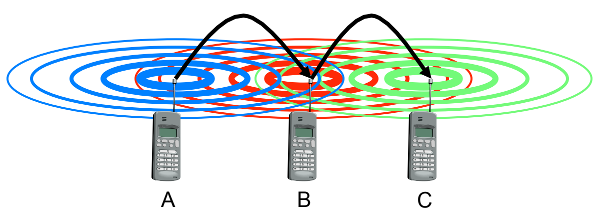
Mobile Ad Hoc Networks

Dominic Duggan
Based on materials by Jochen Schiller

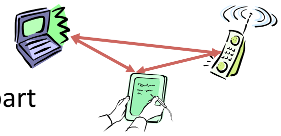
Motivation

- Standard Mobile IP needs an infrastructure
- Sometimes there is no infrastructure!
  - remote areas, ad-hoc meetings, disaster areas
- Main topic: routing
  - no default router available
  - every node should be able to forward

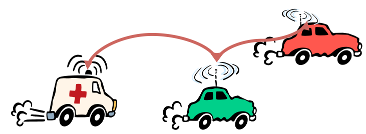


Mobile Ad Hoc Networks

- Network without infrastructure
  - Use components of participants for networking
- Examples
  - Single-hop: All partners max. one hop apart
    - Bluetooth piconet, gaming devices…



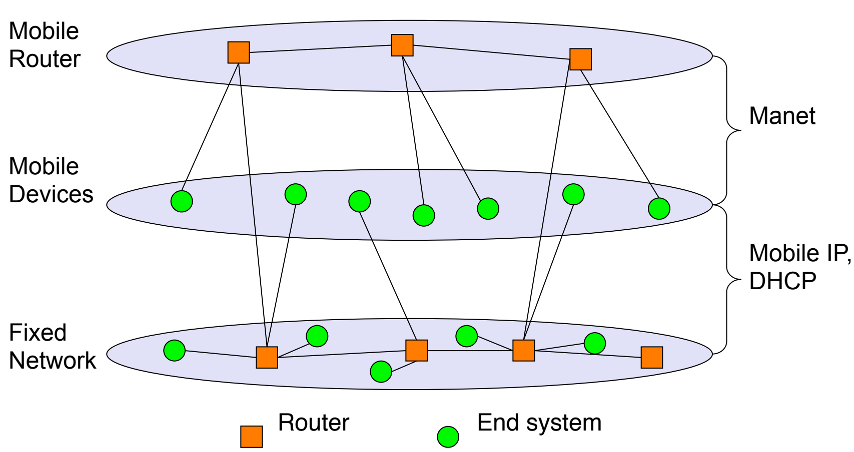
  - Multi-hop: Cover larger distances, circumvent obstacles
    - Bluetooth scatternet, TETRA police network, …



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

3

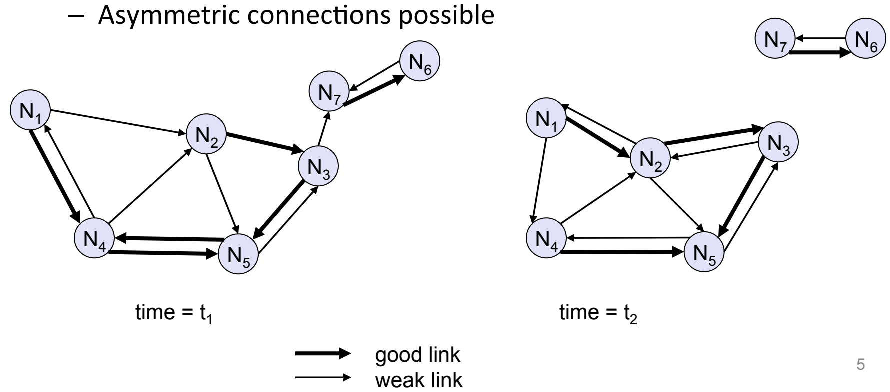
MANET: Mobile Ad-hoc Networking



4

Problem: 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
- Link State
  - periodic notification of all routers about the current state of all physical links
  - router gets 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

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
  - limited bandwidth reduced even more due to exchange
  - links can be asymmetric

7

Dynamic Source Routing I

- Split routing into discovering a path and maintaining a path
- Discover a path
  - only if no path is currently available
- Maintaining a path
  - only while the path is in use
- No periodic updates needed!

8

Dynamic source routing II

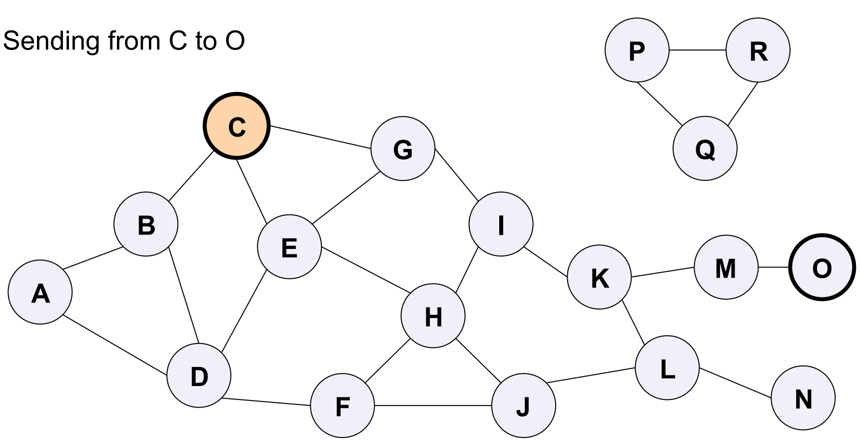
- Path discovery
  - broadcast a packet with destination address and unique ID
  - if a station receives a broadcast packet
    - if the station is the destination, then return the packet to the sender
    - if the packet already received (identified via ID) then discard
    - otherwise, append own address 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

9

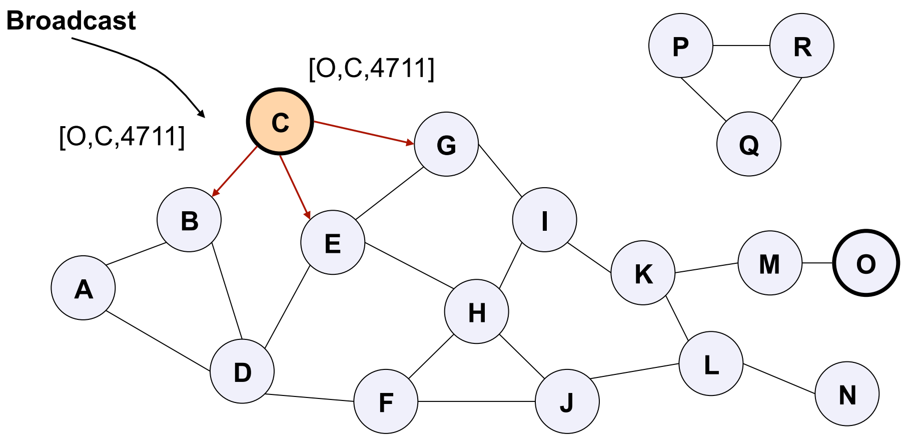
DSR: Route Discovery

Sending from C to O



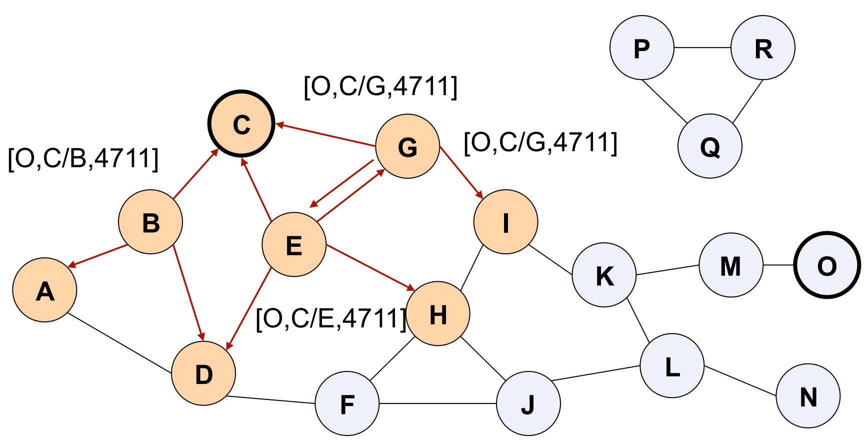
10

DSR: Route Discovery



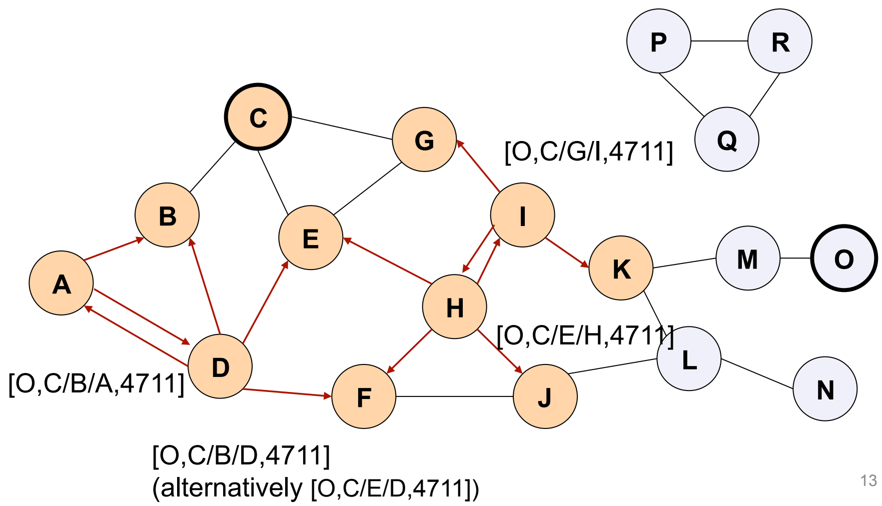
11

DSR: Route Discovery



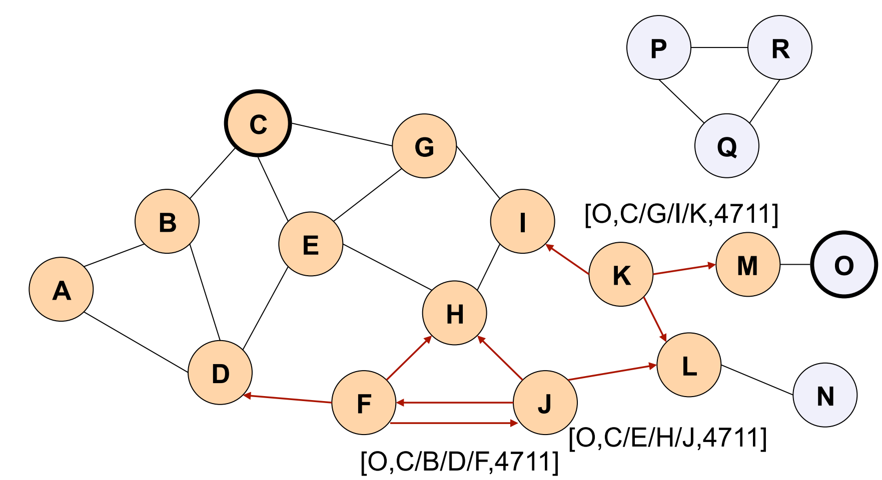
12

DSR: Route Discovery



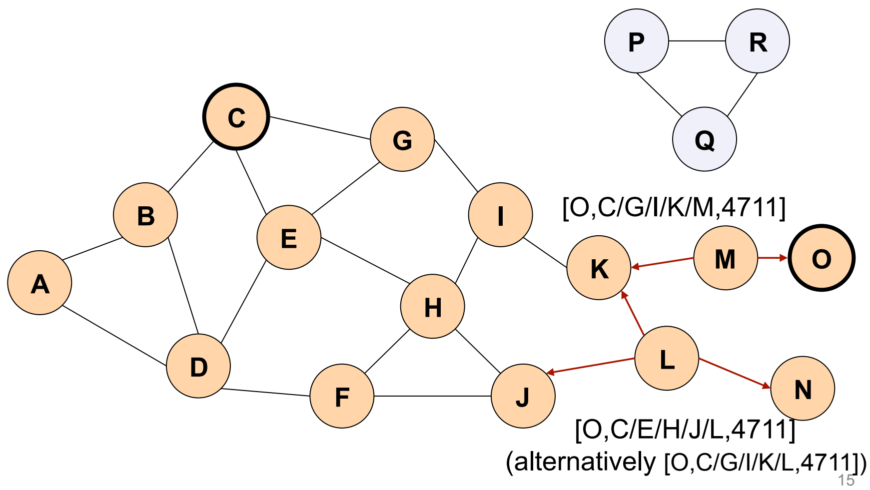
13

DSR: Route Discovery



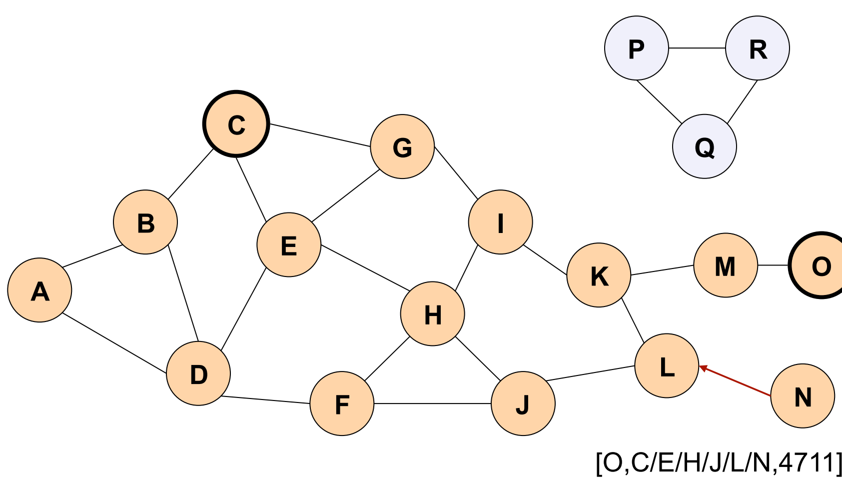
14

DSR: Route Discovery



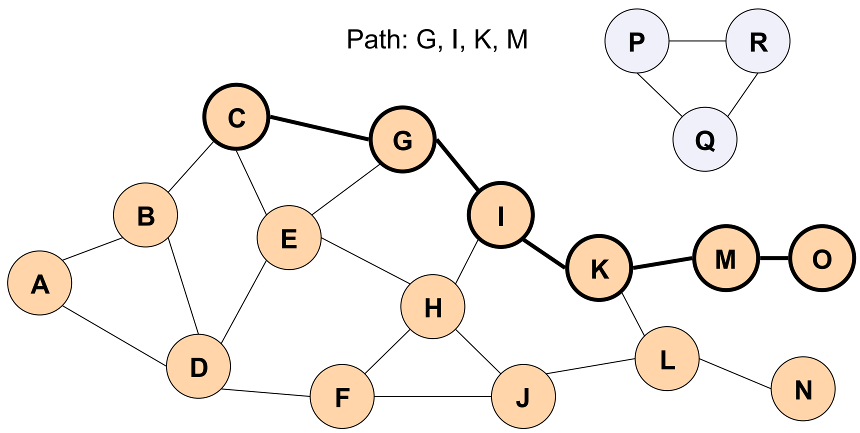
15

DSR: Route Discovery



16

DSR: Route Discovery



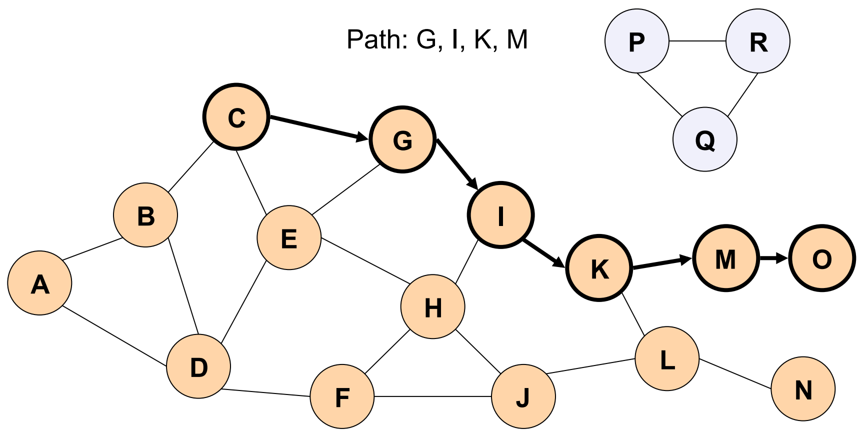
17

Dynamic Source Routing III

- Asymmetric Links
  - Links may not be symmetric
  - Only dest knows route from source to dest
- How does destination communicate route back to source?
  - Route discovery in reverse
    - Now source knows route from dest to source!

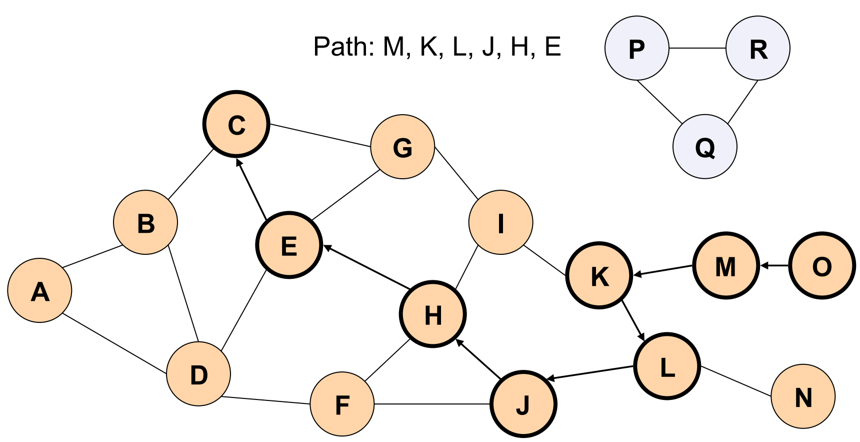
18

DSR: Route Discovery



19

DSR: Route Discovery



20

Dynamic Source Routing IV

- 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

21

Ad-Hoc On Demand Distance Vector (AODV)

- If node S has message for D, but no route:
  - Broadcasts / floods a route request (RREQ)
  - Eventually, either destination (D) or intermediate node with "fresh enough" route cache is reached

22

Ad-Hoc On Demand Distance Vector (AODV)

- If node S has message for D, but no route:
  - Broadcasts / floods a route request (RREQ)
  - Eventually, either destination (D) or intermediate node with "fresh enough" route cache is reached
- Each node maintains a sequence number as well as a broadcast ID
  - Broadcast ID is incremented for each RREQ
  - Combination of node address and broadcast ID uniquely identifies a RREQ

23

AODV

- Source RREQ also includes the most recent sequence number for the destination
  - Intermediate nodes can only respond if they have fresher information

24

AODV

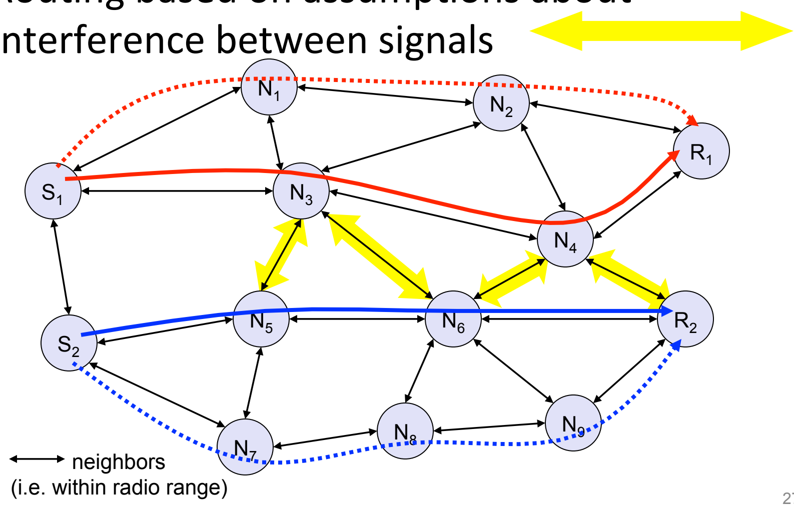
- Source RREQ also includes the most recent sequence number for the destination
  - Intermediate nodes can only respond if they have fresher information
- Route Reply (RREP) is sent back along the path by which each node received route request
  - Nodes in that route establish forward routes for the destination

AODV

- Advantage of AODV over DSR:
  - Packet header sizes are no longer proportional to the length of the path
- Disadvantage
  - Requires symmetric links

Interference-based routing

- Routing based on assumptions about interference between signals



27

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

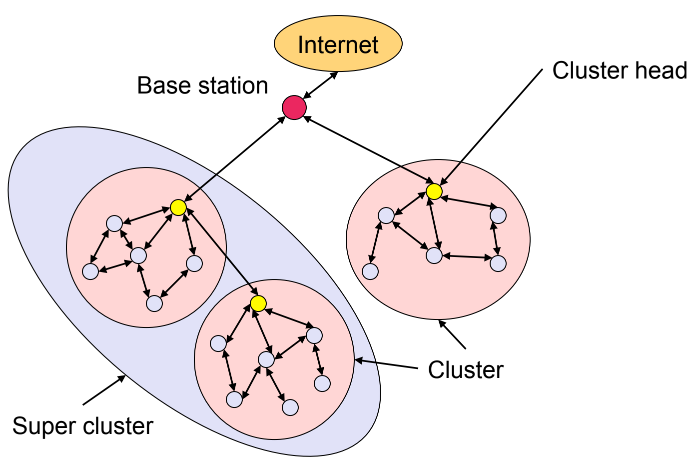
28

A plethora of ad hoc routing protocols

- 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

29

Clustering of ad-hoc networks



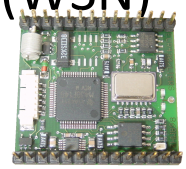
30

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

WIRELESS SENSOR NETWORKS

Wireless Sensor Networks (WSN)



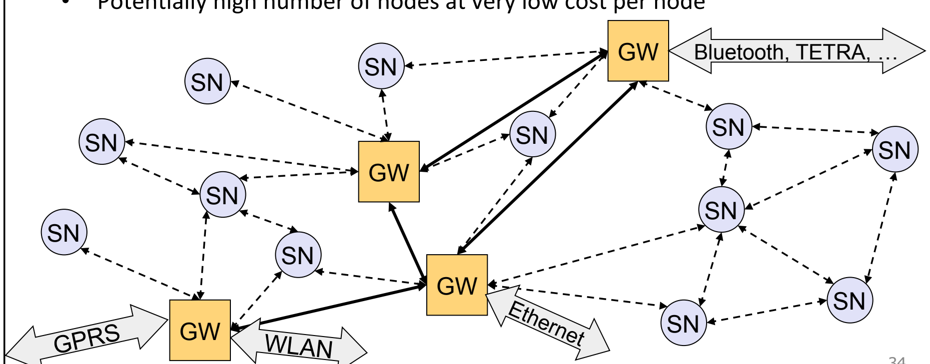
Example:
www.scatterweb.net

- 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** …

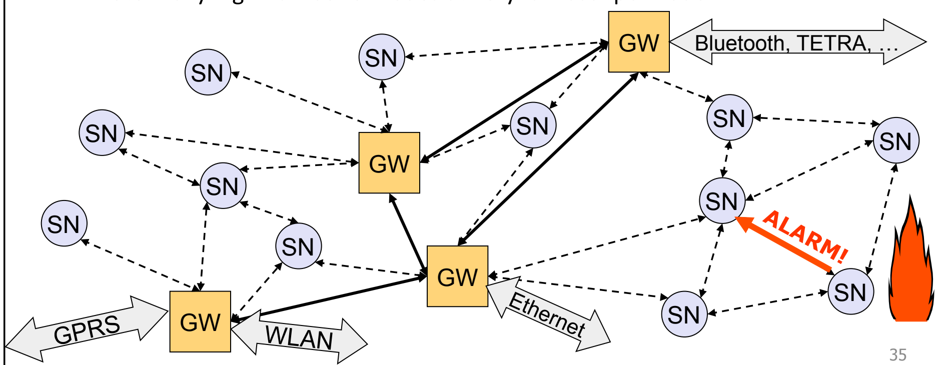
Properties of wireless sensor networks

- 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



Properties of wireless sensor networks

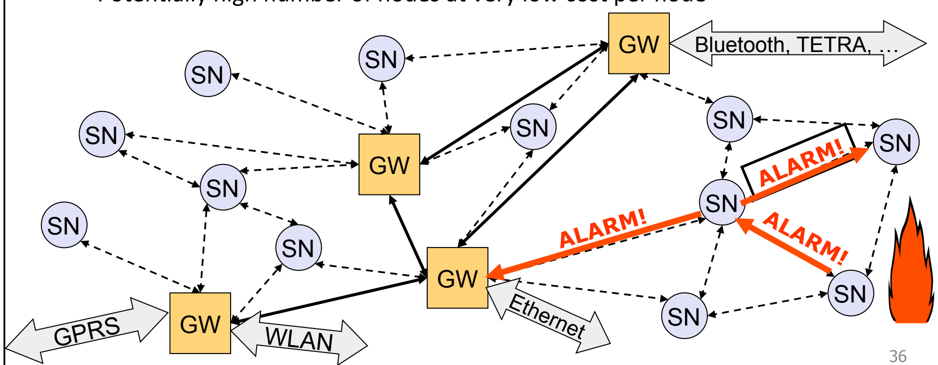
- Sensor nodes (SN) monitor and control the environment
- Nodes process data and forward data via radio
- Integration into the environment, typically attached to other networks over a gateway (GW)
- Network is self-organizing and energy efficient
- Potentially high number of nodes at very low cost per node



35

Properties of wireless sensor networks

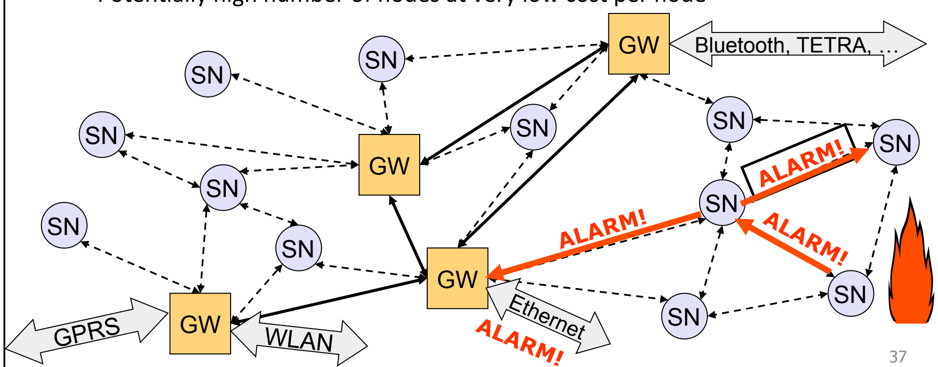
- Sensor nodes (SN) monitor and control the environment
- Nodes process data and forward data via radio
- Integration into the environment, typically attached to other networks over a gateway (GW)
- Network is self-organizing and energy efficient
- Potentially high number of nodes at very low cost per node



36

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



37

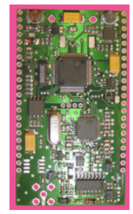
Possible applications for WSNs

- 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

38

Example: ScatterWeb

- Nodes
  - 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)
  - Sensors attached on demand: Acceleration, humidity, temperature, luminosity, noise detection, vibration, PIR movement detection…



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

39

Example: Habitat Monitoring—Skomer Island UK

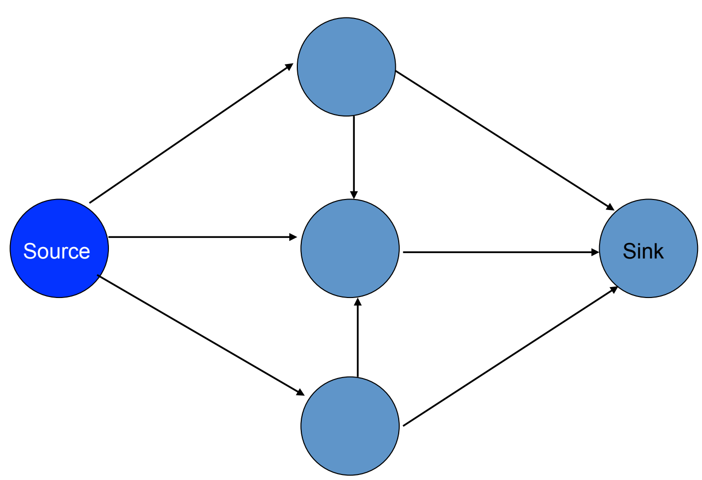
40

Routing in WSNs: Directed Diffusion

- No IP addressing, but simple, locally valid IDs
- Interest: A list of attribute-value pairs describing a task
- Sink: Node originating the interest
- Source: Sensor node that matches the interest, collects data and sends it back
- Gradient: Direction towards which data matching and interest flows and status of demand

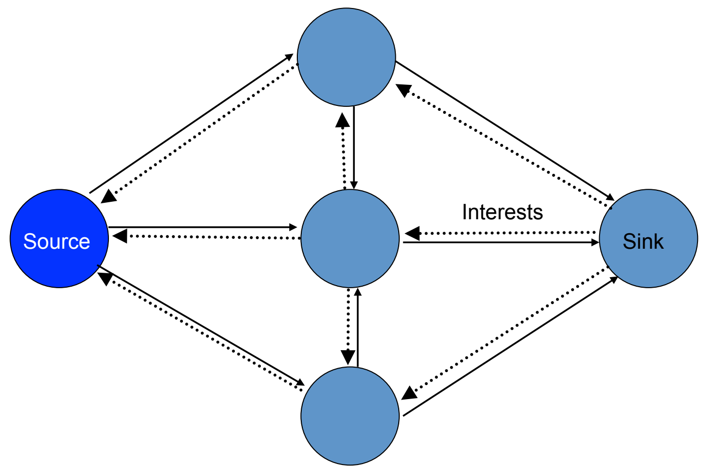
41

Directed Diffusion



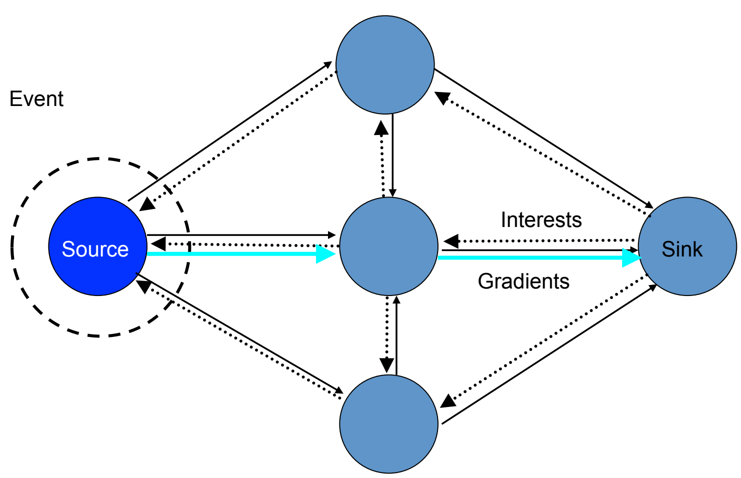
42

Directed Diffusion



43

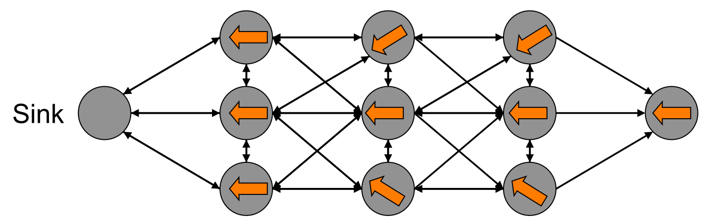
Directed Diffusion



44

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



45

Directed Diffusion

- Intermediary data is cached as it propagates from source to sink.
- Reinforcement
- Negative Reinforcement

46

Attribute Tuples & Matching Rules

- Interests and data messages are composed of attribute-value-operation tuples.
- Keys: Identify attributes. Drawn from central authority.
- Operations: Define interactions of data messages and interests. e.g. GT, LT, GE, LE, EQ, EQ_ANY, IS.
- Actual: Literal or bound value
- Formal: Comparison or unbound value.

47

Interactions of Diffusion & Matching

- Consider an example user query:

```
{class IS interesttype
IS four-legged-animal-search
interval IS 20ms
duration IS 10s
x GE -100
x LE 200
y GE 100
y LE 400}
```

- Sensor detects something it responds with

```
{class IS data
type IS four-legged-animal-search
instance IS elephant
x IS 125
y IS 220
intensity IS 0.6
confidence IS 0.85
timestamp IS 1:20}
```

48

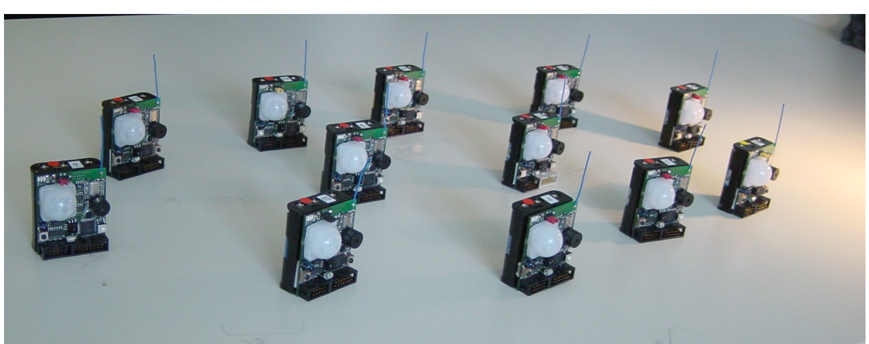
In-network data aggregation

- Multiple detection of target results in unnecessary communications.
- Energy can be conserved if data is aggregated:
  - Binary value – there was a detection.
  - An area – there was a detection in quadrant 2.
  - An application specific aggregation.
- Caching of data by intermediate sensors.

49

Energy-aware routing

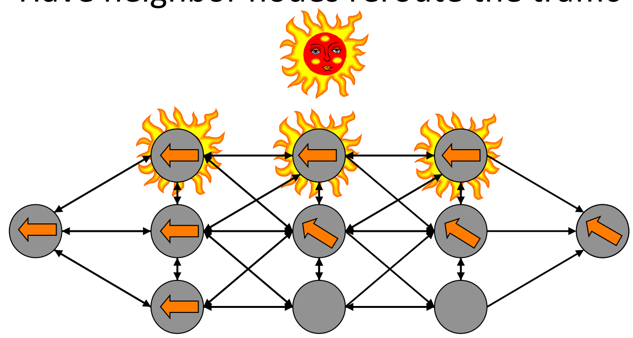
- Only sensors with sufficient energy forward data for other nodes
- Example: Routing via nodes with enough solar power is considered “for free”



50

Solar-aware Routing

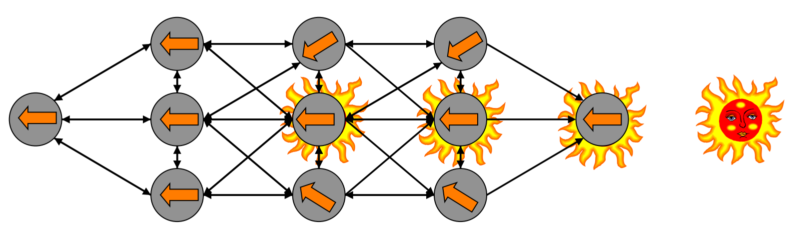
- Solar-powered node
  - Send status updates to neighbors
    - Either proactive or when sniffing ongoing traffic
  - Have neighbor nodes reroute the traffic



51

Solar-aware Routing

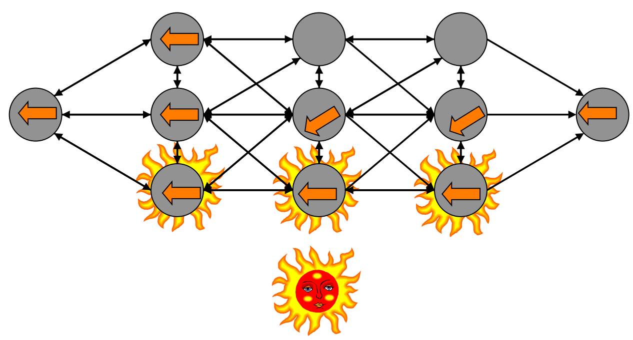
- Solar-powered node
  - Send status updates to neighbors
    - Either proactive or when sniffing ongoing traffic
  - Have neighbor nodes reroute the traffic



52

Solar-aware Routing

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



53

Conclusions

- Mobile ad-hoc networks
  - Mobile routers
- Sensor networks
  - Content-based, interest-based routing

54