Mobile Communications Chapter 8: 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 => change of IP address to have a topological correct address (standard IP)

Solution: Temporarily change routing table entries for mobile host

- Problem: does not scale if many mobile hosts or frequent location changes

Solution: Change mobile host IP-address

- adjust the host IP address depending on the current location
- DNS updates take to long time
- Old TCP connections break

Requirements to Mobile IP (RFC 3344, was: 3220, was: 2002)

Transparency

- mobile end-systems keep IP address
- Continuous service after link interruption
- point of connection to the fixed network can be changed

Compatibility

- No changes to current hosts, OS, routers
- mobile end-systems can communicate with fixed systems

Security

- authentication of all registration messages

Efficiency and scalability

- only few additional messages to mobile system (low bandwidth)
- Global support for large number of mobile systems

Terminology

Mobile Node (MN)

- ❑ Laptop, PDA, etc.. that may move about

Home Agent (HA)

- ❑ Router in home network of the MN, helps in forwarding
- ❑ registers current MN location, tunnels IP datagrams to COA

Foreign Agent (FA)

- ❑ Router in current foreign network of MN
- ❑ forwards tunneled datagrams to the MN

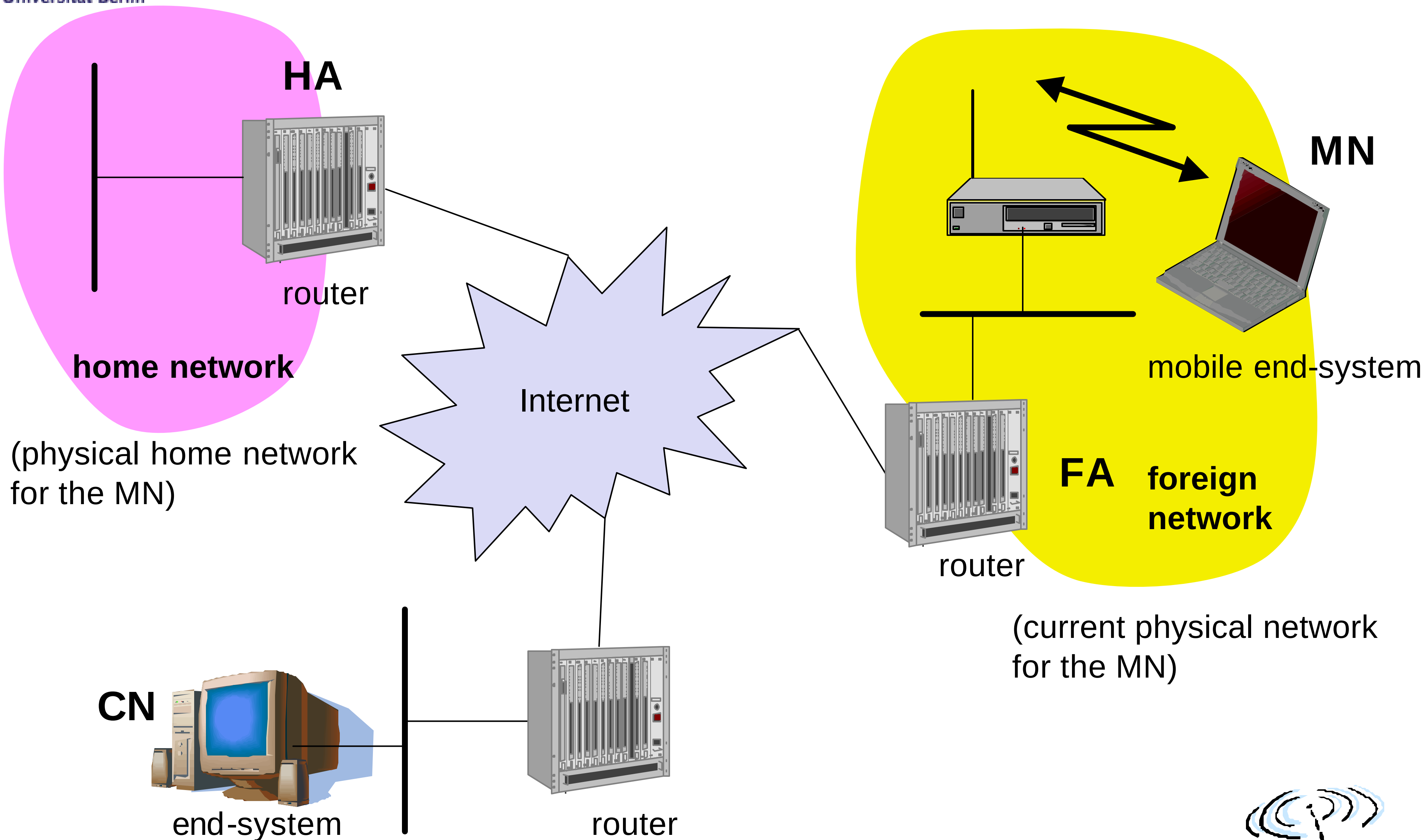
Care-of Address (COA)

- ❑ address of the current tunnel end-point for the MN (at FA or MN)
- ❑ can be chosen, e.g., via DHCP

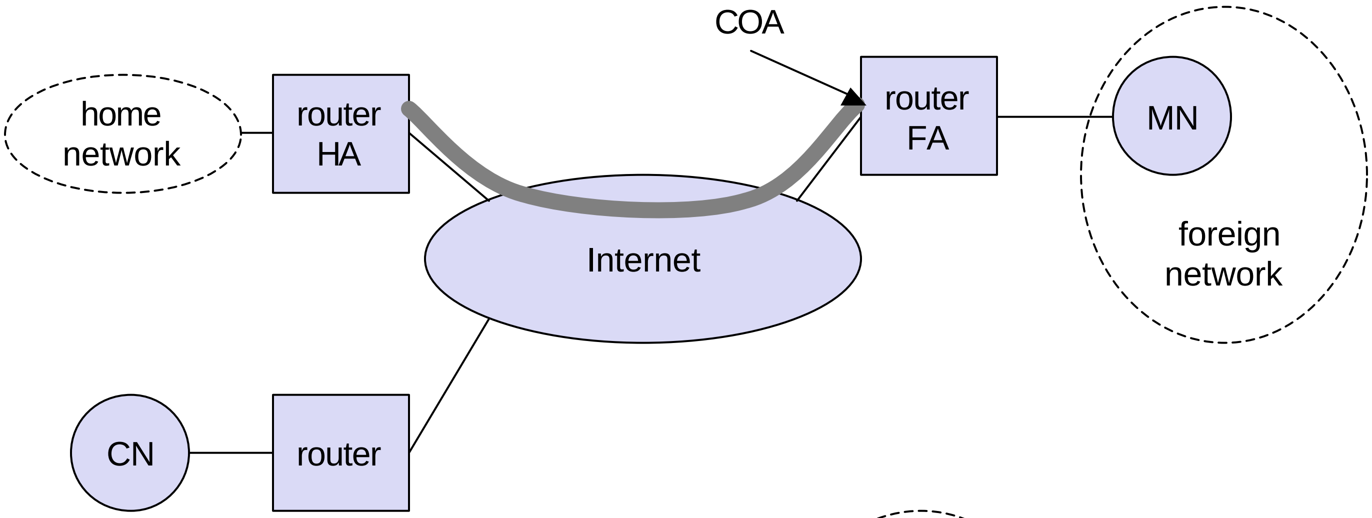
Correspondent Node (CN)

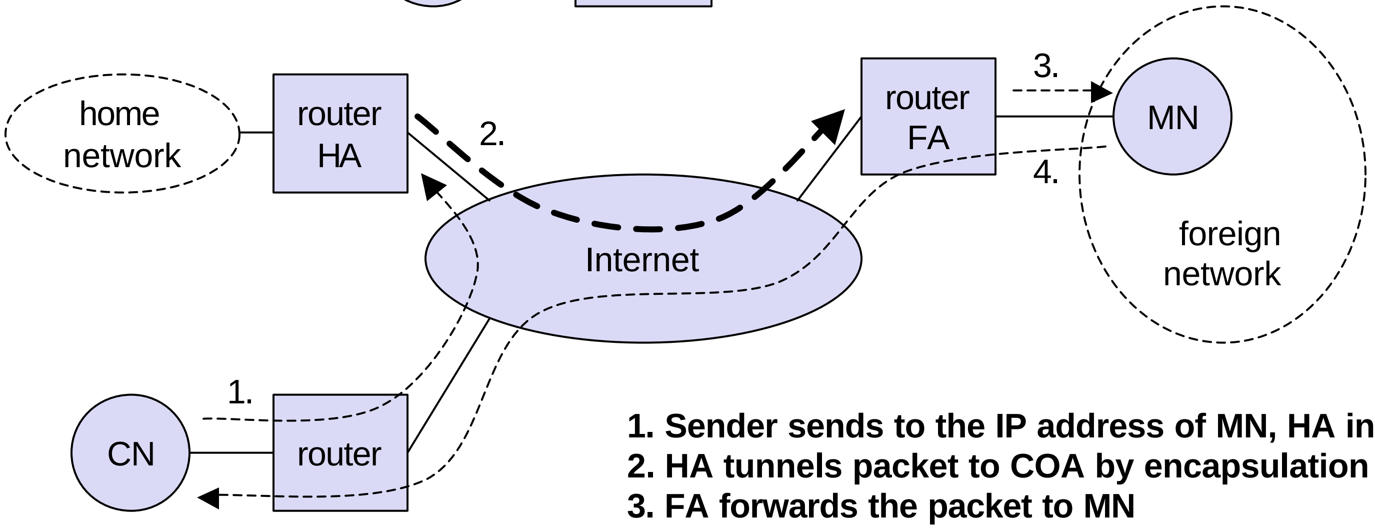
- ❑ Node that wants to communicate with MN

Example network



Overview





1. Sender sends to the IP address of MN, HA intercepts packet
2. HA tunnels packet to COA by encapsulation
3. FA forwards the packet to MN
4. Reverse: Sender sends to IP address of receiver, FA is default router

Network integration

Agent Advertisement

- HA and FA periodically send advertisement messages into their subnets
- MN reads a COA from the FA advertisement messages

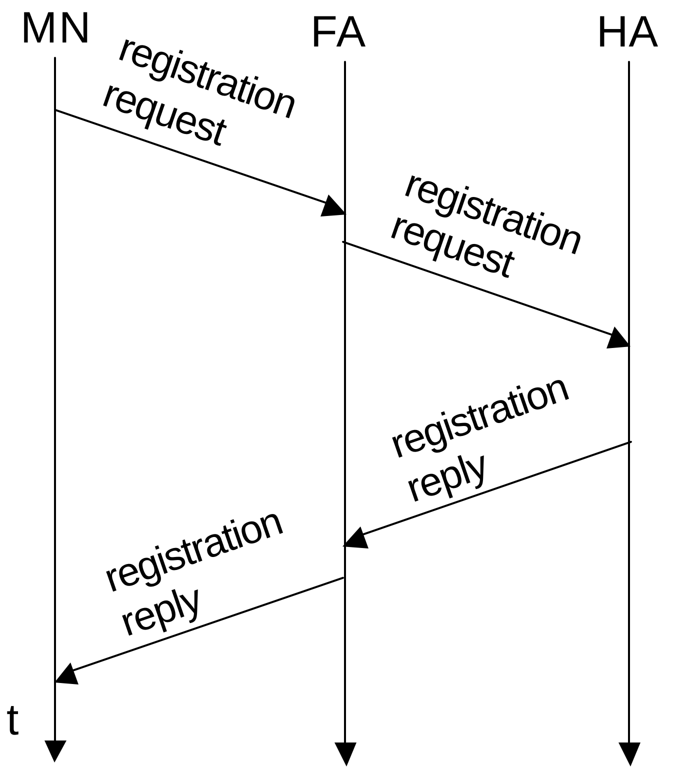
Registration (always limited lifetime!)

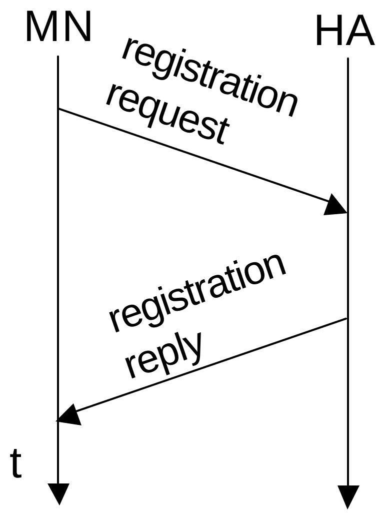
- MN signals COA to the HA via the FA, HA acknowledges
- Messeges need to be secured by authentication

Advertisement

- HA advertises the MN IP address (as for fixed systems)
- routers adjust their entries, (HA responsible for a long time)
- All packets to MN are sent to HA

Registration

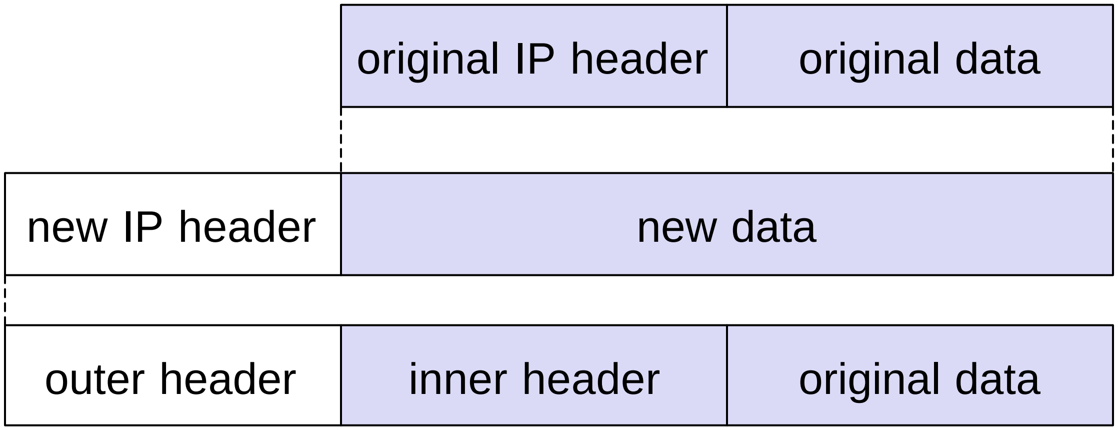




Encapsulation

Encapsulation of one packet into another as payload

- ❑ e.g. IP-in-IP-encapsulation (mandatory, RFC 2003)
- ❑ tunnel between HA and COA



original IP header | original data

new IP header | new data

outer header | inner header | original data

Optimization of packet forwarding

Triangular Routing

- sender sends all packets via HA to MN
- Triangular routes longer, higher latency and network load

“Solutions”

- HA informs a sender about the location of MN
- sender learns current location of MN
- direct tunneling to this location
- 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 forwards remaining packets to new FA
- Update also enables old FA to release resources for MN

Mobile IP and IPv6

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

- security is integrated, not add-on, authentication of registration included
- COA can be assigned via auto-configuration (DHCPv6 is one candidate)
- every node has address autoconfiguration
- no need for a separate FA, **all** routers perform router advertisement
- MN can signal a sender directly the COA, without HA
- „soft“ hand-over, i.e. without packet loss supported
    - MN sends the new COA to its old router
    - old router encapsulates all packets for MN, forwards them to new COA
    - authentication is always granted

Problems with mobile IP

Security

- FA typically belongs to another organization
- authentication with FA problematic
- patent and export restrictions

Firewalls

- Firewalls filter based on IP addresses
- FA encapsulates packets from MN
- Home firewalls rejects packet from MN (unless reverse tunneling)
- MN can no longer send packets back to home network

QoS, etc..

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

IP Micro-mobility support

Micro-mobility support:

- Efficient local handover inside foreign domain without involving a home agent
- Reduces control traffic on backbone
- Especially needed for route optimization

Example approaches:

- Cellular IP
- HAWAII
- Hierarchical Mobile IP (HMIP)

Cellular IP

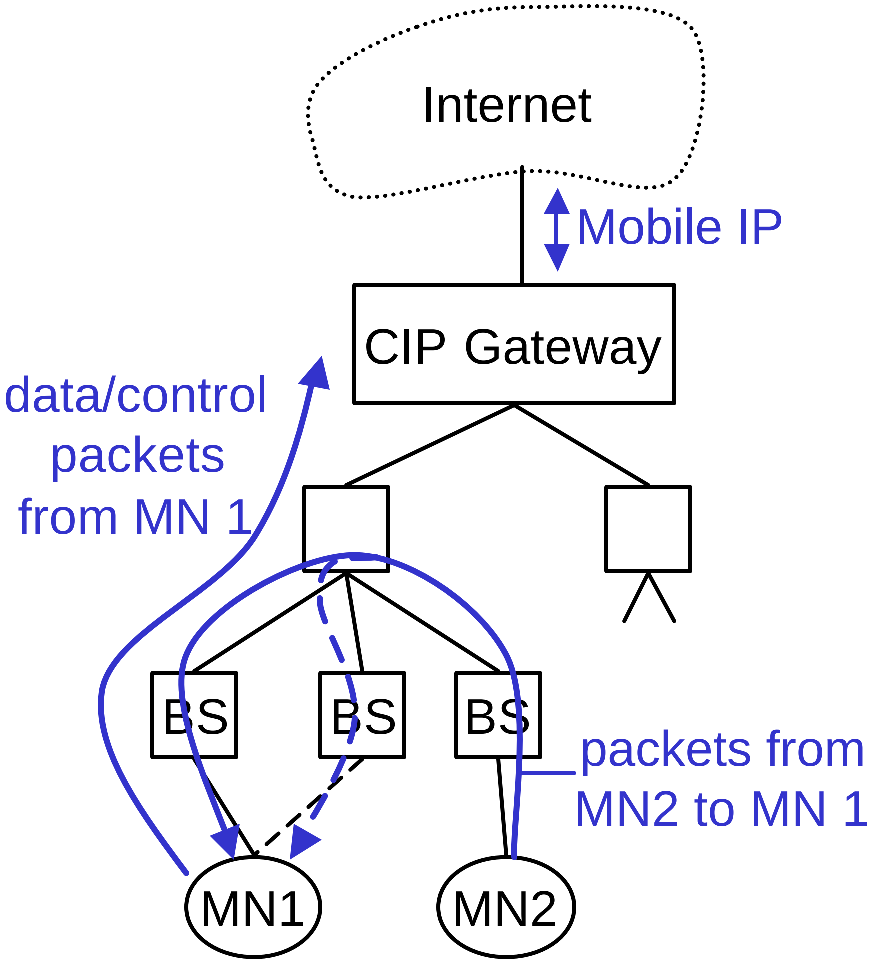
Operation:

- „CIP Nodes“ maintain routing entries (soft state) for MNs
- Multiple entries possible
- Routing entries updated based on update packets sent by MN

CIP Gateway:

- Mobile IP tunnel endpoint
- Initial registration processing

- Other micromobility protocols
  - HAWAII
  - Hierarchical Mobile IPv6 (HMIPv6)



DHCP: Dynamic Host Configuration Protocol

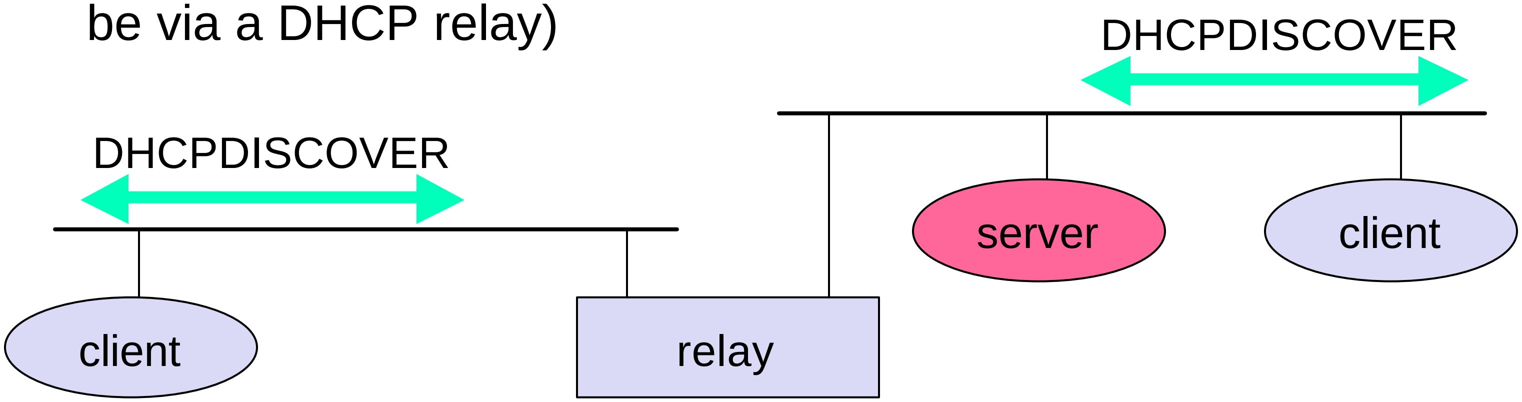
Main idea: E.g WPI has pool of IP addresses it can “lease” to hosts for short term use, claim back when done

Application

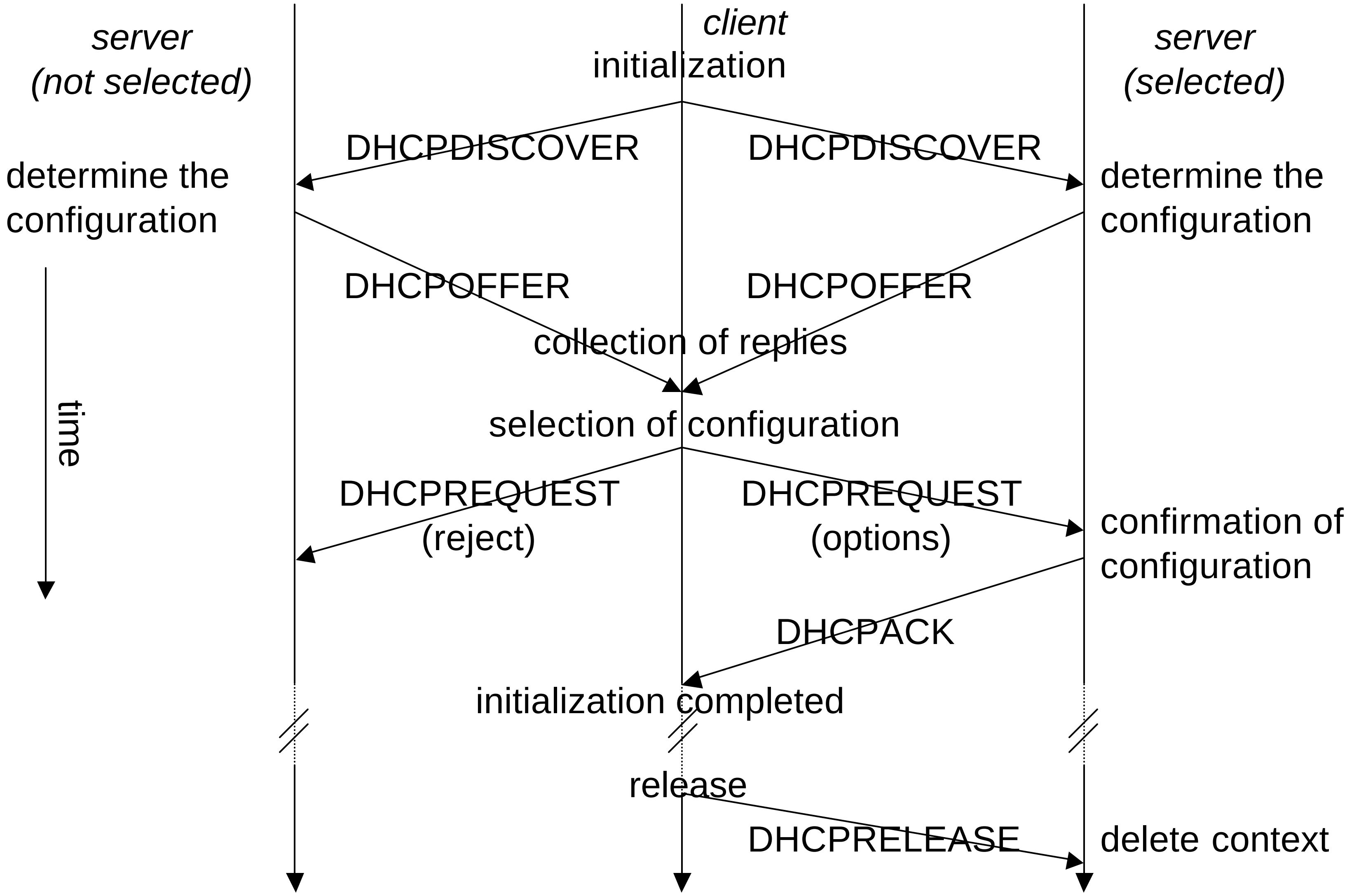
- simplification of installation and maintenance of networked computers
- supplies systems with all necessary information, such as IP address, DNS server address, domain name, subnet mask, default router etc.
- enables automatic integration of systems into an Intranet or the Internet, can be used to 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

Big security problems!

- no authentication of DHCP information specified

Mobile ad hoc networks

Standard Mobile IP needs an infrastructure

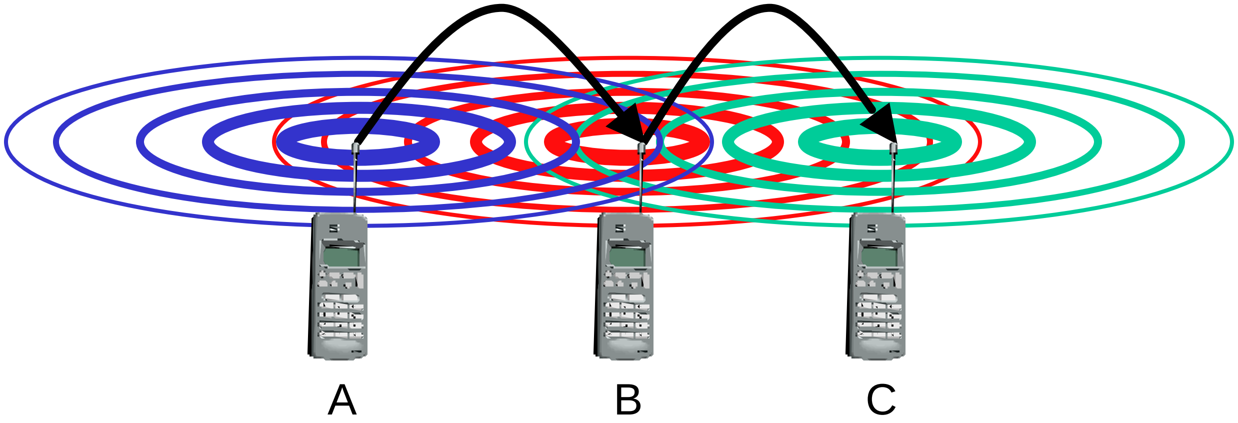
- ❑ Home Agent/Foreign Agent in the fixed network
- ❑ DNS, routing etc. not designed for mobility

Sometimes there is no infrastructure!

- ❑ remote areas, ad-hoc meetings, disaster areas
- ❑ cost can also be argument against infrastructure!

Main topic: routing

- ❑ no default router available
- ❑ every node should be able to forward



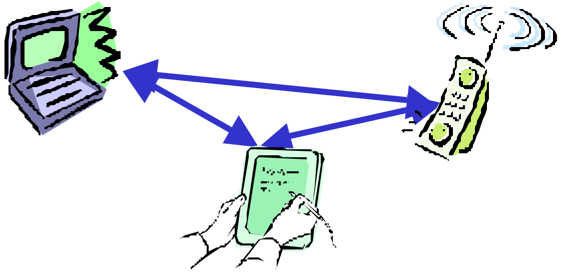
Solution: Wireless ad-hoc networks

Network without infrastructure

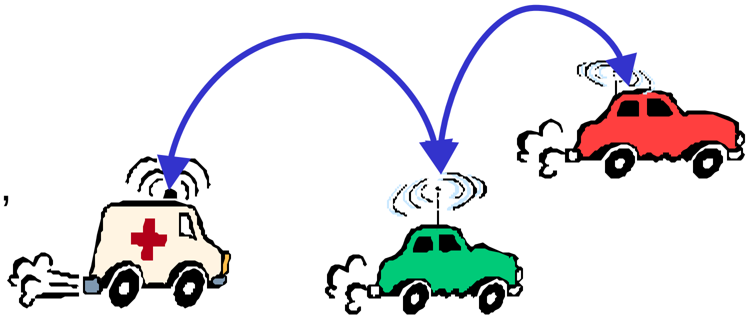
- ❑ Use components of participants for networking

Examples

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

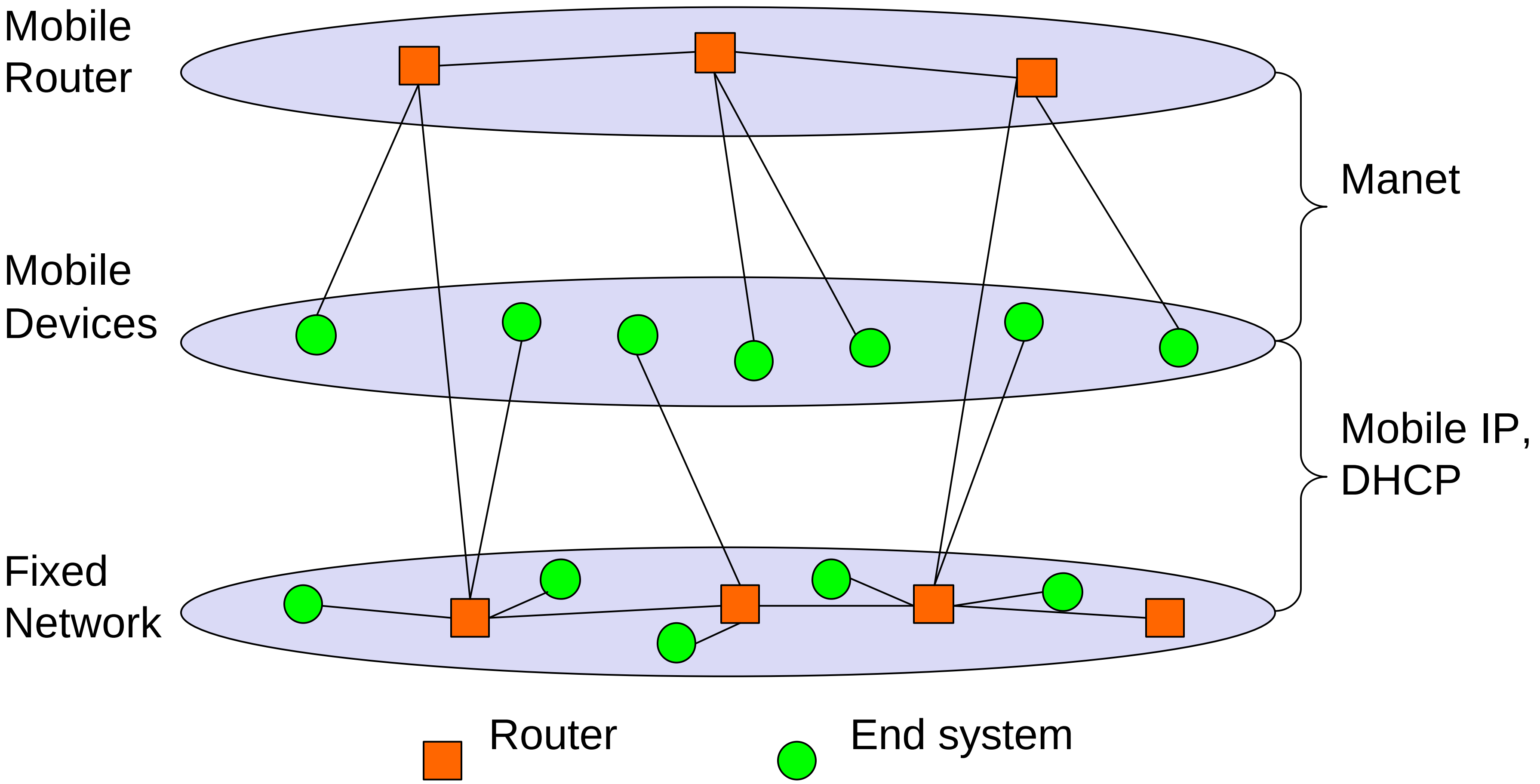


- ❑ Multi-hop: Cover larger distances, circumvent obstacles
  - Bluetooth scatternet, TETRA police network, car-to-car networks…



Internet: MANET (Mobile Ad-hoc Networking) group

Manet: Mobile Ad-hoc Networking



Mobile Router

Mobile Devices

Fixed Network

Manet

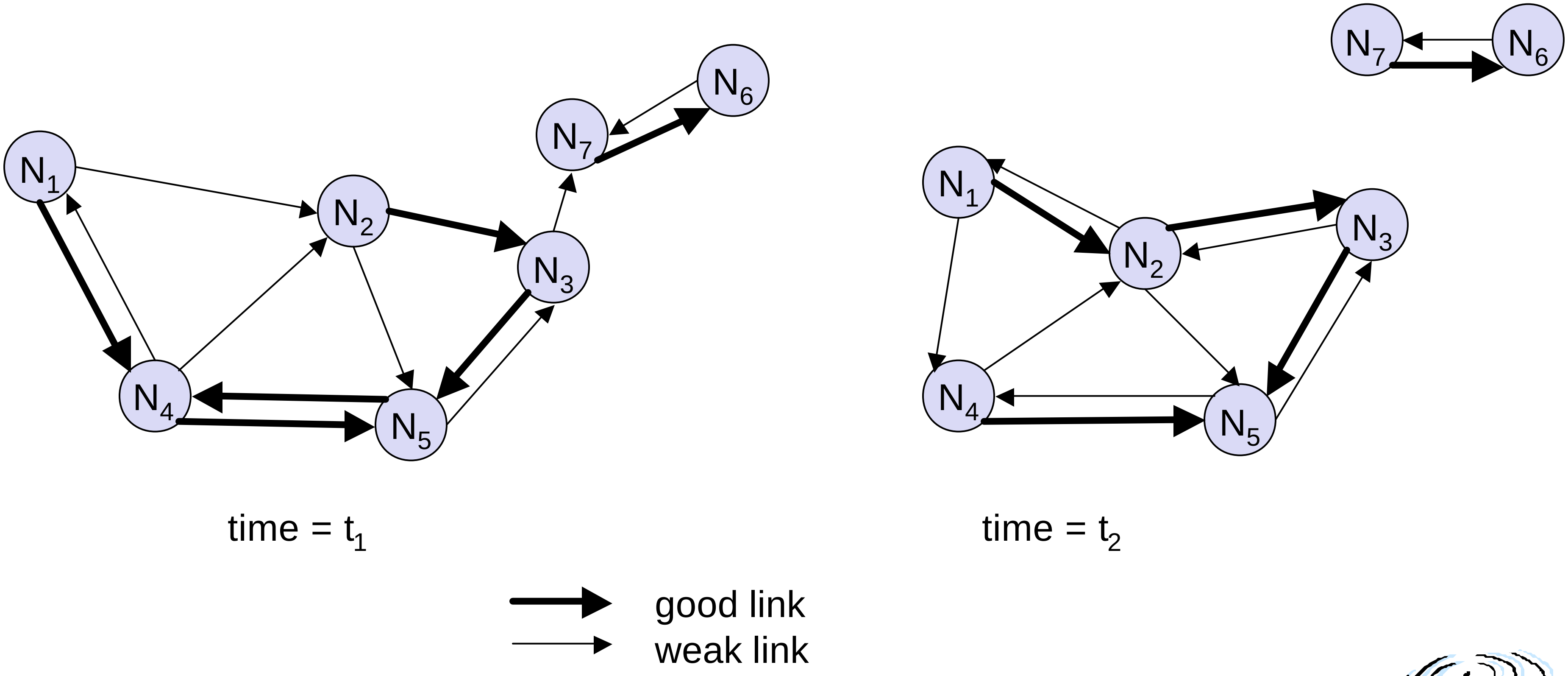
Mobile IP, DHCP

■ Router

● End system

Problem No. 1: Routing

- Highly dynamic network topology
  - Device mobility *and* varying channel quality
  - Asymmetric connections possible



time = t_1

time = t_2

Traditional routing algorithms

Distance Vector

- periodic exchange of cost to everyone else, with neighbors
- selection of shortest path if several paths available

Link State

- periodic notification of all routers about the current cost to neighbors
- routers get a complete picture of the network, run Djikstra’s algorithm

Example

- ARPA packet radio network (1973), DV-Routing
- every 7.5s exchange of routing tables including link quality
- Receive packets, update tables

Routing in ad-hoc networks

THE big topic in many research projects

- Far > 50 different proposals exist
- The most simplest one: Flooding!

Reasons

- Classical approaches from fixed networks fail
  - Fast link quality changes, slow convergence, large overhead
- Highly dynamic, low bandwidth, low computing power

Metrics for routing

- Minimize
  - Number of hops, loss rate, delay, congestion, interference …
- Maximal
  - Stability of 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 routing table updates need energy, sleep modes difficult
- limited bandwidth further reduced due to routing info exchange
- links can be asymmetric, directional transmission quality

DSDV (Destination Sequenced Distance Vector)

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 receiver (i.e., has the correct destination address) then return packet to the sender (path was collected in the packet)
  - if the packet already 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) received
  - stations can use the cached information for path discovery (own paths or paths for other hosts)

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

Examples for interference based routing

Routing based on assumptions about interference between signals

Examples

- □ Least Interference Routing (LIR)
- □ Max-Min Residual Capacity Routing (MMRCR)
- □ Least Resistance Routing (LRR)

A plethora of ad hoc routing protocols

Flat

- ❑ proactive
  - FSLS – Fuzzy Sighted Link State
  - FSR – Fisheye State Routing
  - OLSR – Optimised Link State Routing Protocol
  - TBRPF – Topology Broadcast Based on Reverse Path Forwarding
- ❑ reactive
  - **AODV** – Ad hoc On demand Distance Vector
  - DSR – Dynamic Source Routing

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

Further difficulties and research areas

Auto-Configuration

- ❑ Assignment of addresses,

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

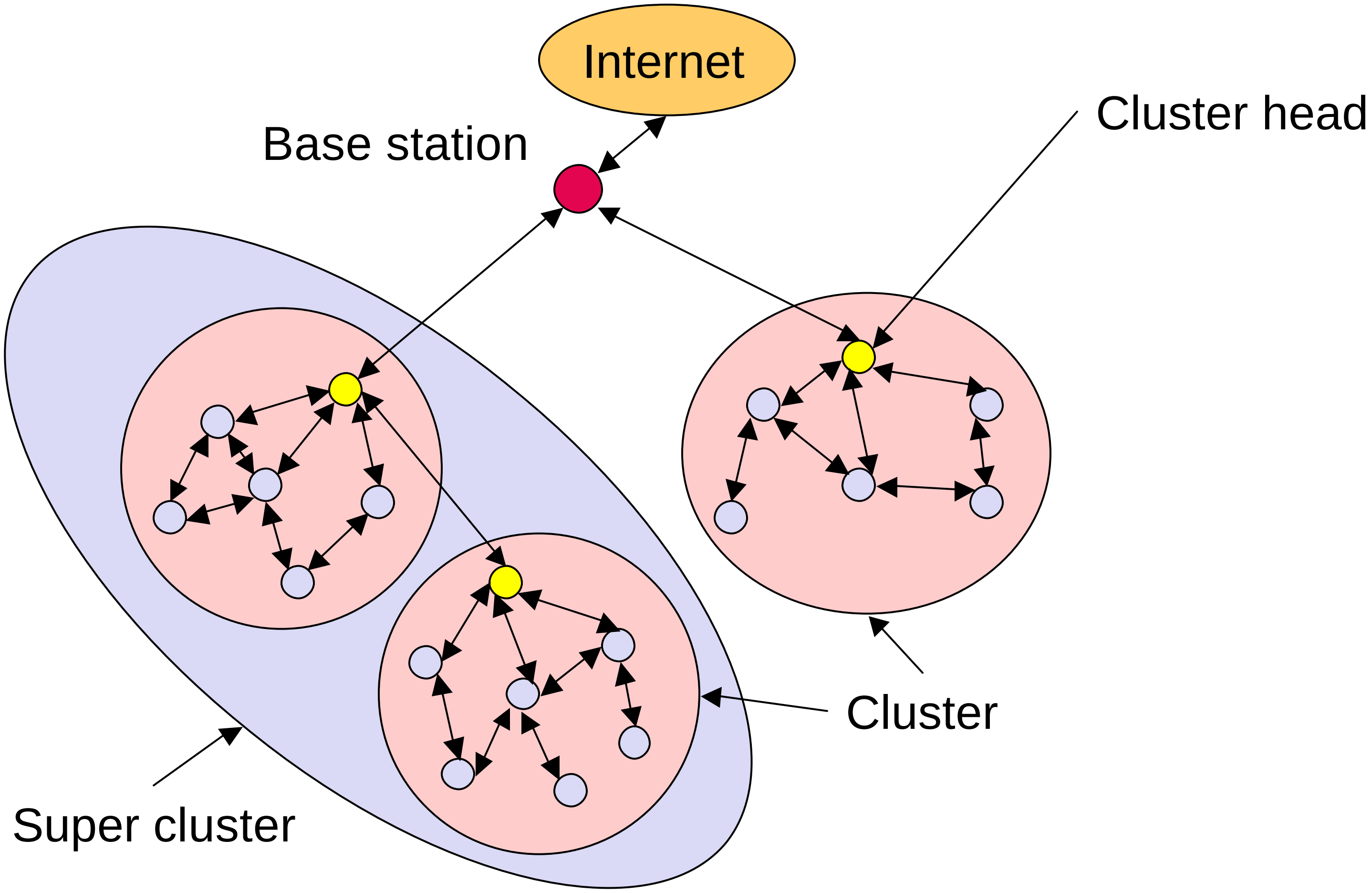
- ❑ Data integrity, protection from attacks (e.g. Denial of Service)

Scalability

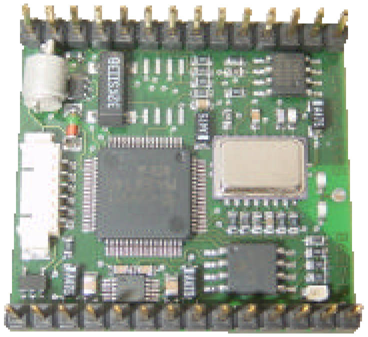
- ❑ 10 nodes? 100 nodes? 1000 nodes? 10000 nodes?

Integration with fixed networks

Clustering of ad-hoc networks



The next step: Wireless Sensor Networks (WSN)



Main idea thousands of networked sensors thrown into phenomenon to be sensed

Example: www.scatterweb.net

Commonalities with MANETs

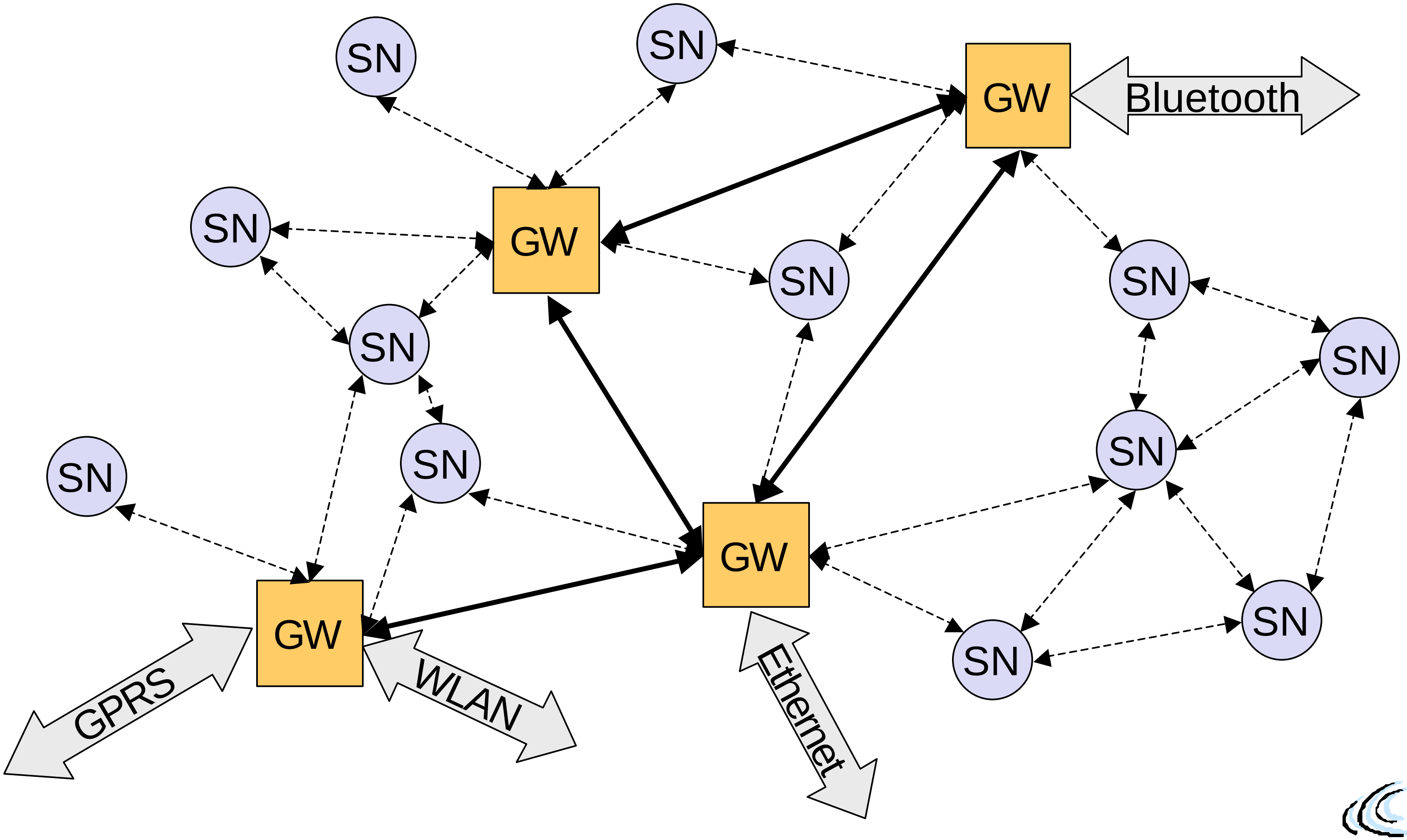
- ❑ Self-organization, multi-hop
- ❑ Typically wireless, should be energy efficient

Differences from 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** …

A typical WSN

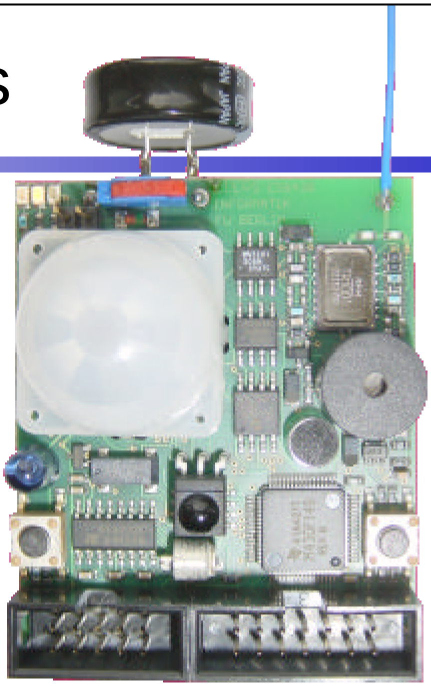
Integration of Sensor Nodes (SN) and Gateways (GW)



Example: ScatterWeb Sensor Nodes

Embedded Sensor Board

- ❑ Sensors
  - ● Luminosity, noise detection, gas, vibration, PIR movement detection, pressure…
- ❑ Microphone/speaker, camera, display, IR sender/receiver, precise timing
- ❑ Communication using 868 MHz radio transceiver
  - ● Range up to 2 km LOS, 500 m indoor
- ❑ Software
  - ● Simple programming (C interface)
  - ● Optional: operating systems TinyOS, Contiki …
  - ● Optional: TCP/IP, web server …
  - ● Routing, management, flashing …



Embedded Sensor Board

Modular Sensor Node

Further information:
www.scatterweb.net

Sensor Networks: Challenges and Research Areas

Long-lived, autonomous networks

- ❑ Use environmental energy sources
- ❑ Embed and forget
- ❑ Self-healing

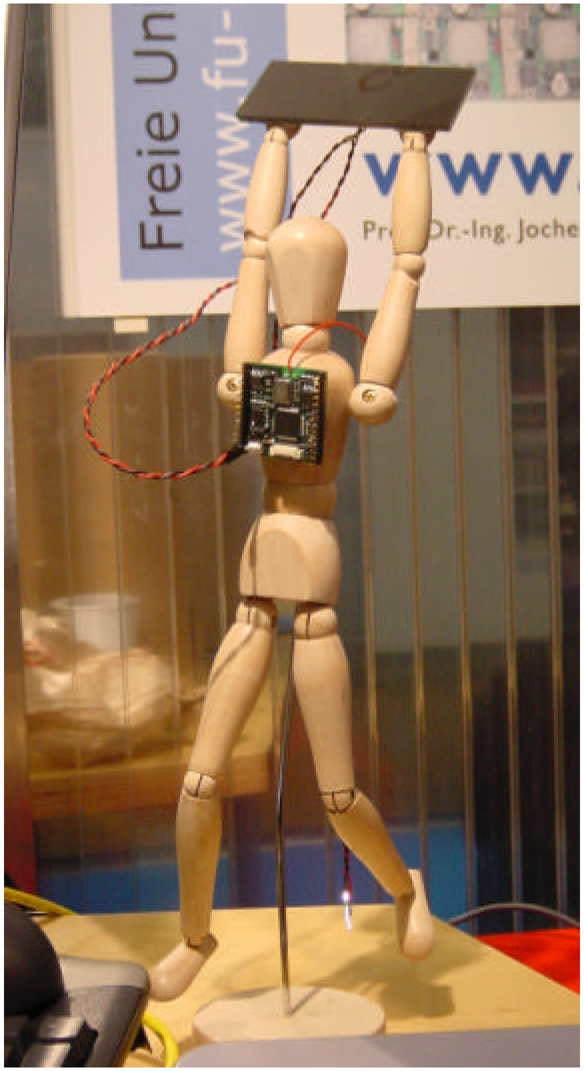
Self-configuring networks

- ❑ Routing
- ❑ Data aggregation
- ❑ Localization

Managing wireless sensor networks

- ❑ Tools for access and programming
- ❑ Update distribution

Scalability, Quality of Service…



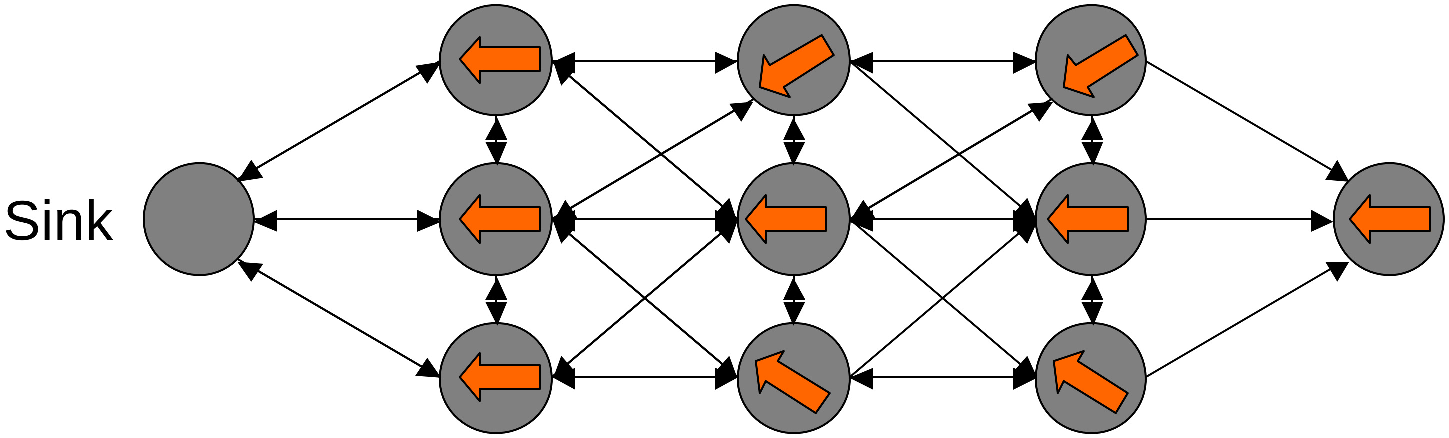
veritas
iustitia
libertas
Freie Universität Berlin

Routing in WSNs is different

No IP addressing, but simple, locally valid IDs

Example: directed diffusion

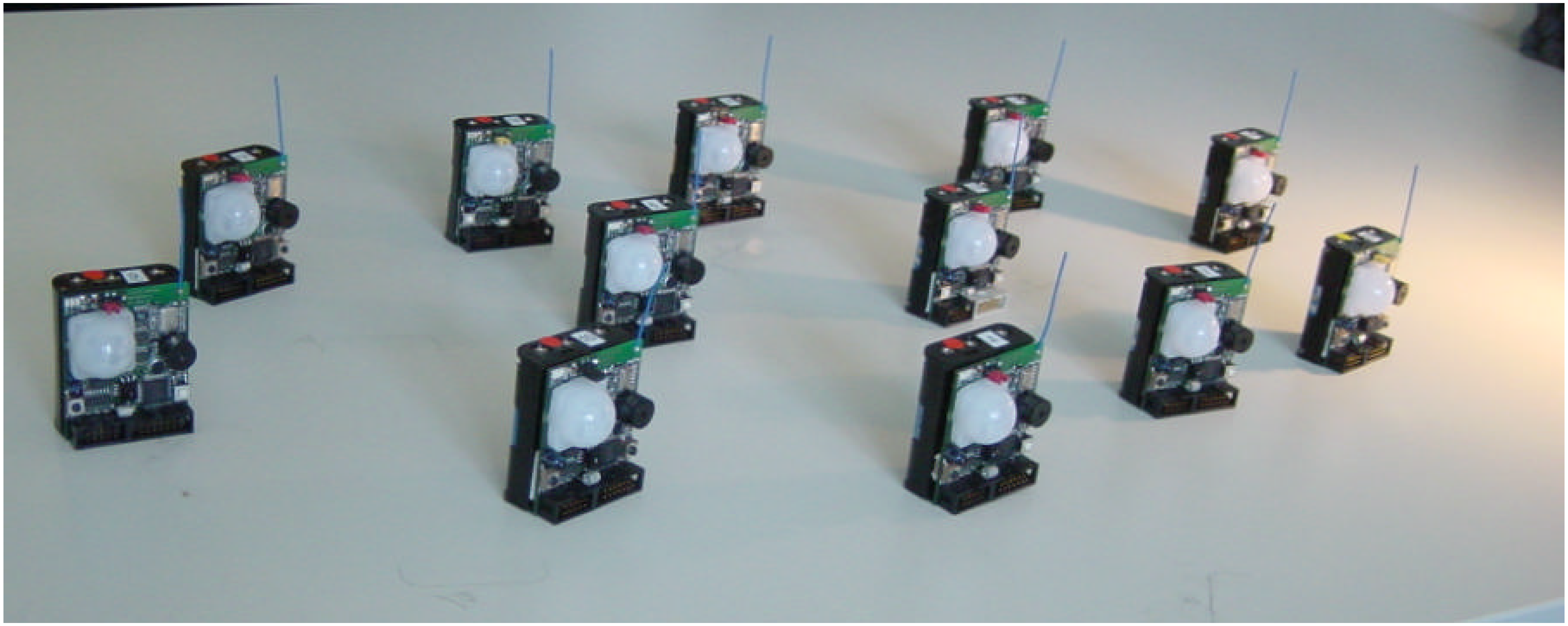
- ❑ Interest Messages
  - Interest in sensor data: Attribute/Value pair
  - Gradient: remember direction of interested node
- ❑ Data Messages
  - Send back data using gradients
  - Hop count guarantees shortest path



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”



Today's WSNs

First generation of WSNs is available

- Diverse sensor nodes, several gateways
- Even with special sensors: cameras, body temperature…
- Basic software
  - Routing, energy conservation, management

Several prototypes for different applications

- Environmental monitoring, industrial automation, wildlife monitoring …

Many see new possibilities for monitoring, surveillance, protection

- Sensor networks: cheap and flexible for surveillance
- Monitoring and protection of goods
  - Chemicals, food, vehicles, machines, containers, …
- Large application area besides military
  - Law enforcement, disaster recovery, industry, private homes, …