Chapter 12: Introduction to Wireless Sensor Networks

Prof. **Yuh-Shyan Chen**

Department of Computer Science and Information Engineering

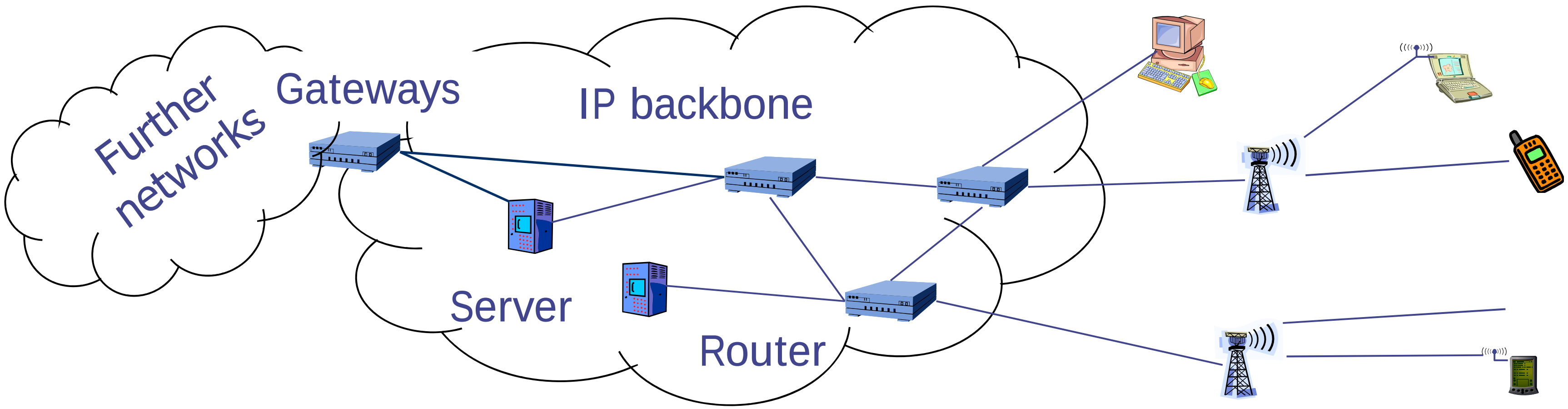
National Taipei University

Outline

- ***Infrastructure for wireless?***
- (Mobile) ad hoc networks
- Wireless sensor networks
- Comparison

Infrastructure-based wireless networks

- Typical wireless network: Based on infrastructure
  - E.g., GSM, UMTS, …
  - Base stations connected to a wired backbone network
  - Mobile entities communicate wirelessly to these base stations
  - Traffic between different mobile entities is relayed by base stations and wired backbone
  - Mobility is supported by switching from one base station to another
  - Backbone infrastructure required for administrative tasks

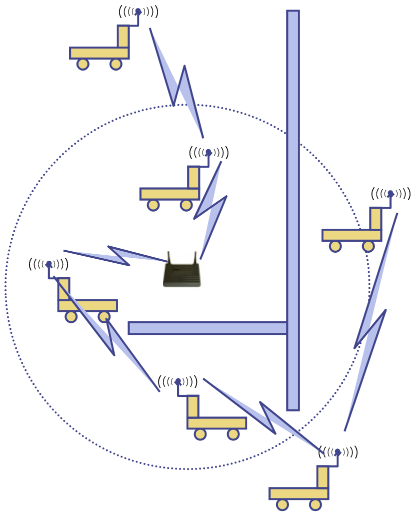


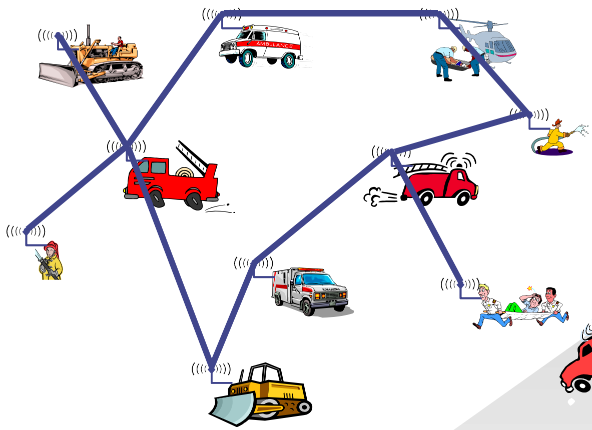
Infrastructure-based wireless networks – Limits?

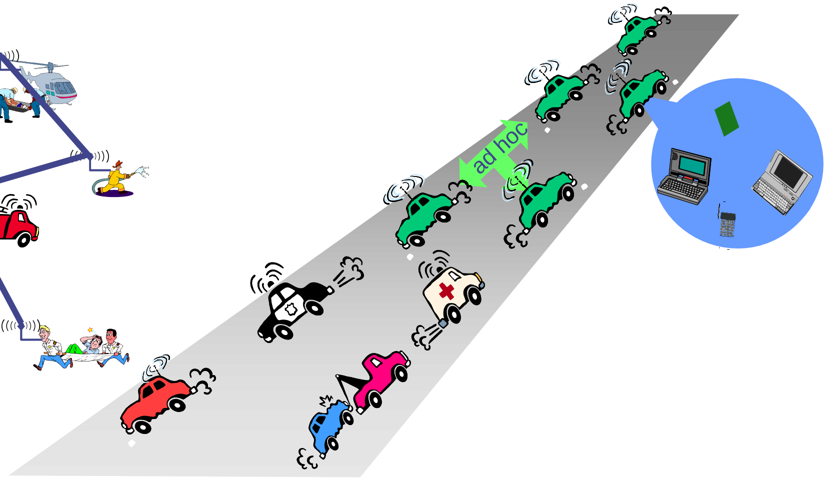
- What if …
  - No infrastructure is available? – E.g., in disaster areas
  - It is too expensive/inconvenient to set up? – E.g., in remote, large construction sites
  - There is no time to set it up? – E.g., in military operations

Possible applications for infrastructure-free networks

- Factory floor automation
- Disaster recovery
- Car-to-car communication

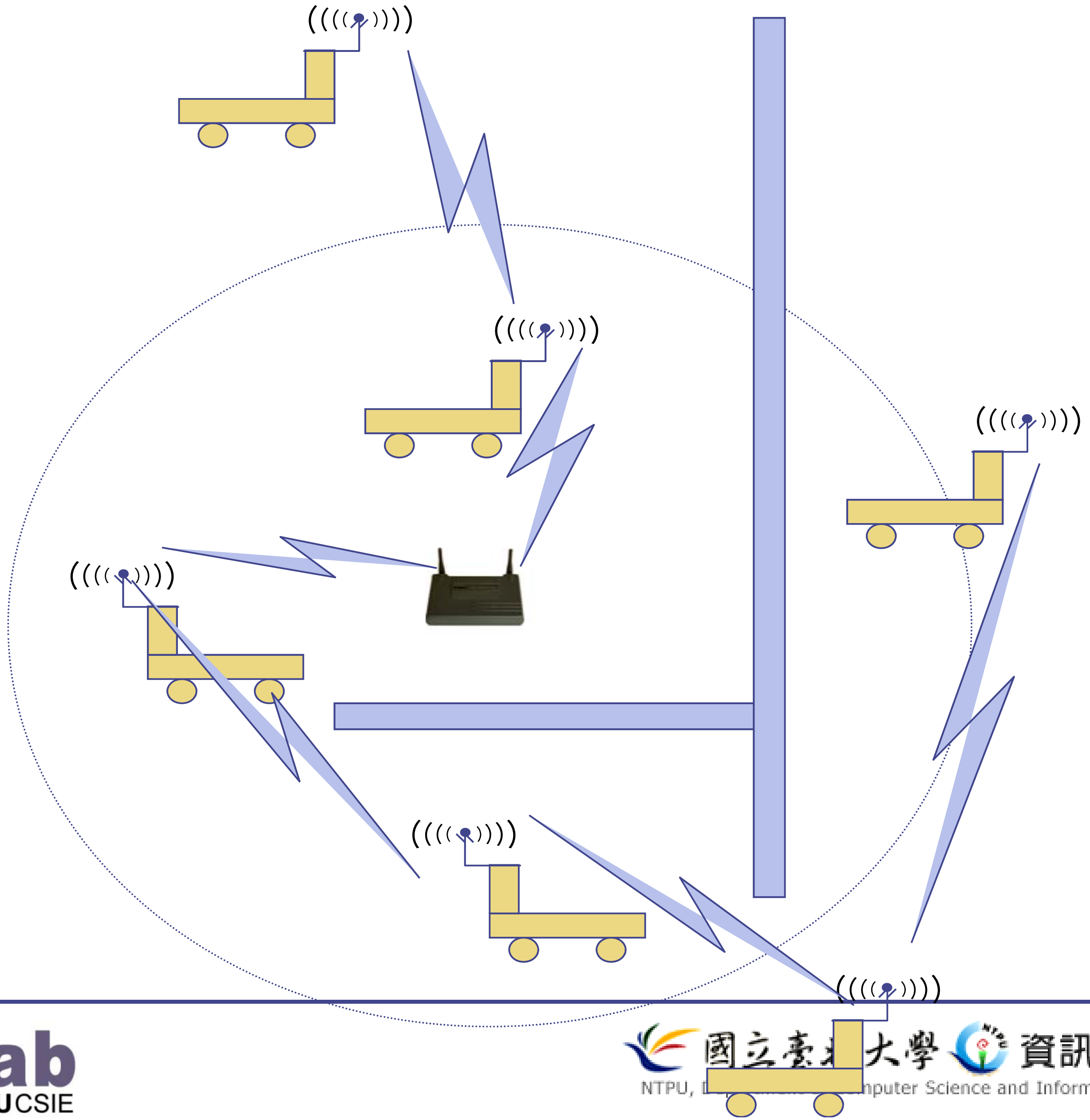




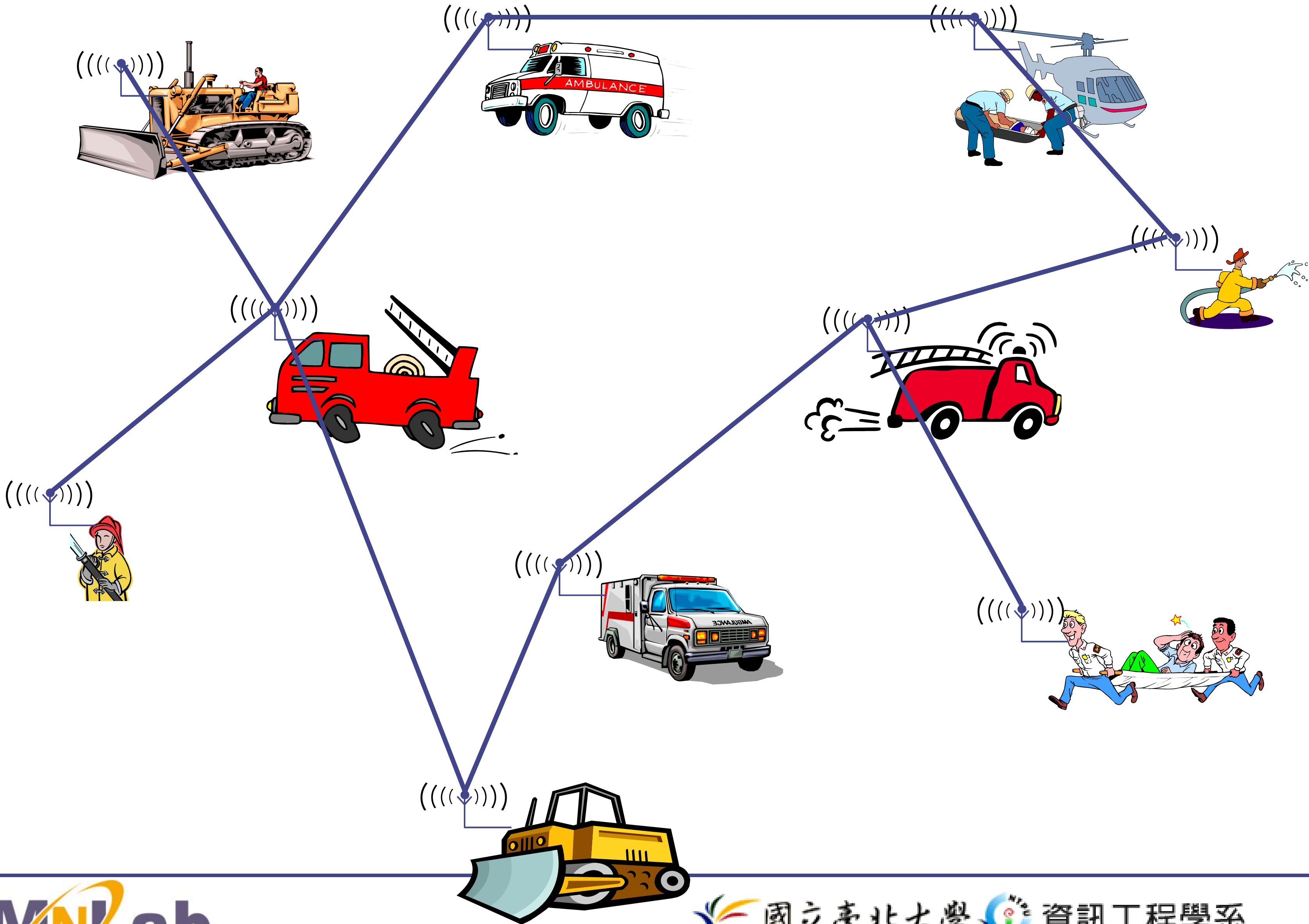


- Military networking: Tanks, soldiers, …
- Finding out empty parking lots in a city, without asking a server
- Search-and-rescue in an avalanche
- Personal area networking (watch, glasses, PDA, medical appliance, …)
- …

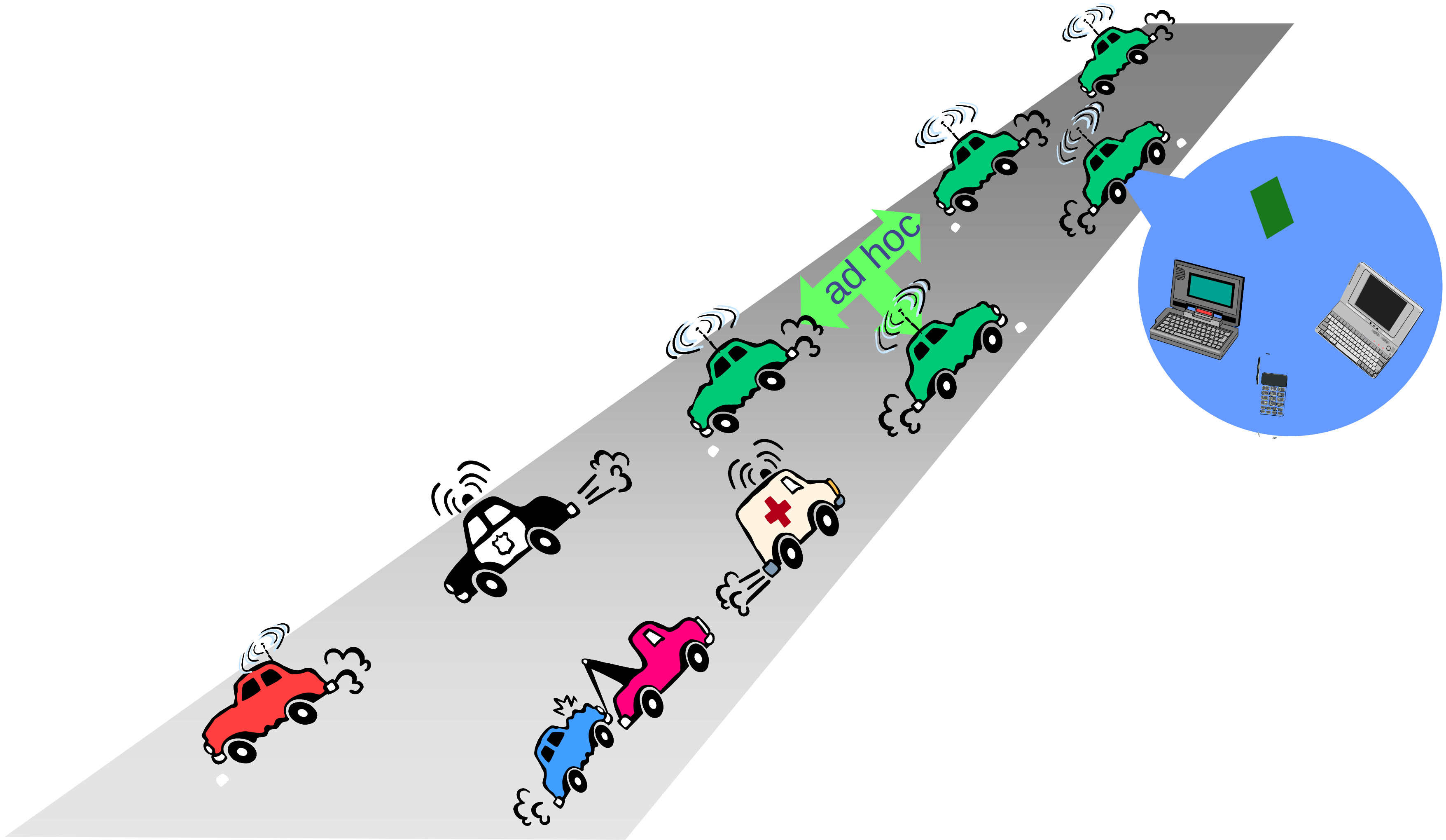
Factory floor automation



Disaster recovery



Car-to-car communication



Outline

- Infrastructure for wireless?
- ***(Mobile) ad hoc networks***
- Wireless sensor networks
- Comparison

Solution: (Wireless) ad hoc networks

- Try to construct a network without infrastructure, using networking abilities of the participants
  - This is an ***ad hoc network*** – a network constructed "for a special purpose"

- Simplest example: Laptops in a conference room – a ***single-hop ad hoc network***

Problems/challenges for ad hoc networks

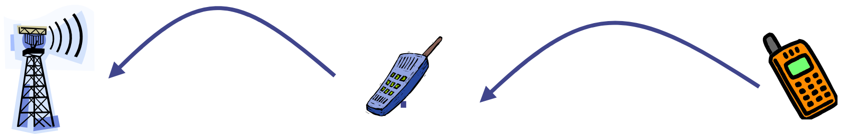
- Without a central infrastructure, things become much more difficult
- Problems are due to
  - Lack of central entity for organization available
  - Limited range of wireless communication
  - Mobility of participants
  - Battery-operated entities

No central entity → self-organization

- Without a central entity (like a base station), participants must organize themselves into a network (***self-organization***)
- Pertains to (among others):
  - **Medium access control** – no base station can assign transmission resources, must be decided in a distributed fashion
  - Finding a **route** from one participant to another

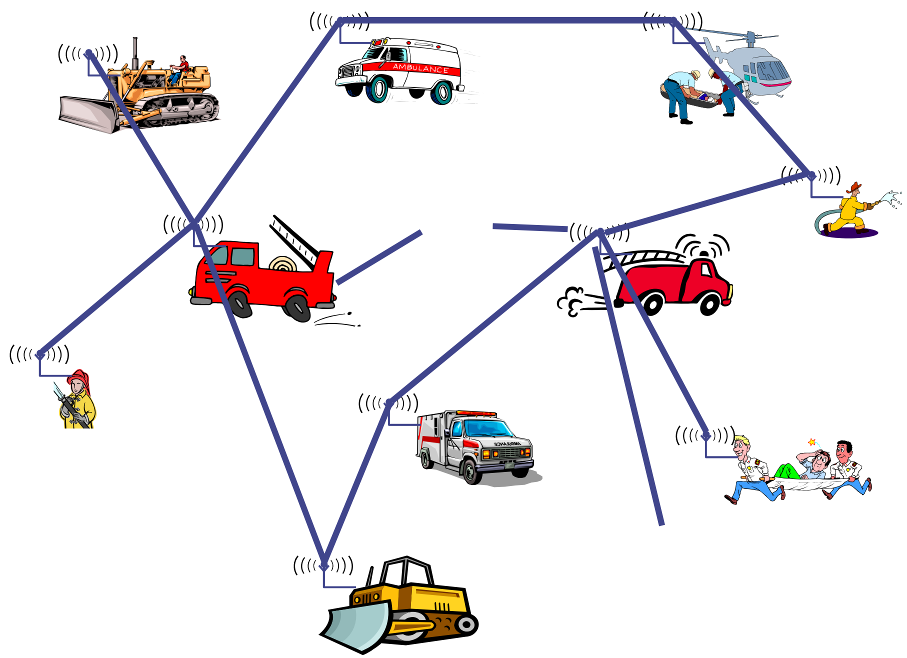
Limited range → multi-hopping

- For many scenarios, communication with peers outside immediate communication range is required
  - Direct communication limited because of distance, obstacles, …
  - Solution: ***multi-hop network***



Mobility → Suitable, adaptive protocols

- In many (not all!) ad hoc network applications, participants move around
  - In cellular network: simply hand over to another base station
- In ***mobile ad hoc networks (MANET)***:
  - Mobility changes neighborhood relationship
  - Must be compensated for
  - E.g., routes in the network have to be changed



- Complicated by scale
  - Large number of such nodes difficult to support

Battery-operated devices → energy-efficient operation

- Often (not always!), participants in an ad hoc network draw energy from batteries
- Desirable: long run time for
  - Individual devices
  - Network as a whole

→ Energy-efficient networking protocols

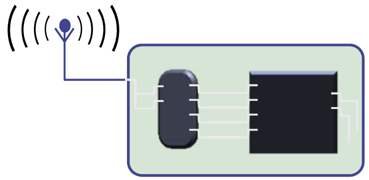
  - E.g., use multi-hop routes with low energy consumption (energy/bit)
  - E.g., take available battery capacity of devices into account
  - How to resolve conflicts between different optimizations?

Outline

- Infrastructure for wireless?
- (Mobile) ad hoc networks
- ***Wireless sensor networks***
  - ***Applications***
  - Requirements & mechanisms
- Comparison

Wireless sensor networks

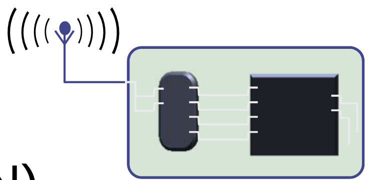
- Participants in the previous examples were devices close to a human user, interacting with humans



- Alternative concept:

  Instead of focusing interaction on humans, focus on interacting with ***environment***

  - Network is ***embedded*** in environment
  - Nodes in the network are equipped with ***sensing*** and ***actuation*** to measure/influence environment
  - Nodes process information and communicate it wirelessly

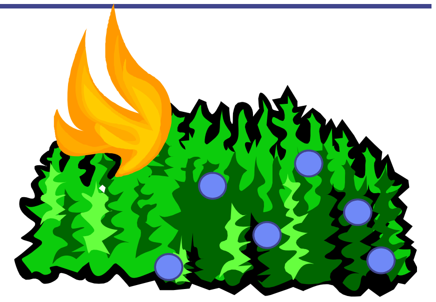


$\rightarrow$ ***Wireless sensor networks*** (WSN)

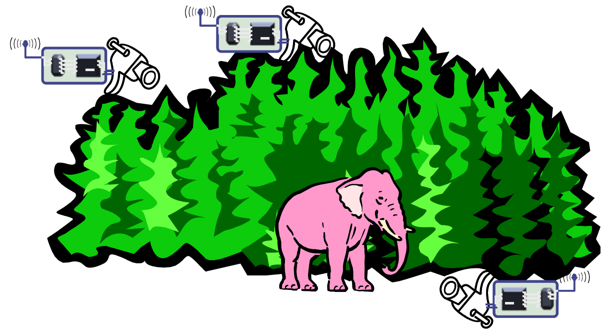
- Or: ***Wireless sensor & actuator networks*** (WSAN)

WSN application examples

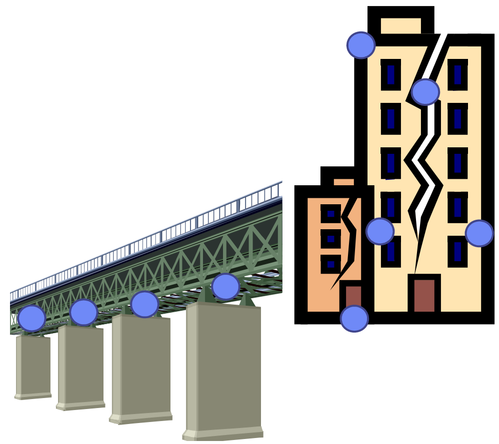
- Disaster relief operations
  - Drop sensor nodes from an aircraft over a wildfire
  - Each node measures temperature
  - Derive a “temperature map”



- Biodiversity mapping
  - Use sensor nodes to observe wildlife

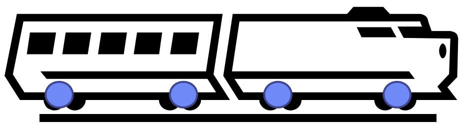


- Intelligent buildings (or bridges)
  - Reduce energy wastage by proper humidity, ventilation, air conditioning (HVAC) control
  - Needs measurements about room occupancy, temperature, air flow, …
  - Monitor mechanical stress after earthquakes



WSN application scenarios

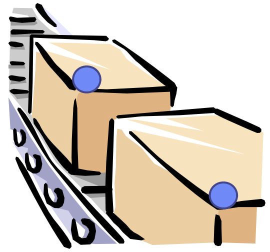
- Facility management
  - Intrusion detection into industrial sites
  - Control of leakages in chemical plants, …
- Machine surveillance and preventive maintenance
  - Embed sensing/control functions into places no cable has gone before
  - E.g., tire pressure monitoring



- Precision agriculture
  - Bring out fertilizer/pesticides/irrigation only where needed
- Medicine and health care
  - Post-operative or intensive care
  - Long-term surveillance of chronically ill patients or the elderly

WSN application scenarios

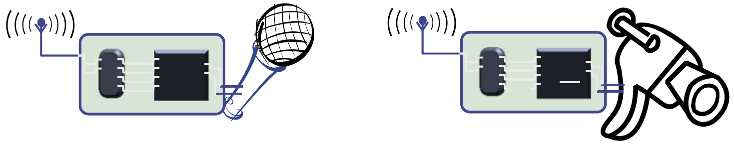
- Logistics
  - Equip goods (parcels, containers) with a sensor node
  - Track their whereabouts – ***total asset management***
  - Note: passive readout might suffice – compare RF IDs



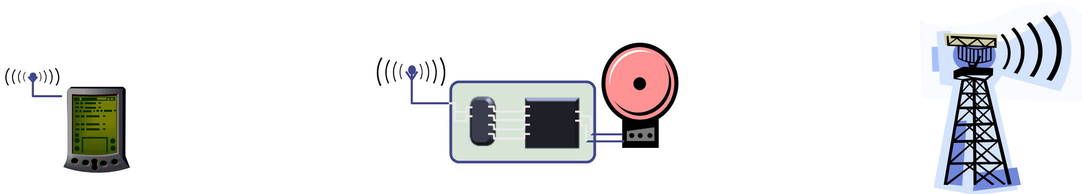
- Telematics
  - Provide better traffic control by obtaining finer-grained information about traffic conditions
  - ***Intelligent roadside***
  - Cars as the sensor nodes

Roles of participants in WSN

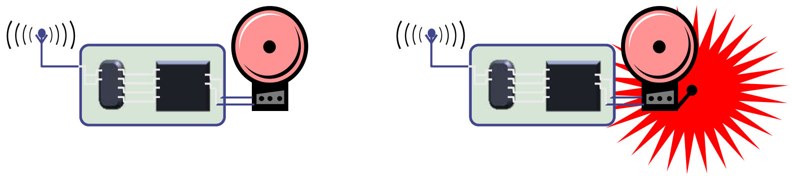
- ***Sources*** of data: Measure data, report them "somewhere"
  - Typically equip with different kinds of actual sensors



- ***Sinks*** of data: Interested in receiving data from WSN
  - May be part of the WSN or external entity, PDA, gateway, …



- ***Actuators***: Control some device based on data, usually also a sink



Structuring WSN application types

- ***Interaction patterns*** between sources and sinks classify application types
  - ***Event detection***: Nodes locally detect events (maybe jointly with nearby neighbors), report these events to interested sinks
    - ***Event classification*** additional option
  - ***Periodic measurement***
  - ***Function approximation:*** Use sensor network to approximate a function of space and/or time (e.g., temperature map)
  - ***Edge detection:*** Find edges (or other structures) in such a function (e.g., where is the zero degree border line?)
  - ***Tracking*****:** Report (or at least, know) position of an observed intruder ("pink elephant")

Deployment options for WSN

- How are sensor nodes deployed in their environment?
  - Dropped from aircraft → ***Random deployment***
    - Usually uniform random distribution for nodes over finite area is assumed
    - Is that a likely proposition?
  - Well planned, fixed → ***Regular deployment***
    - E.g., in preventive maintenance or similar
    - Not necessarily geometric structure, but that is often a convenient assumption
  - ***Mobile*** sensor nodes
    - Can move to compensate for deployment shortcomings
    - Can be passively moved around by some external force (wind, water)
    - Can actively seek out "interesting" areas

Maintenance options

- Feasible and/or practical to maintain sensor nodes?
  - E.g., to replace batteries?
  - Or: unattended operation?
  - Impossible but not relevant? Mission lifetime might be very small

- Energy supply?
  - Limited from point of deployment?
  - Some form of recharging, energy scavenging from environment?
    - E.g., solar cells

Outline

- Infrastructure for wireless?
- (Mobile) ad hoc networks
- ***Wireless sensor networks***
  - Applications
  - ***Requirements & mechanisms***
- Comparison

Characteristic requirements for WSNs

- Type of service of WSN
  - Not simply moving bits like another network
  - Rather: provide ***answers*** (not just numbers)
  - Issues like geographic scoping are natural requirements, absent from other networks
- Quality of service
  - Traditional QoS metrics do not apply
  - Still, service of WSN must be "good": Right answers at the right time
- Fault tolerance
  - Be robust against node failure (running out of energy, physical destruction, …)
- Lifetime
  - The ***network*** should fulfill its task as long as possible – definition depends on application
  - Lifetime of individual nodes relatively unimportant
  - But often treated equivalently

Characteristic requirements for WSNs

- Scalability
  - Support large number of nodes
- Wide range of densities
  - Vast or small number of nodes per unit area, very application-dependent
- Programmability
  - Re-programming of nodes in the field might be necessary, improve flexibility
- Maintainability
  - WSN has to adapt to changes, self-monitoring, adapt operation
  - Incorporate possible additional resources, e.g., newly deployed nodes

Required mechanisms to meet requirements

- Multi-hop wireless communication
- Energy-efficient operation
  - Both for communication and computation, sensing, actuating
- Auto-configuration
  - Manual configuration just not an option
- Collaboration & in-network processing
  - Nodes in the network collaborate towards a joint goal
  - Pre-processing data in network (as opposed to at the edge) can greatly improve efficiency

Required mechanisms to meet requirements

- Data centric networking
  - Focusing network design on ***data***, not on ***node identifies*** (id-centric networking)
  - To improve efficiency
- Locality
  - Do things locally (on node or among nearby neighbors) as far as possible
- Exploit tradeoffs
  - E.g., between invested energy and accuracy

Outline

- Infrastructure for wireless?
- (Mobile) ad hoc networks
- Wireless sensor networks
- ***Comparison***

MANET vs. WSN

- Many commonalities: Self-organization, energy efficiency, (often) wireless multi-hop
- Many differences
  - ***Applications, equipment***: MANETs more powerful (read: expensive) equipment assumed, often “human in the loop”-type applications, higher data rates, more resources
  - ***Application-specific***: WSNs depend much stronger on application specifics; MANETs comparably uniform
  - ***Environment interaction***: core of WSN, absent in MANET
  - ***Scale***: WSN might be much larger (although contestable)
  - ***Energy***: WSN tighter requirements, maintenance issues
  - ***Dependability/QoS***: in WSN, individual node may be dispensable (network matters), QoS different because of different applications
  - ***Data centric*** vs. id-centric networking
  - ***Mobility***: different mobility patterns like (in WSN, sinks might be mobile, usual nodes static)

Wireless fieldbuses and WSNs

- Fieldbus:
  - Network type invented for real-time communication, e.g., for factory-floor automation
  - Inherent notion of sensing/measuring and controlling
  - Wireless fieldbus: Real-time communication over wireless

$\rightarrow$ Big similarities

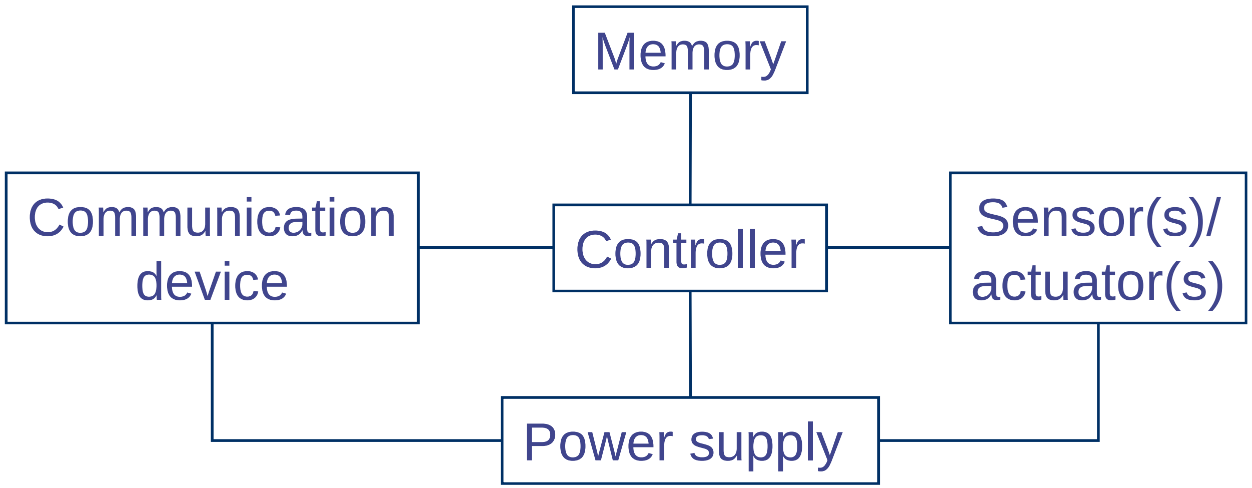
- Differences
  - Scale – WSN often intended for larger scale
  - Real-time – WSN usually not intended to provide (hard) real-time guarantees as attempted by fieldbuses

Enabling technologies for WSN

- Cost reduction
  - For wireless communication, simple microcontroller, sensing, batteries
- Miniaturization
  - Some applications demand small size
  - “Smart dust” as the most extreme vision
- Energy scavenging
  - Recharge batteries from ambient energy (light, vibration, …)

Sensor node architecture

- Main components of a WSN node
  - Controller
  - Communication device(s)
  - Sensors/actuators
  - Memory
  - Power supply

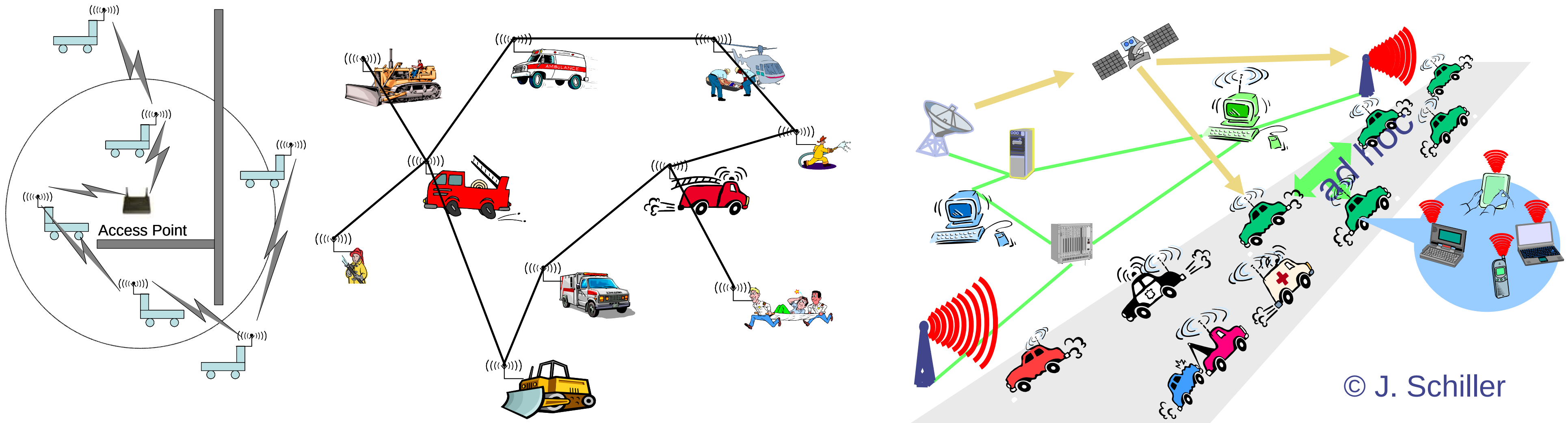


Outline

- ***Network scenarios***
- Optimization goals
- Design principles
- Service interface
- Gateway concepts

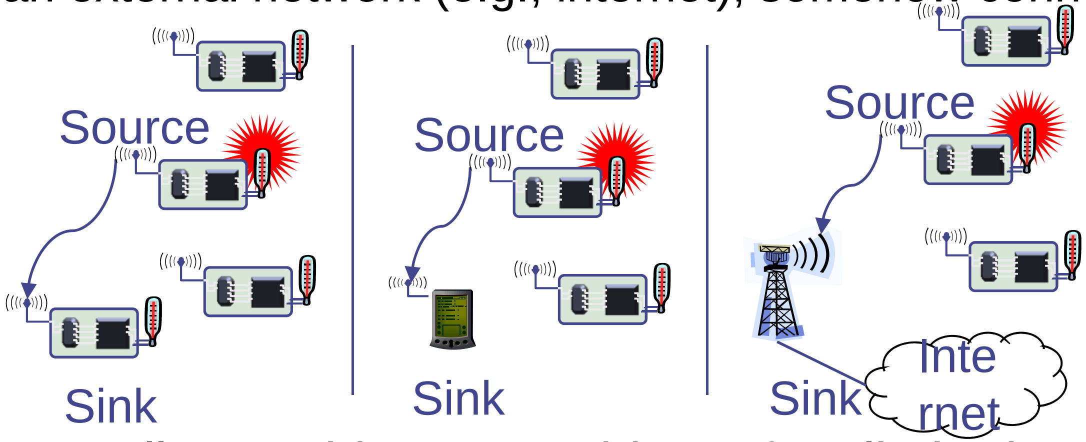
Basic scenarios: Ad hoc networks

- (Mobile) ad hoc scenarios
  - Nodes talking to each other
  - Nodes talking to “some” node in another network (Web server on the Internet, e.g.)
    - Typically requires some connection to the fixed network
  - Applications: Traditional data (http, ftp, collaborative apps, …) & multimedia (voice, video) → humans in the loop



Basic scenarios: sensor networks

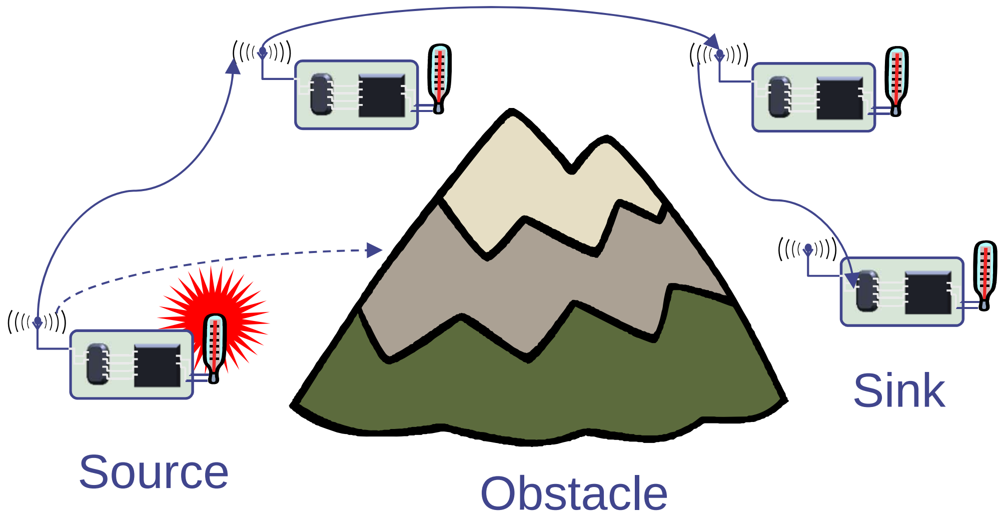
- Sensor network scenarios
  - ***Sources***: Any entity that provides data/measurements
  - ***Sinks***: Nodes where information is required
    - Belongs to the sensor network as such
    - Is an external entity, e.g., a PDA, but directly connected to the WSN
      - Main difference: comes and goes, often moves around, …
    - Is part of an external network (e.g., internet), somehow connected to the WSN



  - Applications: Usually, machine to machine, often limited amounts of data, different notions of importance

Single-hop vs. multi-hop networks

- One common problem: limited range of wireless communication
  - Essentially due to limited transmission power, path loss, obstacles
- Option: multi-hop networks
  - Send packets to an intermediate node
  - Intermediate node forwards packet to its destination
  - ***Store-and-forward*** multi-hop network
- Basic technique applies to both WSN and MANET
- Note: Store&forward multi-hopping NOT the only possible solution
  - E.g., collaborative networking, network coding
  - Do not operate on a per-packet basis

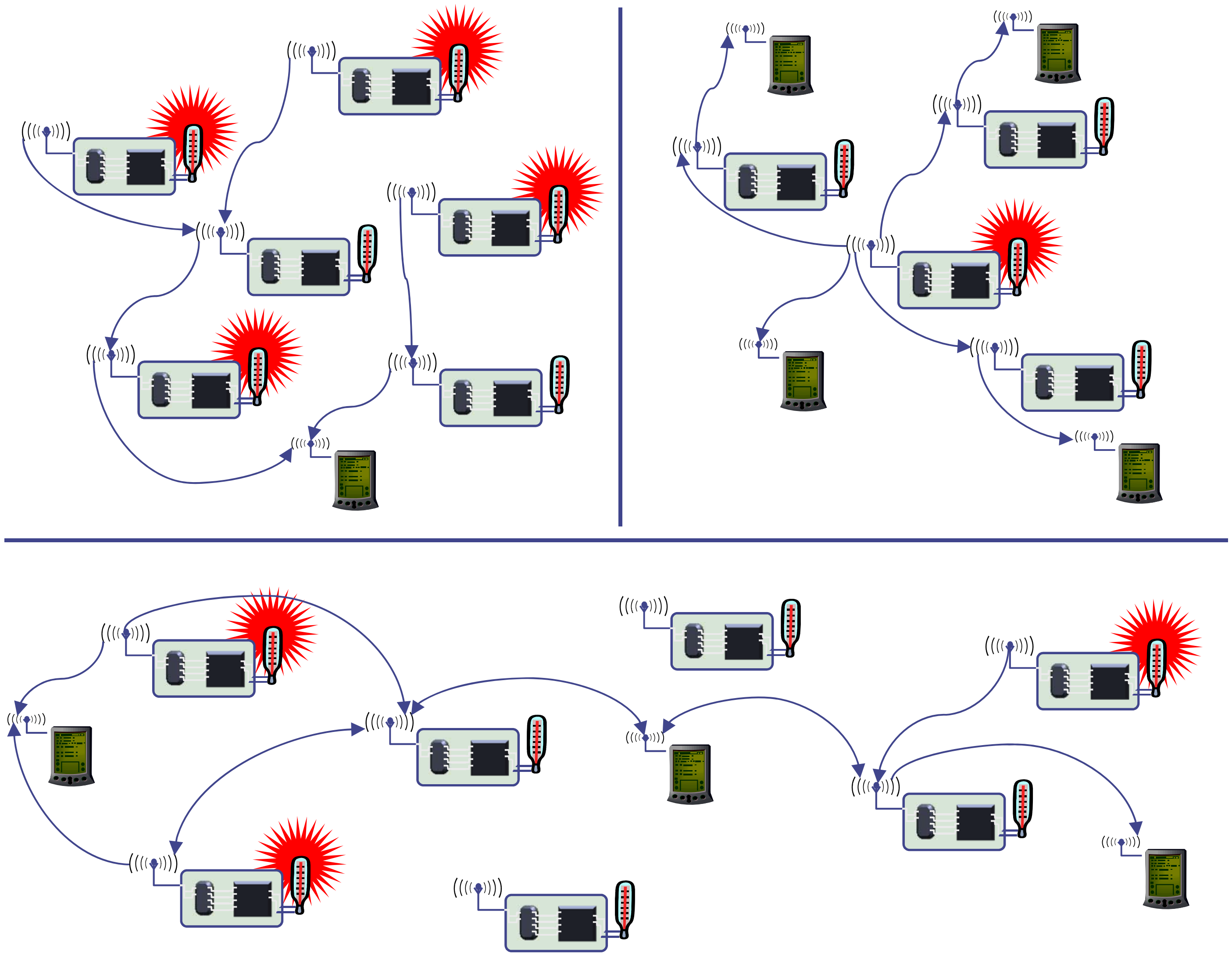


Energy efficiency of multi-hopping?

- Obvious idea: Multi-hopping is more energy-efficient than direct communication
  - Because of path loss $\alpha > 2$, energy for distance d is reduced from cd^{α} to $2c(d/2)^{\alpha}$
    - c some constant
- However: This is usually wrong, or at least very over-simplified
  - Need to take constant offsets for powering transmitter, receiver into account
  - Details see exercise, chapter 2

$\rightarrow$ Multi-hopping for energy savings needs careful choice

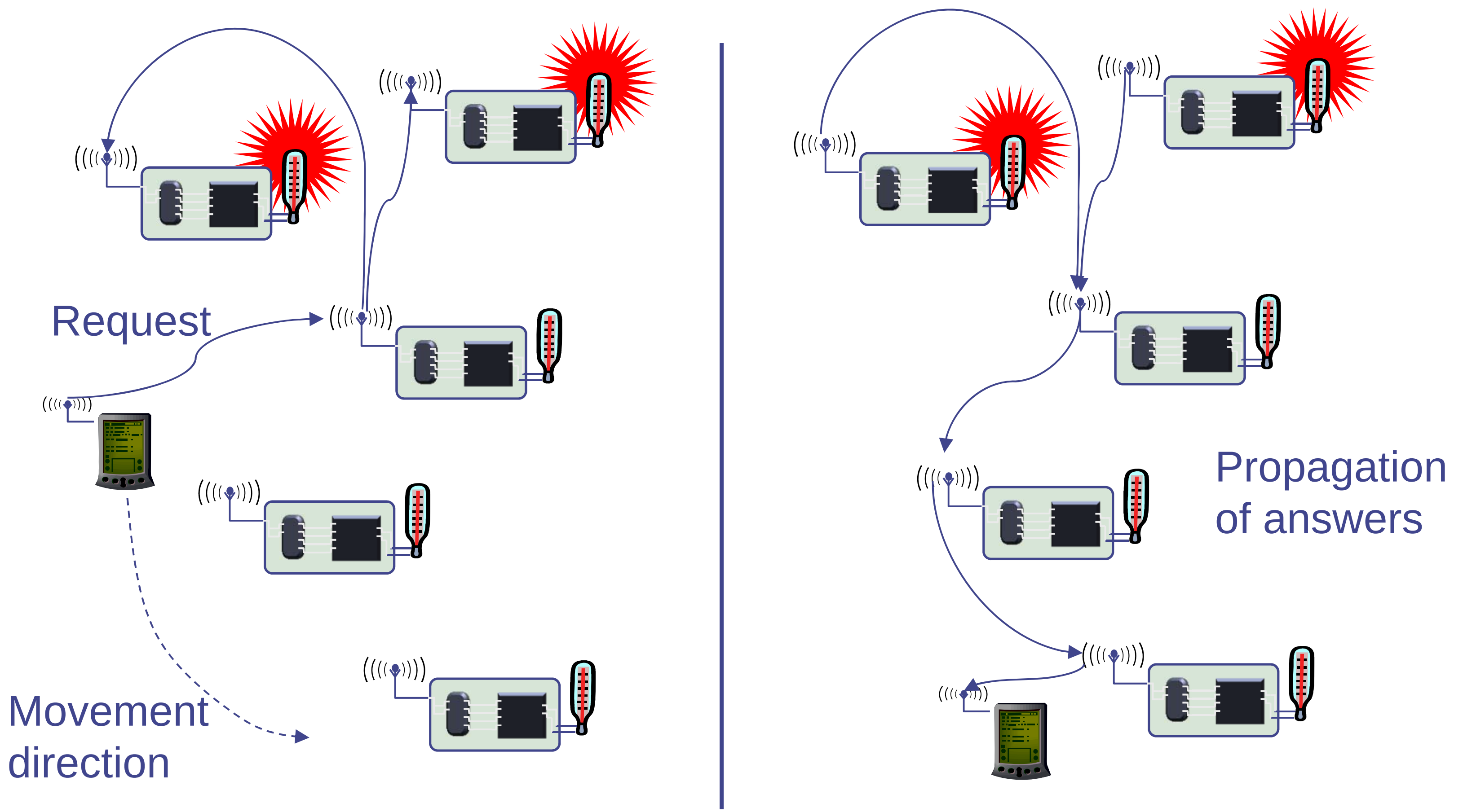
WSN: Multiple sinks, multiple sources



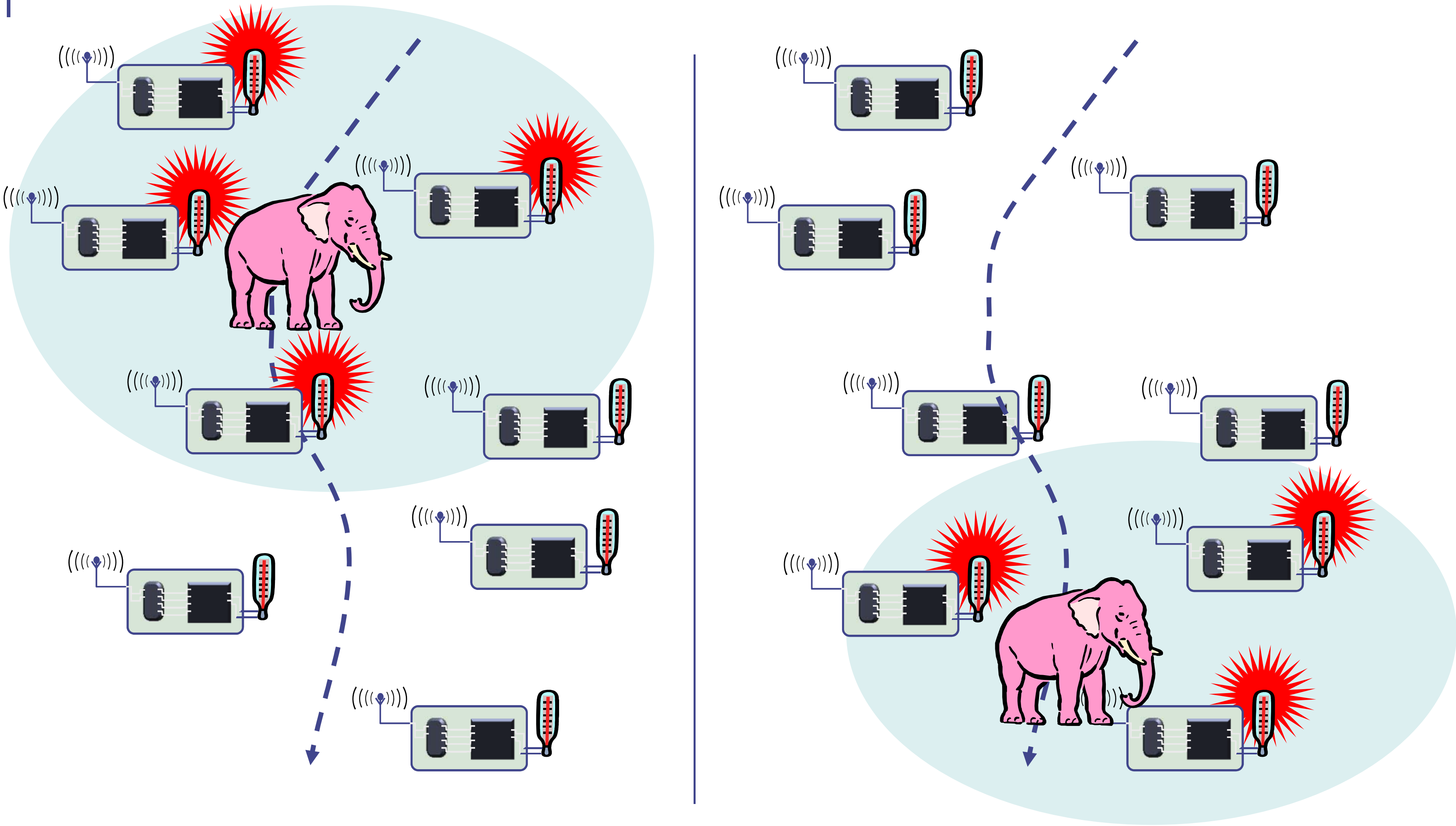
Different sources of mobility

- **Node mobility**
  - A node participating as source/sink (or destination) or a relay node might move around
  - Deliberately, self-propelled or by external force; targeted or at random
  - Happens in both WSN and MANET
- **Sink mobility**
  - In WSN, a sink that is not part of the WSN might move
  - Mobile requester
- **Event mobility**
  - In WSN, event that is to be observed moves around (or extends, shrinks)
  - Different WSN nodes become “responsible” for surveillance of such an event

WSN sink mobility



WSN event mobility: Track the pink elephant



Here: Frisbee model as example

Outline

- Network scenarios
- ***Optimization goals***
- Design principles
- Service interface
- Gateway concepts

Optimization goal: Quality of Service

- In MANET: Usual QoS interpretation
  - Throughput/delay/jitter
  - High perceived QoS for multimedia applications
- In WSN, more complicated
  - Event detection/reporting probability
  - Event classification error, detection delay
  - Probability of missing a periodic report
  - Approximation accuracy (e.g, when WSN constructs a temperature map)
  - Tracking accuracy (e.g., difference between true and conjectured position of the pink elephant)
- Related goal: robustness
  - Network should withstand failure of some nodes

Optimization goal: Energy efficiency

- Umbrella term!
- Energy per correctly received bit
  - Counting all the overheads, in intermediate nodes, etc.
- Energy per reported (unique) event
  - After all, information is important, not payload bits!
  - Typical for WSN
- Delay/energy tradeoffs
- Network lifetime
  - Time to first node failure
  - Network half-life (how long until 50% of the nodes died?)
  - Time to partition
  - Time to loss of coverage
  - Time to failure of first event notification

Optimization goal: Scalability

- Network should be operational regardless of number of nodes
  - At high efficiency
- Typical node numbers difficult to guess
  - MANETs: 10s to 100s
  - WSNs: 10s to 1000s, maybe more (although few people have seen such a network before…)
- Requiring to scale to large node numbers has ***serious*** consequences for network architecture
  - Might not result in the most efficient solutions for small networks!
  - Carefully consider actual application needs before looking for $n \rightarrow \infty$ solutions!

Outline

- Network scenarios
- Optimization goals
- ***Design principles***
- Service interface
- Gateway concepts

Distributed organization

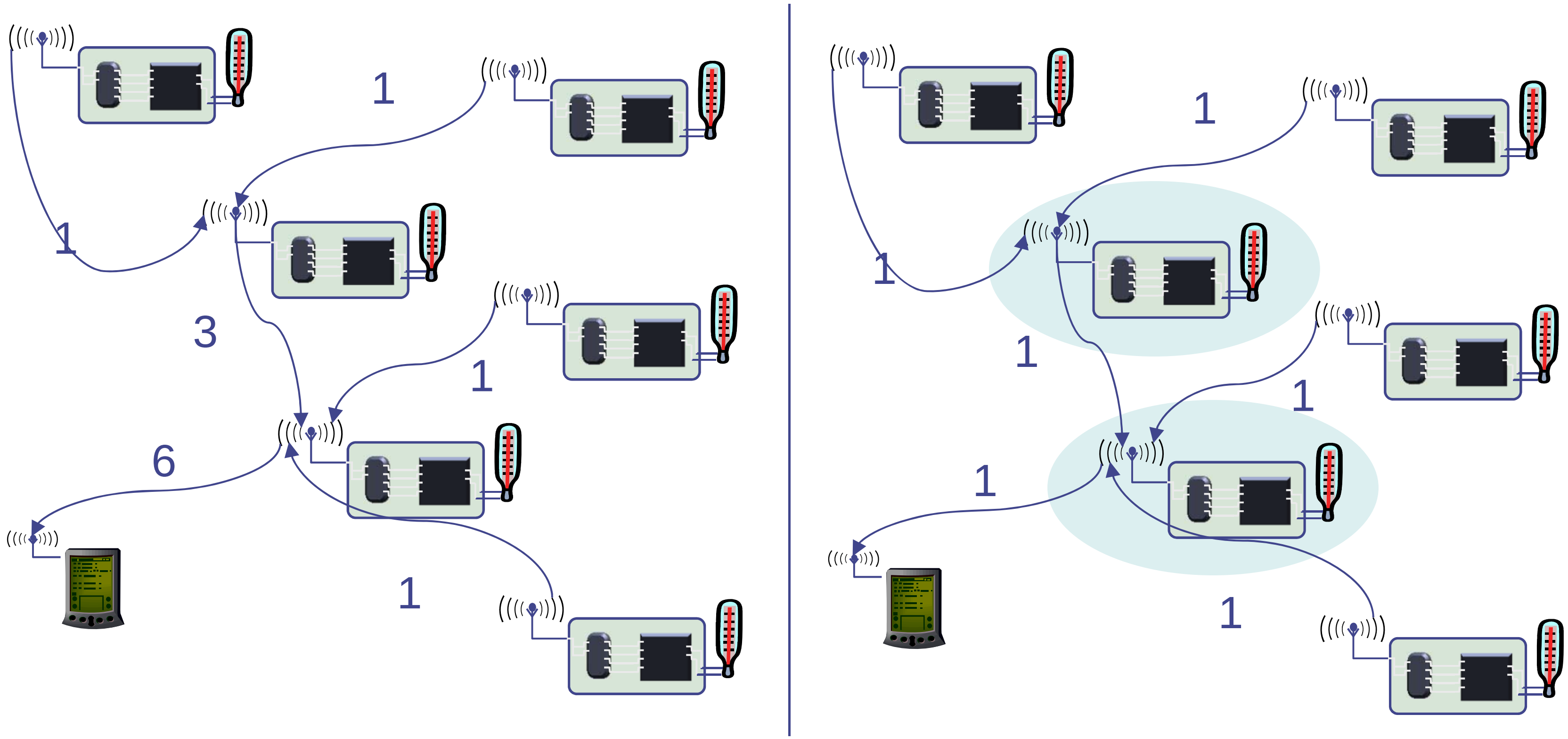
- Participants in a MANET/WSN should cooperate in organizing the network
  - E.g., with respect to medium access, routing, …
  - Centralistic approach as alternative usually not feasible – hinders scalability, robustness
- Potential shortcomings
  - Not clear whether distributed or centralistic organization achieves better energy efficiency (when taking all overheads into account)
- Option: "limited centralized" solution
  - Elect nodes for local coordination/control
  - Perhaps rotate this function over time

In-network processing

- MANETs are supposed to deliver bits from one end to the other
- WSNs, on the other end, are expected to provide information, not necessarily original bits
  - Gives addition options
  - E.g., ***manipulate*** or ***process*** the data in the network
- Main example: aggregation
  - Apply composable aggregation functions to a convergecast tree in a network
  - Typical functions: minimum, maximum, average, sum, …
  - Not amenable functions: median

In-network processing: Aggregation example

- Reduce number of transmitted bits/packets by applying an aggregation function in the network



In-network processing: signal processing

- Depending on application, more sophisticated processing of data can take place within the network
  - Example edge detection: locally exchange raw data with neighboring nodes, compute edges, only communicate edge description to far away data sinks
  - Example tracking/angle detection of signal source: Conceive of sensor nodes as a distributed microphone array, use it to compute the angle of a single source, only communicate this angle, not all the raw data
- Exploit ***temporal*** and ***spatial correlation***
  - Observed signals might vary only slowly in time $\rightarrow$ no need to transmit all data at full rate all the time
  - Signals of neighboring nodes are often quite similar $\rightarrow$ only try to transmit differences (details a bit complicated, see later)

Adaptive fidelity

- Adapt the effort with which data is exchanged to the currently required accuracy/fidelity
- Example event detection
  - When there is no event, only very rarely send short “all is well” messages
  - When event occurs, increase rate of message exchanges
- Example temperature
  - When temperature is in acceptable range, only send temperature values at low resolution
  - When temperature becomes high, increase resolution and thus message length

Data centric networking

- In typical networks (including ad hoc networks), network transactions are addressed to the ***identities*** of specific nodes
  - A “node-centric” or “address-centric” networking paradigm
- In a redundantly deployed sensor networks, specific source of an event, alarm, etc. might not be important
  - Redundancy: e.g., several nodes can observe the same area
- Thus: focus networking transactions on the data directly instead of their senders and transmitters → ***data-centric networking***
  - Principal design change

Implementation options for data-centric networking

- Overlay networks & distributed hash tables (DHT)
  - Hash table: content-addressable memory
  - Retrieve data from an unknown source, like in peer-to-peer networking – with efficient implementation
  - Some disparities remain
    - Static key in DHT, dynamic changes in WSN
    - DHTs typically ignore issues like hop count or distance between nodes when performing a lookup operation
- Publish/subscribe
  - Different interaction paradigm
  - Nodes can ***publish*** data, can ***subscribe*** to any particular kind of data
  - Once data of a certain type has been published, it is delivered to all subscribes
  - Subscription and publication are decoupled in time; subscriber and published are agnostic of each other (decoupled in identity)
- Databases

Further design principles

- Exploit location information
  - Required anyways for many applications; can considerably increase performance
- Exploit activity patterns
- Exploit heterogeneity
  - By construction: nodes of different types in the network
  - By evolution: some nodes had to perform more tasks and have less energy left; some nodes received more solar energy than others; …
- Cross-layer optimization of protocol stacks for WSN
  - Goes against grain of standard networking; but promises big performance gains
  - Also applicable to other networks like ad hoc; usually at least worthwhile to consider for most wireless networks

Outline

- Network scenarios
- Optimization goals
- Design principles
- ***Service interface***
- Gateway concepts

Interfaces to protocol stacks

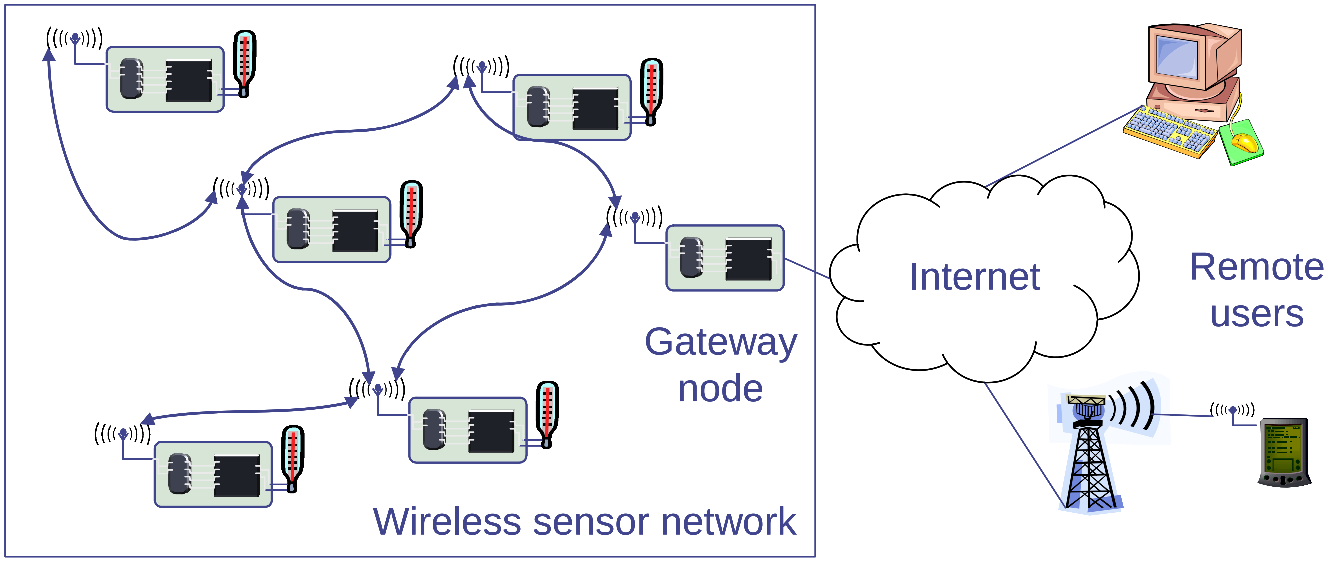
- The world's all-purpose network interface: sockets
  - Good for transmitting data from one sender to one receiver
  - Not well matched to WSN needs (ok for ad hoc networks)
- Expressibility requirements
  - Support for simple request/response interactions
  - Support for asynchronous event notification
  - Different ways for identifying addressee of data
    - By location, by observed values, implicitly by some other form of group membership
    - By some semantically meaningful form – "room 123"
  - Easy accessibility of in-network processing functions
    - Formulate complex events – events defined only by several nodes
  - Allow to specify accuracy & timeliness requirements
  - Access node/network status information (e.g., battery level)
  - Security, management functionality, …
- No clear standard has emerged yet – many competing, unclear proposals

Outline

- Network scenarios
- Optimization goals
- Design principles
- Service interface
- ***Gateway concepts***

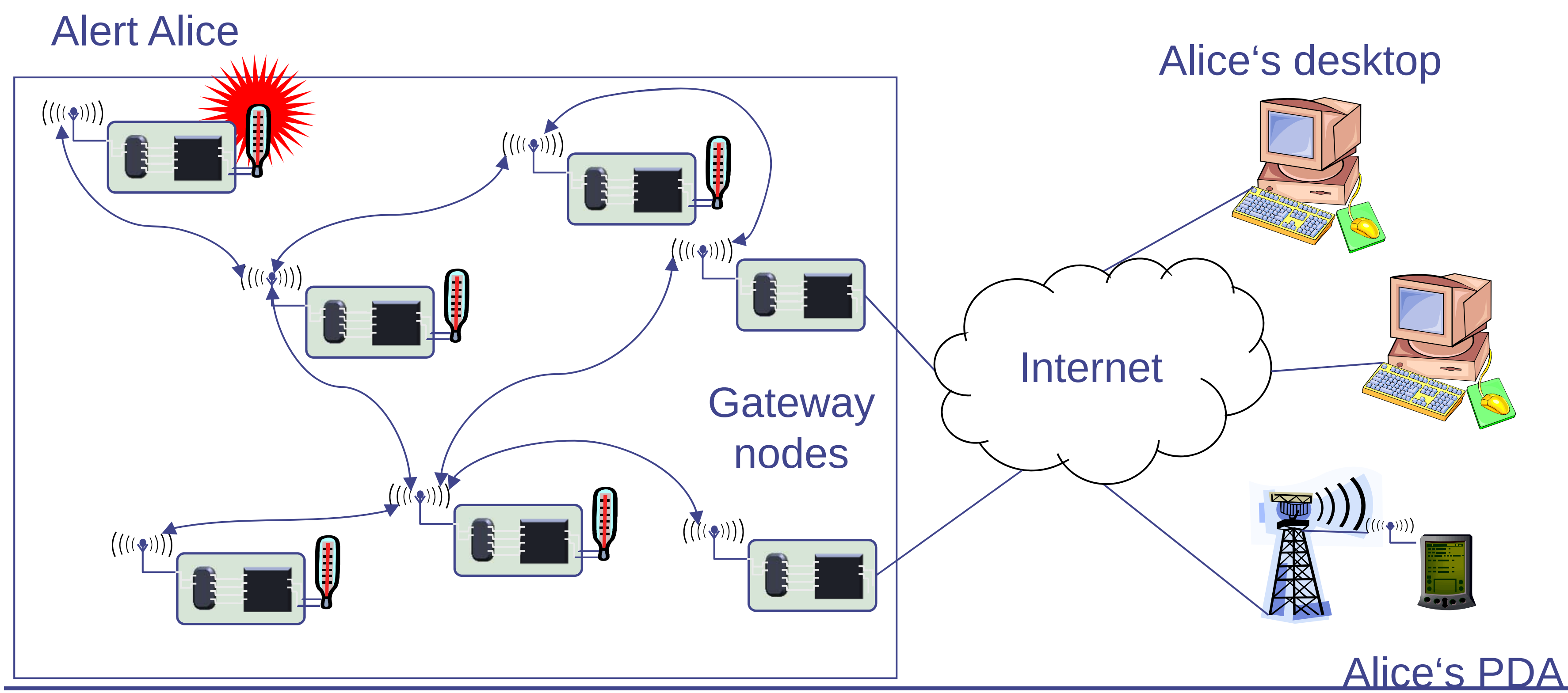
Gateway concepts for WSN/MANET

- Gateways are necessary to the Internet for remote access to/from the WSN
  - Same is true for ad hoc networks; additional complications due to mobility (change route to the gateway; use different gateways)
  - WSN: Additionally bridge the gap between different interaction semantics (data vs. address-centric networking) in the gateway
- Gateway needs support for different radios/protocols, …



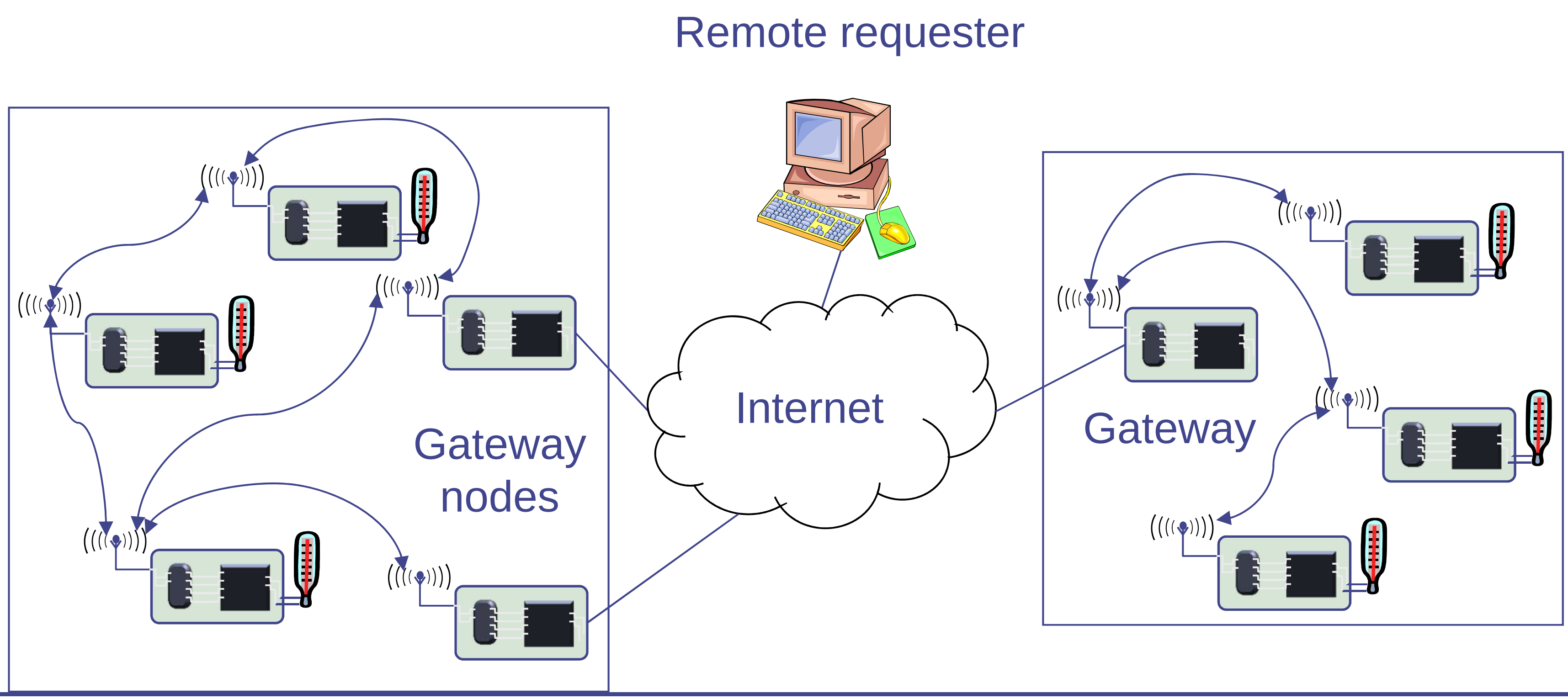
WSN to Internet communication

- Example: Deliver an alarm message to an Internet host
- Issues
  - Need to find a gateway (integrates routing & service discovery)
  - Choose “best” gateway if several are available
  - How to find Alice or Alice’s IP?



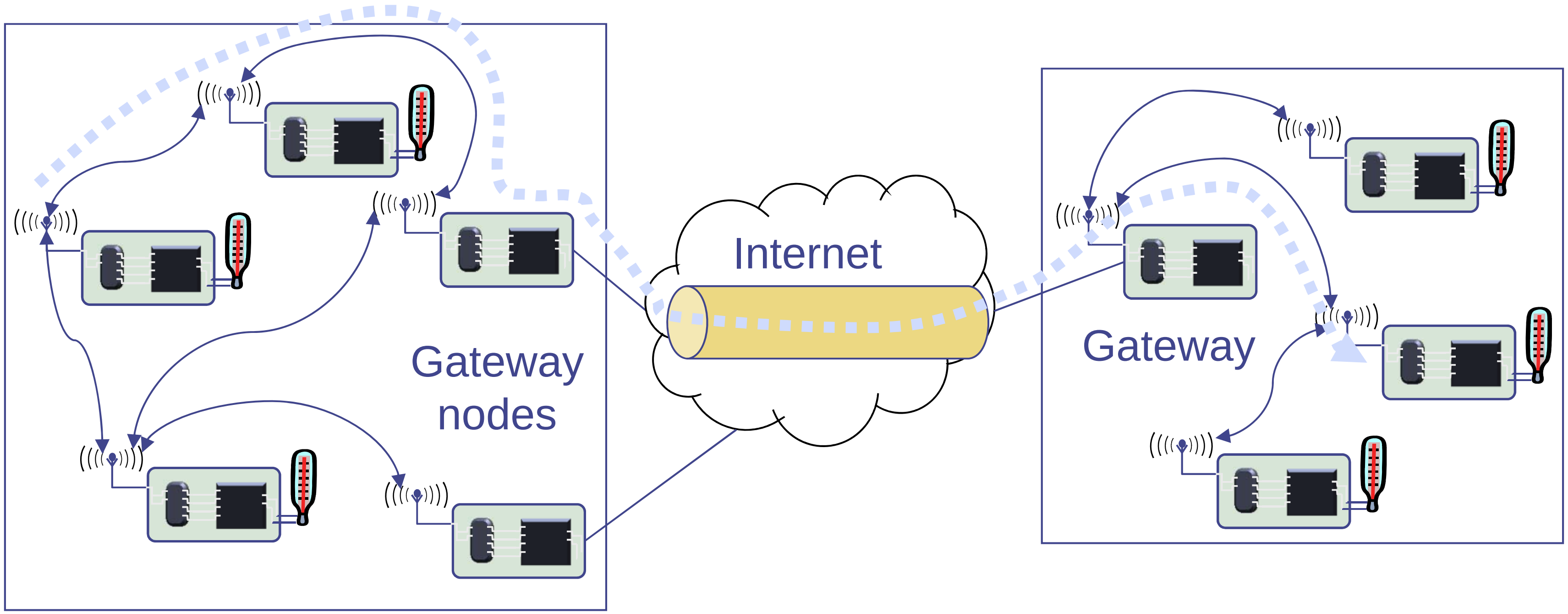
Internet to WSN communication

- How to find the right WSN to answer a need?
- How to translate from IP protocols to WSN protocols, semantics?



WSN tunneling

- Use the Internet to “tunnel” WSN packets between two remote WSNs



Summary

- Network architectures for ad hoc networks are – in principle – relatively straightforward and similar to standard networks
  - Mobility is compensated for by appropriate protocols, but interaction paradigms don't change too much
- WSNs, on the other hand, look quite different on many levels
  - Data-centric paradigm, the need and the possibility to manipulate data as it travels through the network opens new possibilities for protocol design
- The following chapters will look at how these ideas are realized by actual protocols

Homework #12:

1. Describe what's the difference and mobile ad hoc network (MANET) and wireless sensor network (WSN) ?
2. What's the sensor node architecture ?
3. What's difference of node mobility, sink mobility, and event mobility in WSN ?
4. What's in-network processing in WSN ?