



BENHA UNIVERSITY
FACULTY OF ENGINEERING AT SHOUBRA

ECE-508
Sensor Networks

Lecture #3
Network architecture

Instructor:
Dr. Ahmad El-Banna



SPRING 2015

© Ahmad El-Banna

Agenda

- 1 Network scenarios
- 2 Optimization goals
- 3 Design principles
- 4 Service interface
- 5 Gateway concepts

Goals of this chapter

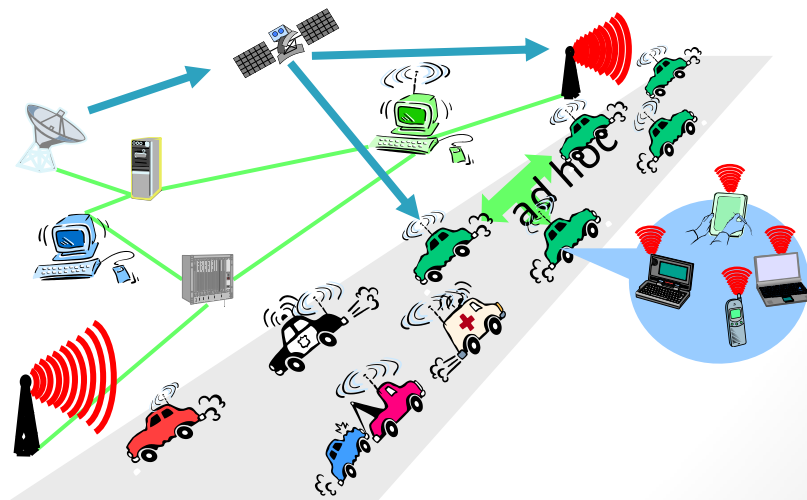
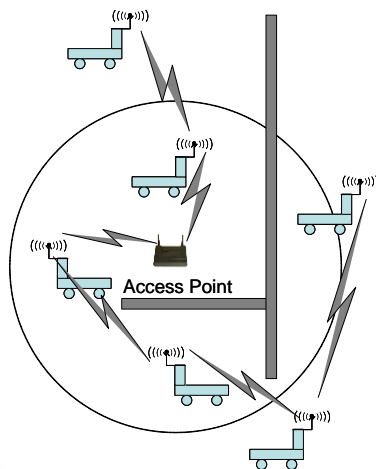
- Look at general principles and architectures how to put the individual nodes together to form a meaningful network.
- We will look at design approaches to both the more conventional ad hoc networks and the non-standard WSNs.

NETWORK SCENARIOS



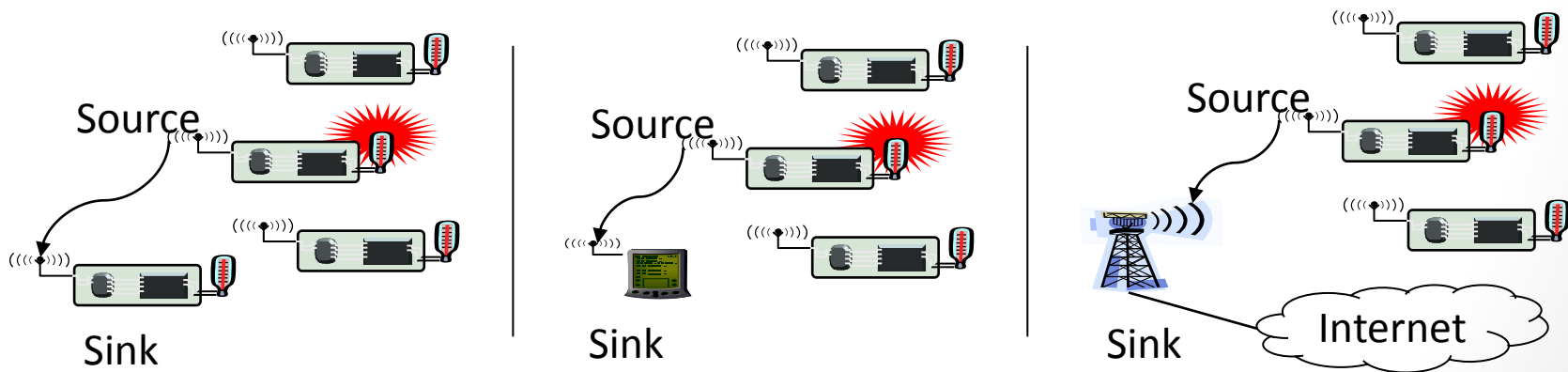
Basic scenarios: Ad hoc networks

- (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

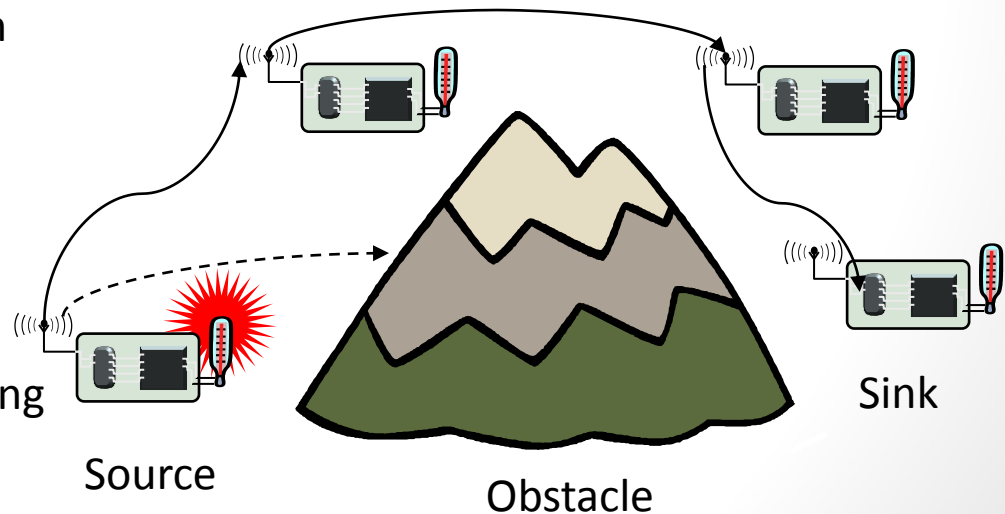
- Sensor network scenarios
 - **Sources:** Any entity that provides data/measurements
 - **Sinks:** Nodes where information is required
 - Belongs to the sensor network as such
 - Is an external entity, e.g., a PDA, but directly connected to the WSN
 - Main difference: comes and goes, often moves around,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

! Multi-hopping for energy savings needs careful choice

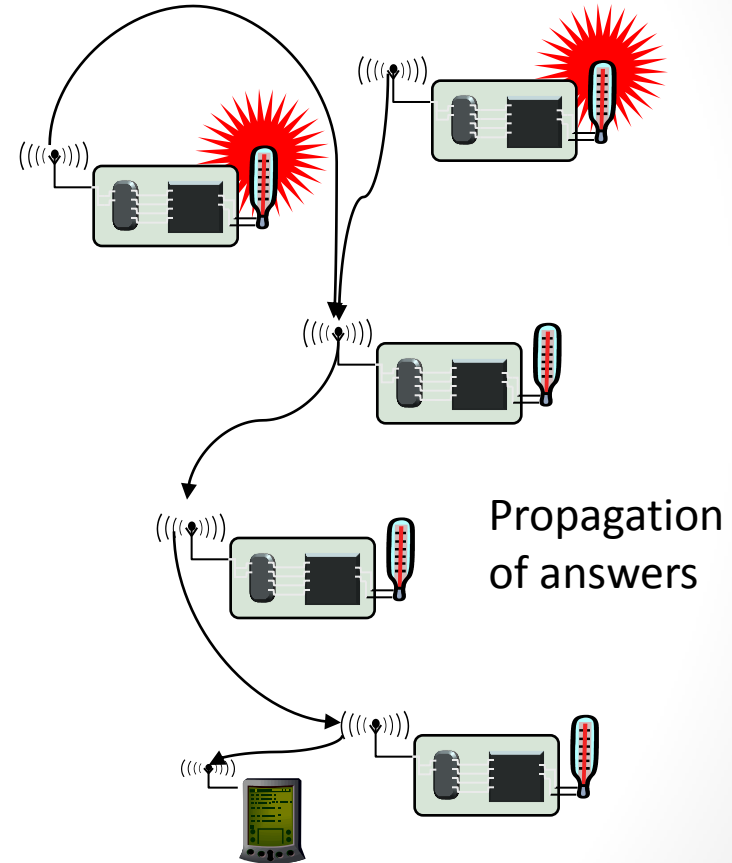
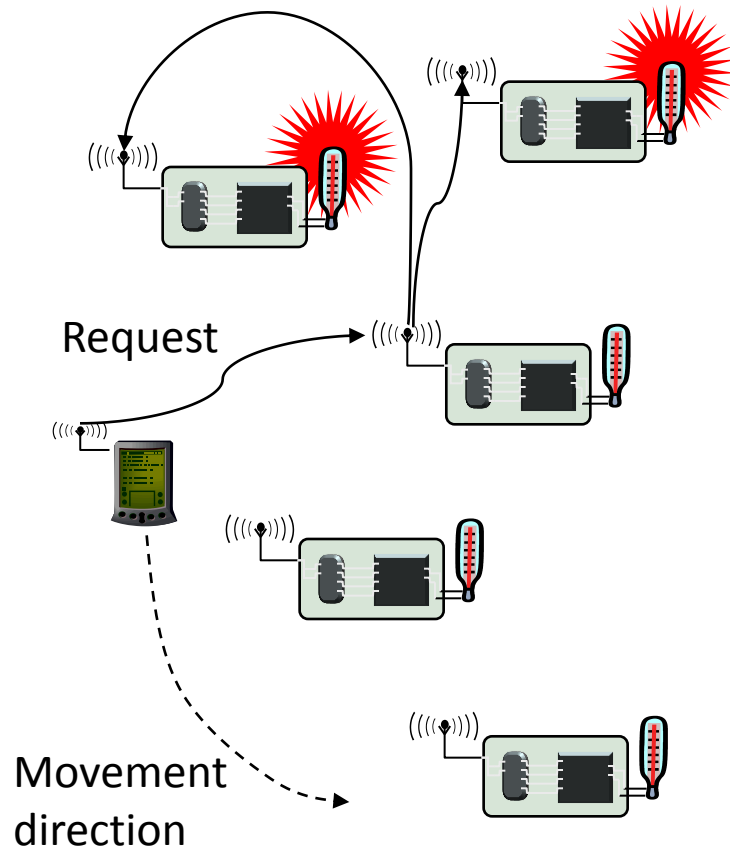


Different sources of mobility

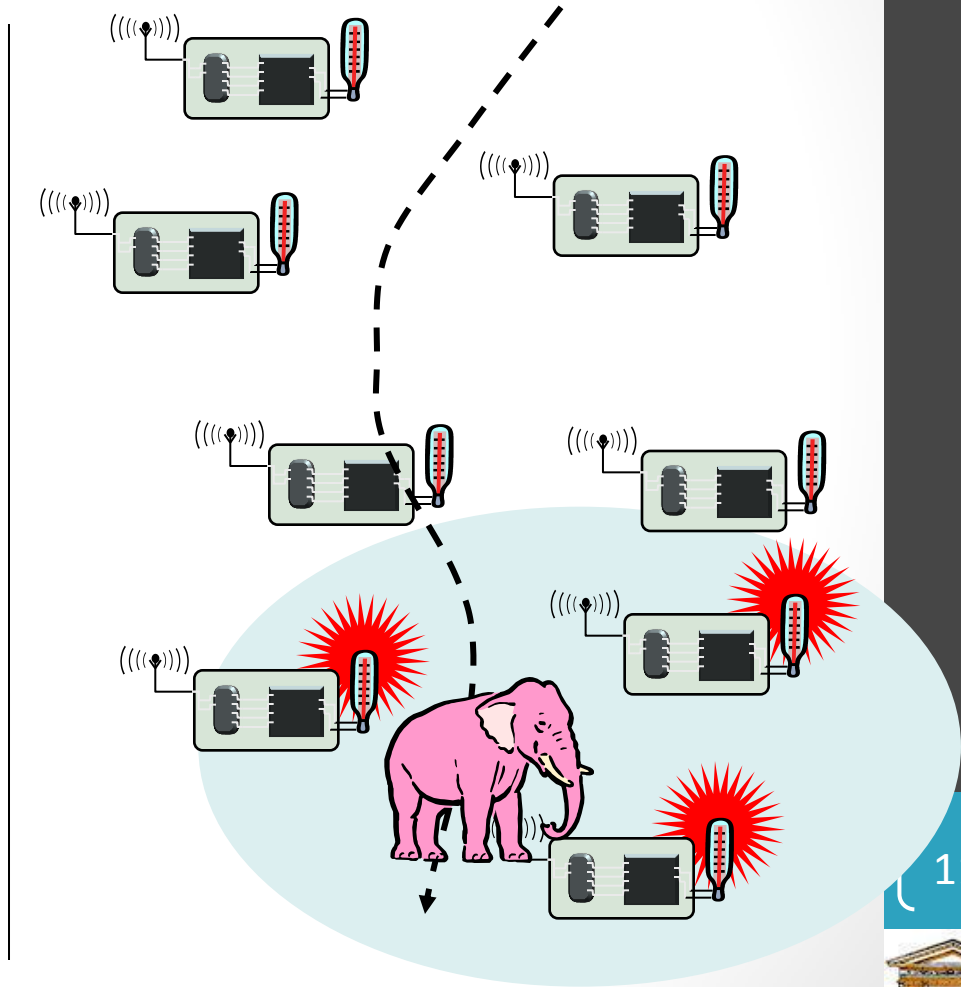
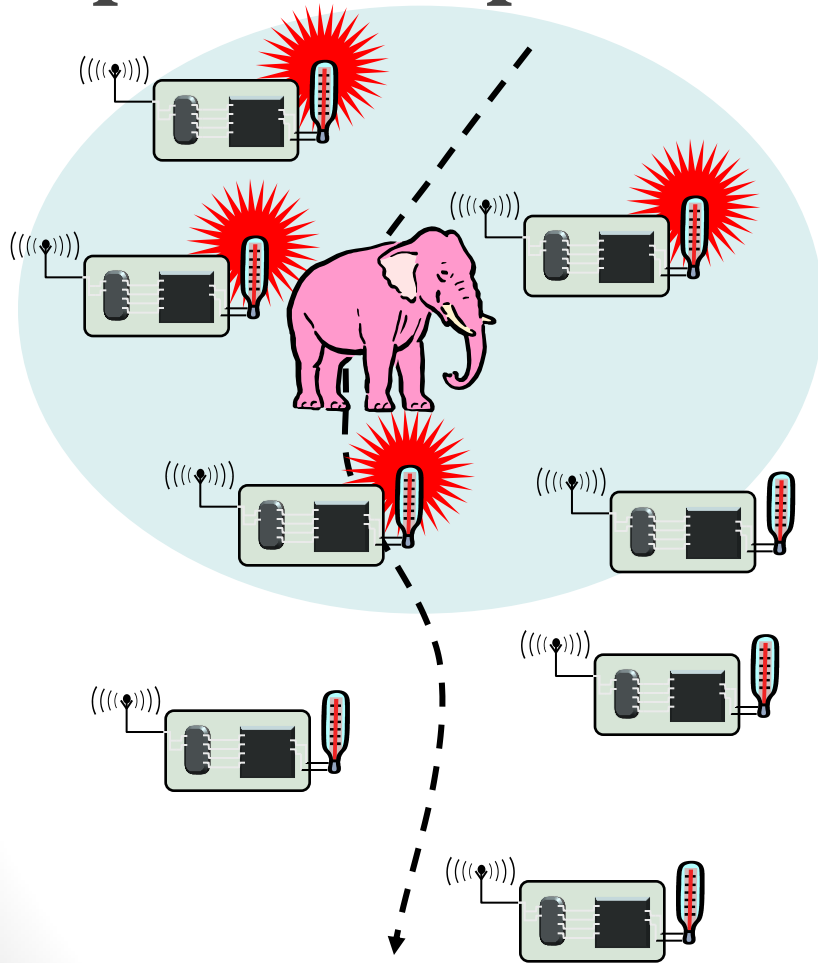
- Node mobility
 - A node participating as source/sink (or destination) or a relay node might move around
 - Deliberately, self-propelled or by external force; targeted or at random
 - Happens in both WSN and MANET
- Sink mobility
 - In WSN, a sink that is not part of the WSN might move
 - Mobile requester
- 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

OPTIMIZATION GOALS



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

- 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 solutions!



DESIGN PRINCIPLES



Distributed organization

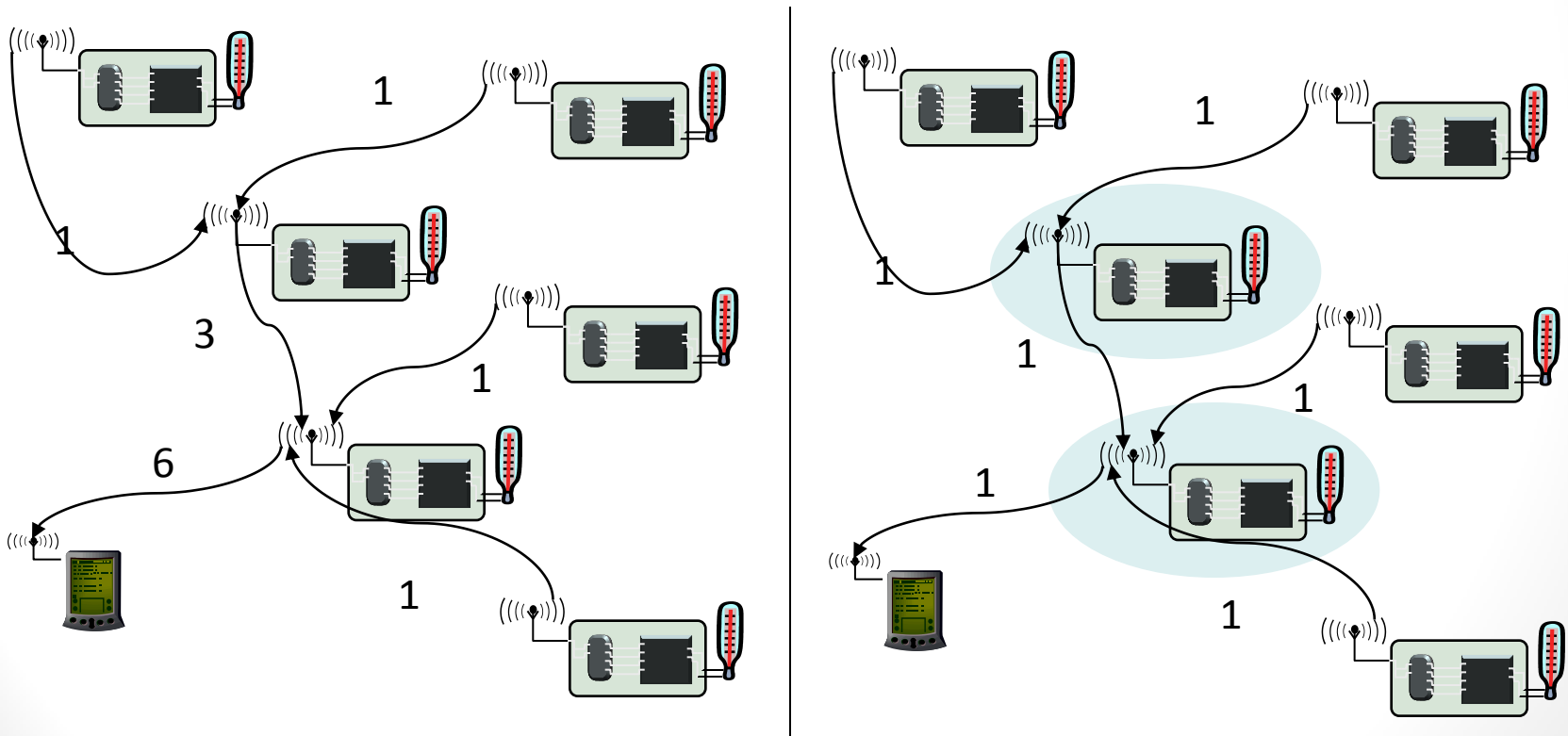
- Participants in a MANET/WSN should cooperate in organizing the network
 - E.g., with respect to medium access, routing, ...
 - Centralistic approach as alternative usually not feasible – hinders scalability, robustness
- Potential shortcomings
 - Not clear whether distributed or centralistic organization 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 ! no need to transmit all data at full rate all the time
 - Signals of neighboring nodes are often quite similar ! 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 subscribers
 - Subscription and publication are decoupled in time; subscriber and publisher 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

SERVICE INTERFACE



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

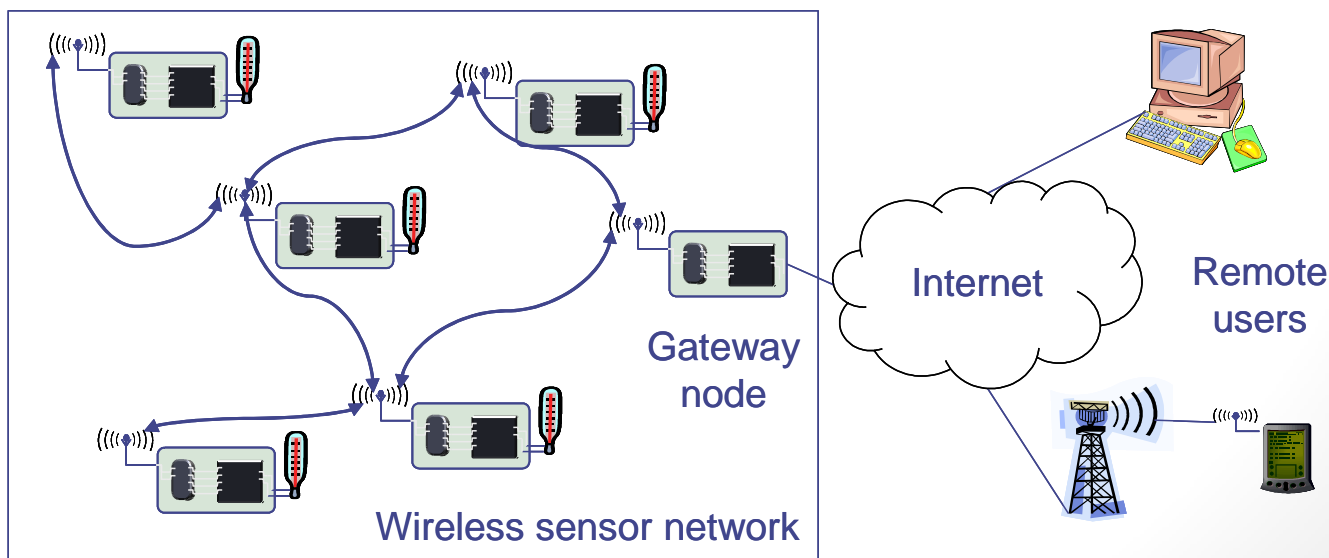


GATEWAY CONCEPTS



Gateway concepts for WSN/MANET

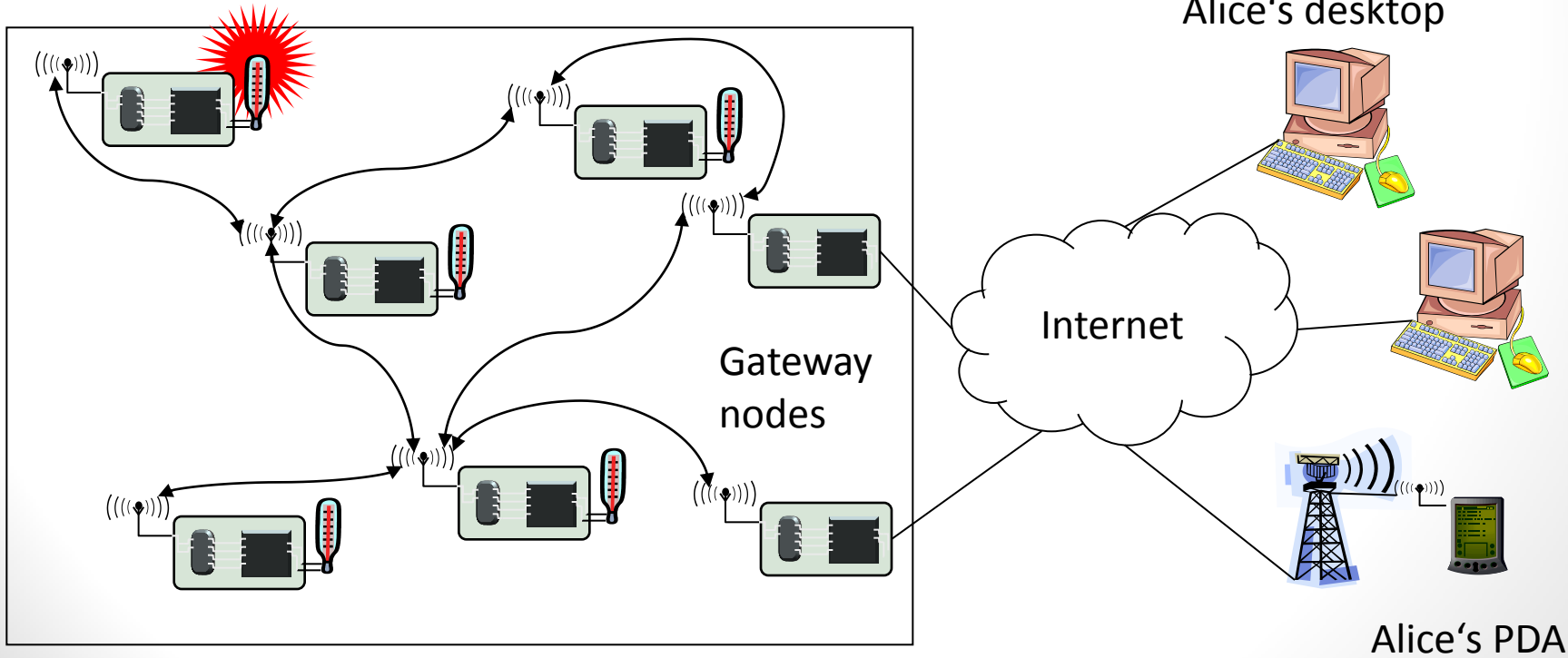
- Gateways are necessary to the Internet for remote access to/from the WSN
 - Same is true for ad hoc networks; additional complications due to mobility (change route to the gateway; use different gateways)
 - WSN: Additionally bridge the gap between different interaction semantics (data vs. address-centric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



WSN to Internet Communication

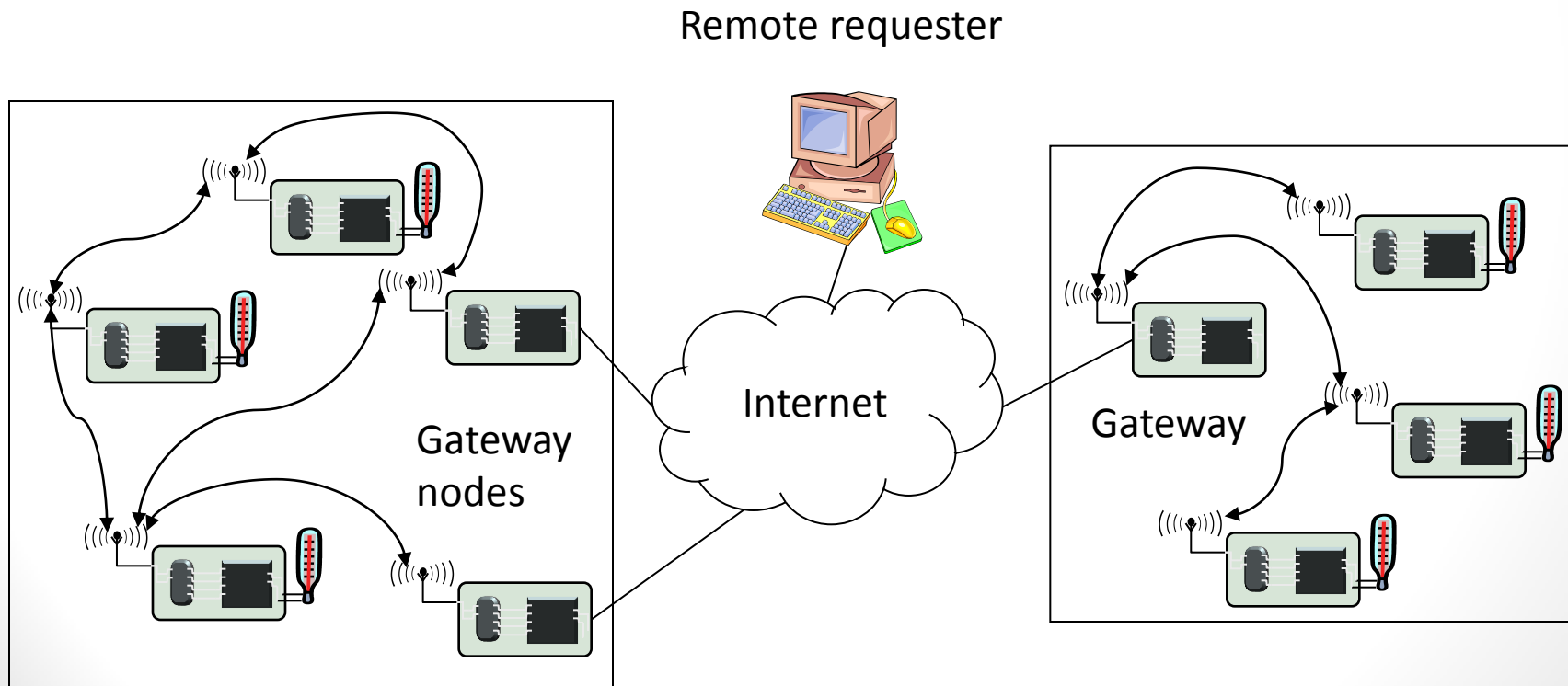
- Example: Deliver an alarm message to an Internet host
- Issues
 - Need to find a gateway (integrates routing & service discovery)
 - Choose “best” gateway if several are available
 - How to find Alice or Alice’s IP?

Alert Alice



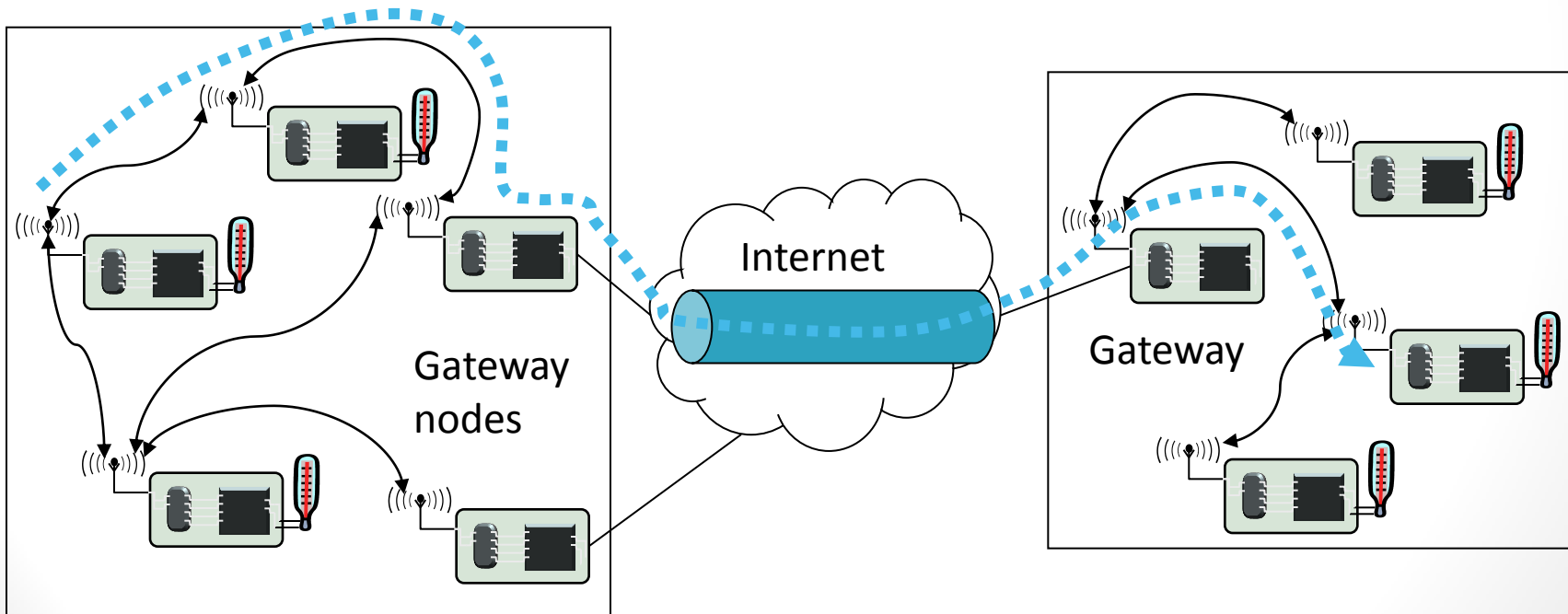
Internet to WSN communication

- 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

- For more details, refer to:
 - Chapter 3, H. Karl and A. Willig, **Protocols and Architectures for Wireless Sensor Networks**, Wiley 2005.
- The lecture is available online at:
 - <http://bu.edu.eg/staff/ahmad.elbanna-courses/12189>
- For inquires, send to:
 - ahmad.elbanna@feng.bu.edu.eg