
- The presence of sequence numbers will let S discover that the routing information from A is outdated
- Principle: when S discovers that link S-D is broken, it increments its local value of DSN(D). In this way, the new local value will be greater than the one stored by A.

AODV (unicast) : Conclusion

- Nodes maintain routing information only for routes that are in active use
- Unused routes expire even when the topology does not change
- Each node maintains at most one next-hop per destination
- Many comparisons with DSR (via simulation) have been performed ➔ no clear conclusion so far

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!

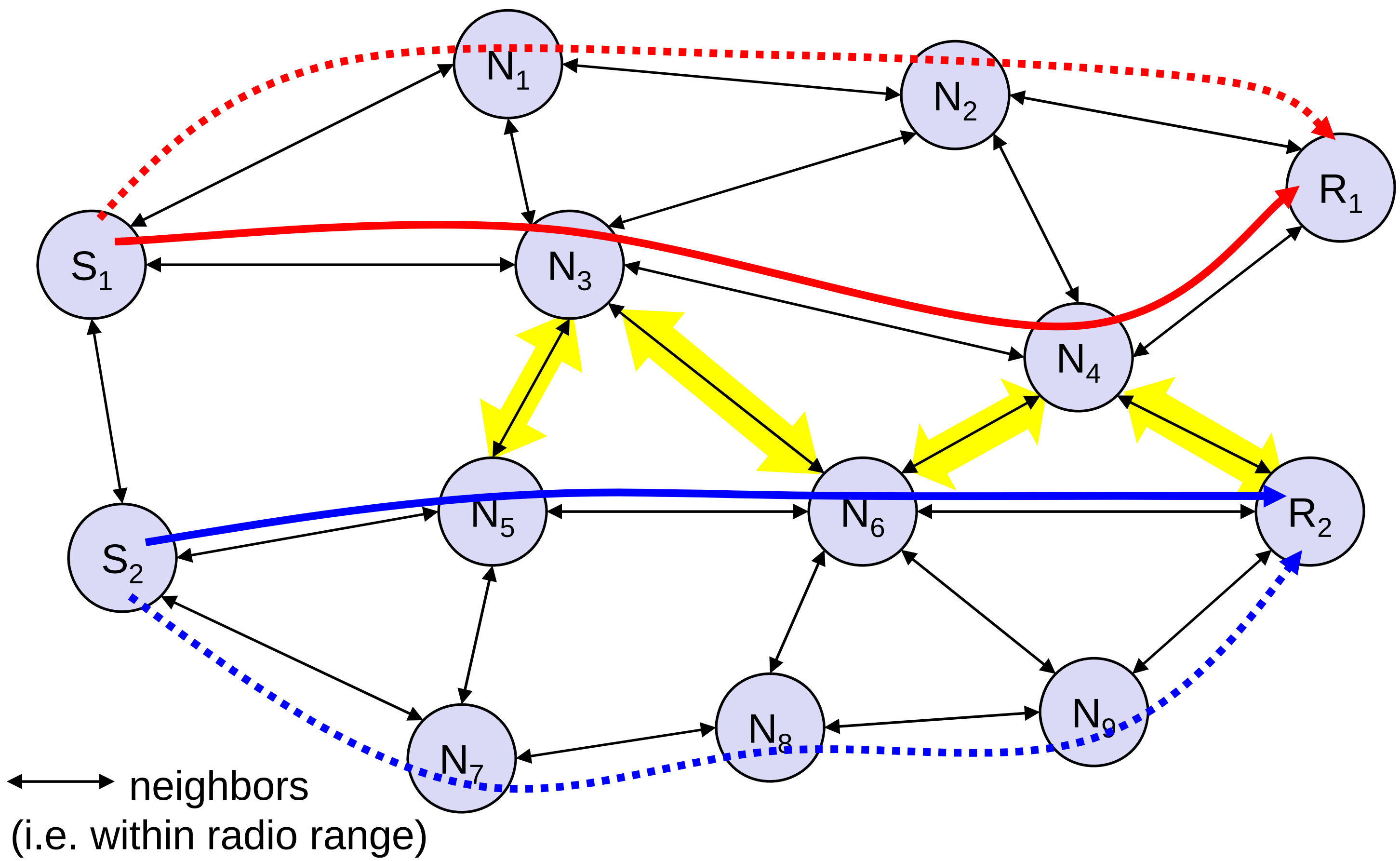
Dynamic source routing II

- 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)

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

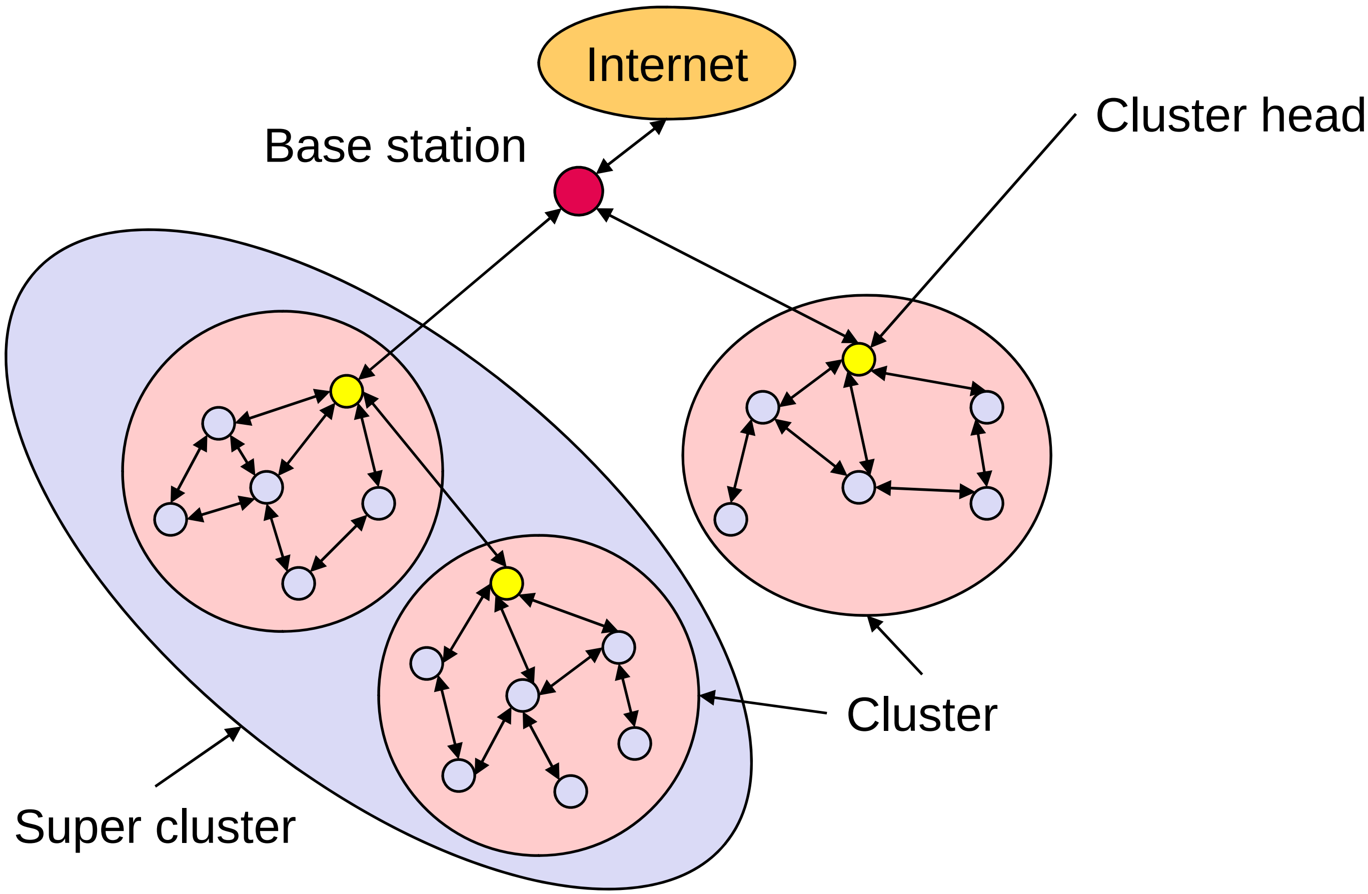
- Flat
  - **proactive**
    - FSLS – Fuzzy Sighted Link State
    - FSR – Fisheye State Routing
    - **OLSR** – Optimized Link State Routing Protocol (RFC 3626)
    - TBRPF – Topology Broadcast Based on Reverse Path Forwarding
  - reactive
    - **AODV** – Ad hoc On demand Distance Vector (RFC 3561)
    - **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

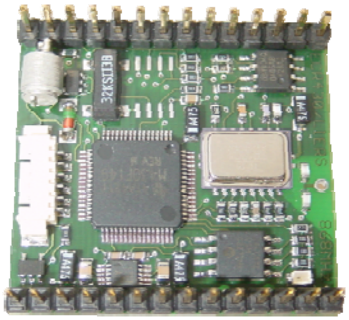
Further difficulties and research areas

- 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)

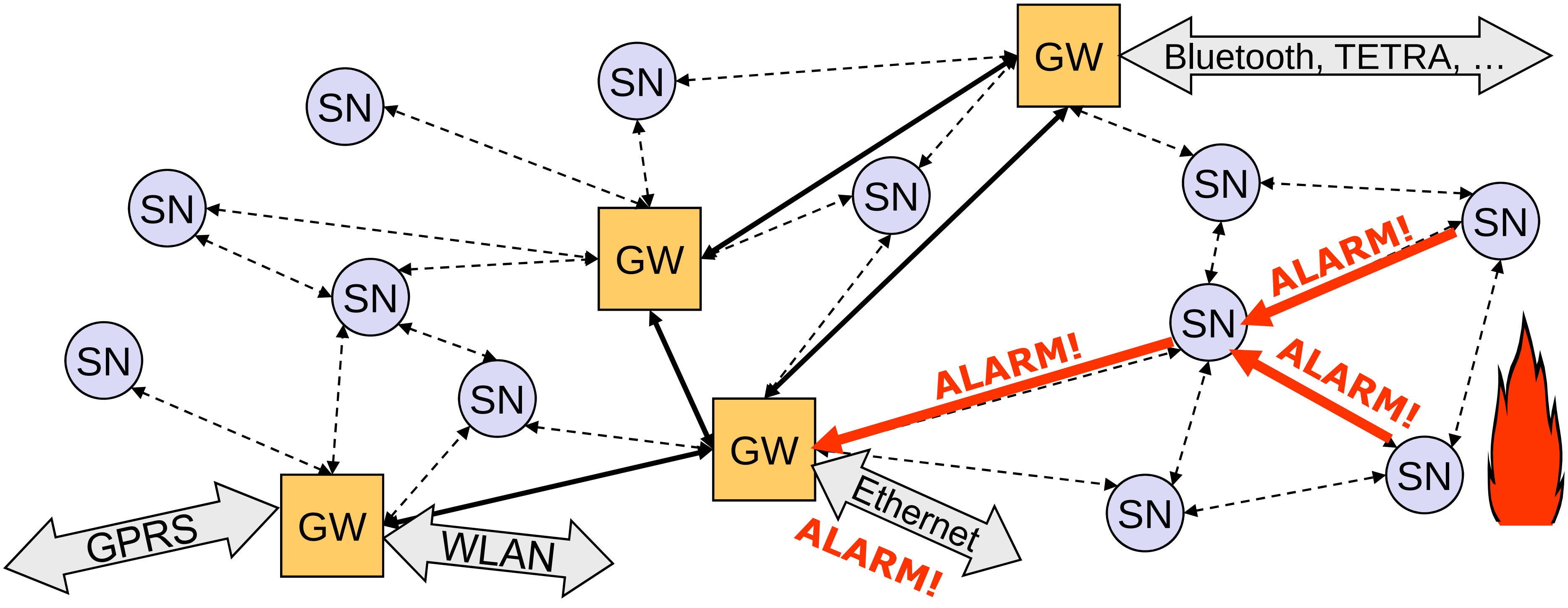


Example:
www.scatterweb.net

- 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!

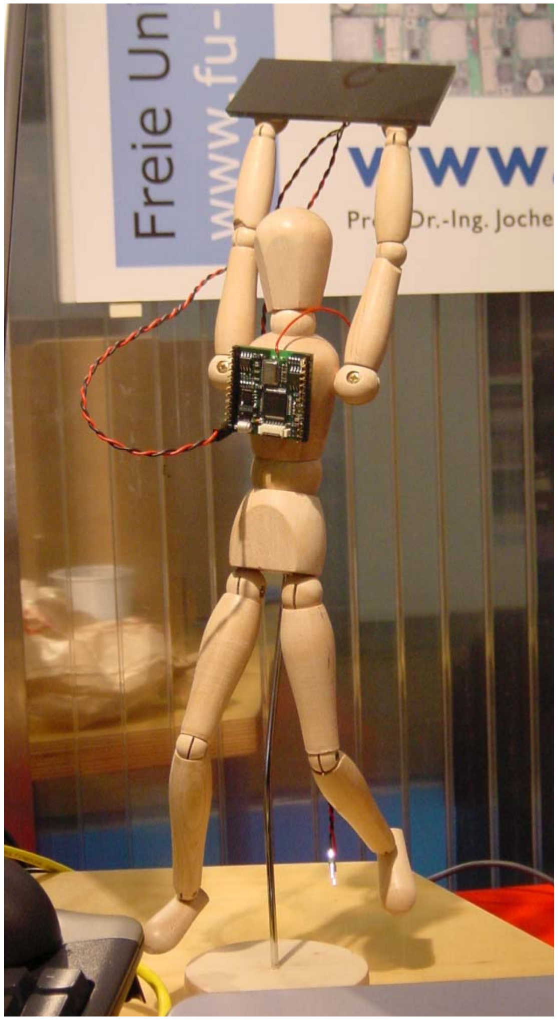
Sensor Networks: Research Areas

- Real-World Integration
  - Gaming, Tourism
  - Emergency, Rescue
  - Monitoring, Surveillance

- Self-configuring networks
  - Robust routing
  - Low-power data aggregation
  - Simple indoor localization

- Managing wireless sensor networks
  - Tools for access and programming
  - Update distribution

- Long-lived, autonomous networks
  - Use environmental energy sources
  - Embed and forget



WSN: Earthquake detection

- The occurrence of an earthquake can be detected automatically by accelerometers.
- Earthquake speed: around 5-10km/s
- If the epicenter of an earthquake is in an unpopulated area 200km from a city center, an instantaneous detection system can give a warning up to 30 seconds before the shockwave hits the city.
- If a proper municipal actuation network is in place:
  - Sirens go off
  - Traffic lights go to red
  - Elevators open at the nearest floor
  - Pipeline valves are shut
- Even with a warning of a few secon the effects of the earthquake can b mitigated.
- Similar concept can be applied to
  - Forest fire
  - Landslides
  - Etc.

WSN: Cold Chain Management

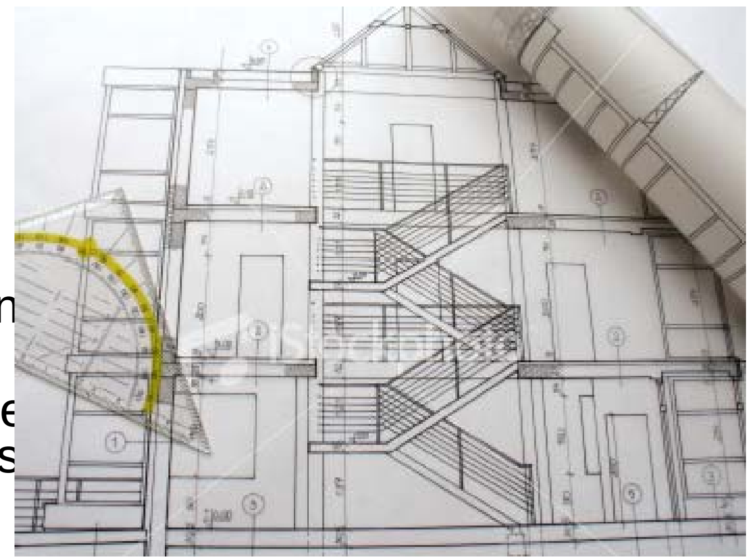
- Supermarket chains need to track the storage temperature of perishable goods in their warehouses and stores.
- Tens if not hundreds of fridges should be monitored in real-time
- Whenever the temperature of a monitored item goes above a threshold
  - An alarm is raised and an attendant is warned (pager, SMS)
  - The refrigeration system is turned on
- History of data is kept in the system for legal purpose

- Similar concept can be applied to pressure and temperature monitoring in
  - Production chains
  - Containers
  - Pipelines

WSN: Home automation

- Temperature management
  - Monitor heating and cooling of a building in an integrated way
  - Temperature in different rooms is monitored centrally
  - A power consumption profile is to be drawn in order to save energy in the future

- Lighting management:
  - Detect human presence in a room to automatically switch lights on and off
  - Responds to manual activation deactivation of switches
  - Tracks movement to anticipate the activation of light-switches on the path of a person



- Similar concept can be applied to
  - Intrusion detection

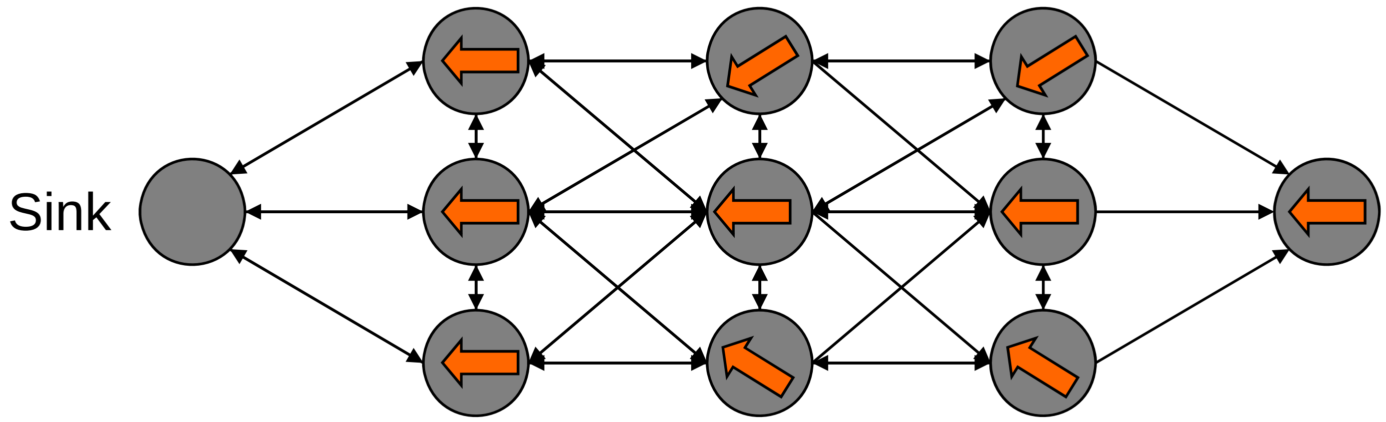
WSN: Precision Agriculture management

- Farming decisions depend on environmental data (typically photo-synthesis):
  - Solar radiation
  - Temperature
  - Humidity
  - Soil moisture

- These data evolve continu-ously over time and space
- A farmer’s means of action to influence crop yield :
  - Irrigation
  - Fertilization
  - Pest treatment
- To be optimal, these actions should be highly localized (homogenous parcels can be as small as one hectare or less)
- Environmental impact is also to be taken into account
  - Salinization of soils
  - Groundwater depletion
  - Well contamination

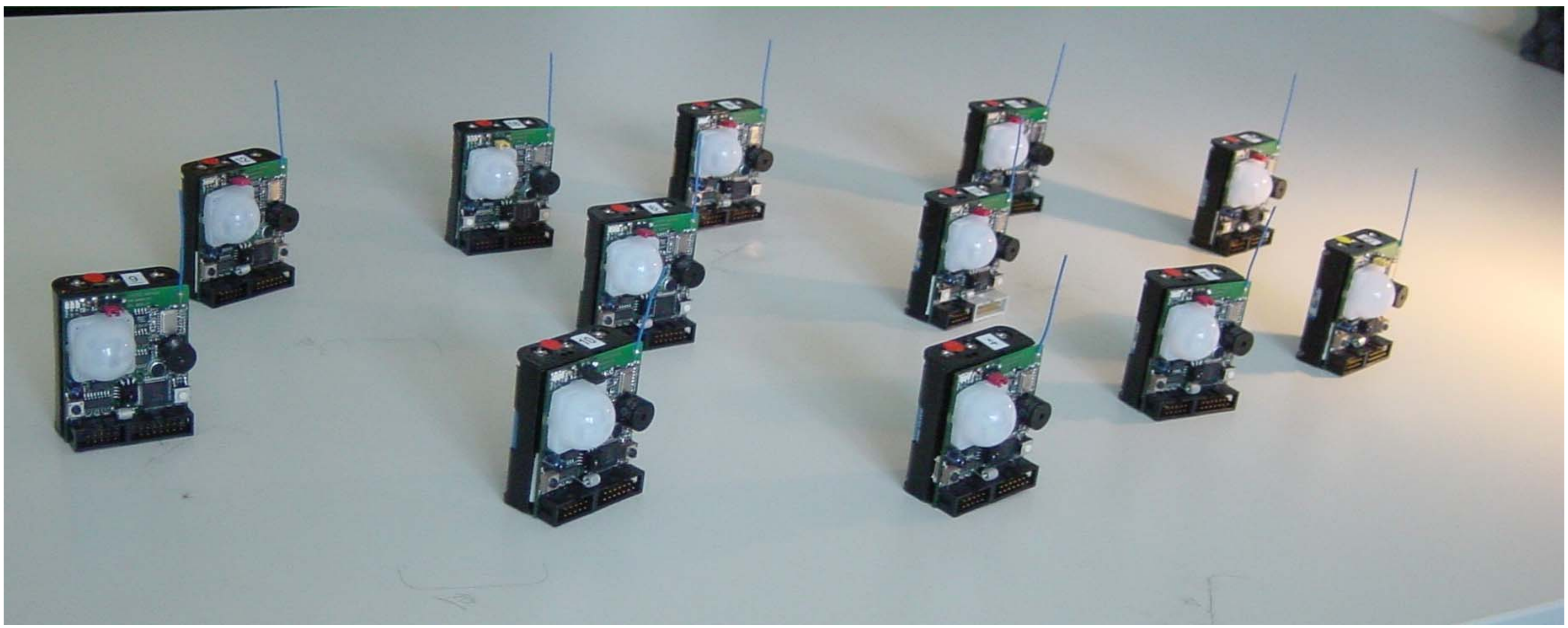
Routing in WSNs is different

- No IP addressing, but simple, locally valid IDs
- Example: directed diffusion
  - Interest Messages
    - Interest in sensor data: Attribute/Value pair
    - Gradient: remember direction of interested node
  - Data Messages
    - Send back data using gradients
    - Hop count guarantees shortest path



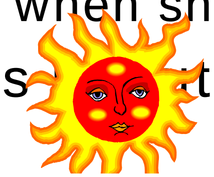
Energy-aware routing

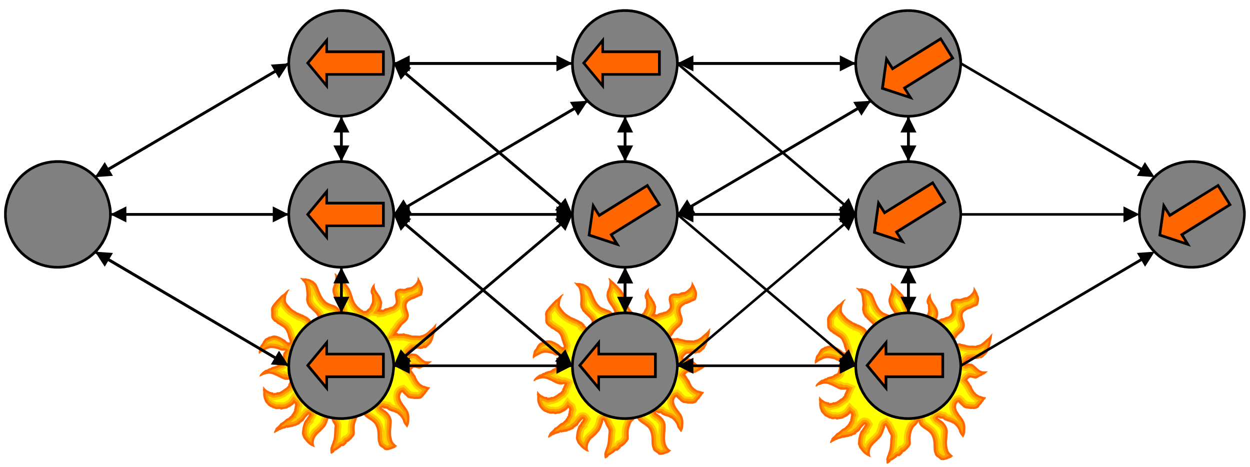
- Only sensors with sufficient energy forward data for other nodes
- Example: Routing via nodes with enough solar power is considered “for free”

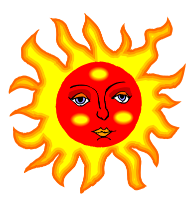


Solar-aware routing

- Solar-powered node
  - Send status updates to neighbors
    - Either proactive or when sniffing ongoing traffic
  - Have neighbor nodes route the traffic







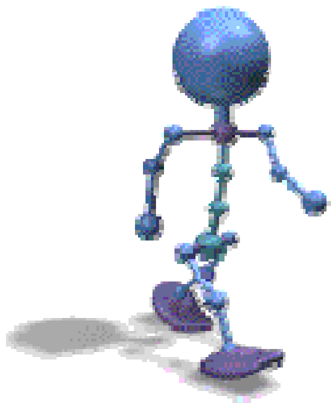
Many different “steps”

- Walking
  - At least one foot on the ground
  - Low step frequency

- Running
  - Periods without ground contact
  - Similar to jumping
  - Higher step frequency, wider steps

- Sprinting
  - Similar to running
  - Highest step frequency
  - Only short distances

- What about crawling, jumping, stumbling…



The Future of WSNs

- Fundamental requirements today only partially fulfilled
  - Long life-time with/without batteries
  - Self-configuring, self-healing networks
  - Robust routing, robust data transmission
  - Management and integration
- Think of new applications
  - Intelligent environments for gaming
  - … <your idea here>
- Still a lot to do…
  - Integration of new/future radio technologies
  - Cheap indoor localization (+/- 10cm)
  - More system aspects (security, middleware, …)
  - Prove scalability, robustness
  - Make it cheaper, simpler to use
- Already today: Flexible add-on for existing environmental monitoring networks