6. Ad-hoc networks, MANETs

PA191: Advanced Computer Networking.

Eva Hladká

Slides by: Tomáš Rebok

Faculty of Informatics Masaryk University

Autumn 2022

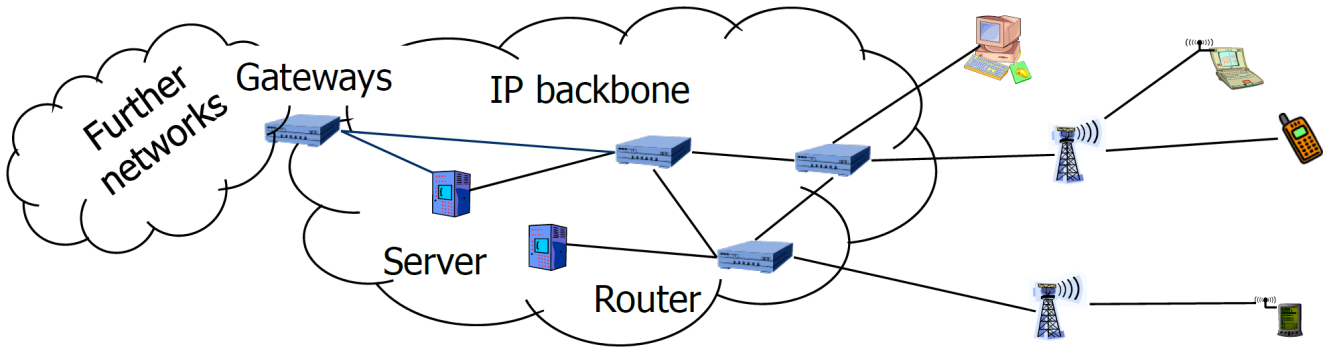
Lecture Overview

1. Wireless Ad-hoc Networks
   - Motivation
   - (Mobile) Wireless Ad-hoc Networks
   - Wireless Sensor Networks
   - MANETs vs. WSNs
   - MANETs vs. P2P
2. Medium Access Control in Ad-hoc and Sensor Networks
   - Protocols' Classification
   - Contention-based protocols
   - Improving Energy Efficiency
3. Ad-hoc Routing
   - Address-based Ad-hoc Routing Protocols
   - Proactive Protocols
   - Reactive Protocols
   - Specialized Routing Protocols
4. Conclusion & Information Sources

Lecture Overview

Wireless Networks I.

- *A need: how to access computing and communication services* **on the move?**
  - $\Rightarrow$ wireless networks
- *wireless networks* are traditionally based on a *cellular infrastructure*
  - a land area that should be covered with a radio service is divided into cells
  - each cell is covered by a (base) station
    - base stations connected to a wired backbone network
  - the mobile nodes communicate wirelessly to these 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
  - e.g., GSM, UMTS, WLAN, ...



Wireless Networks II.

- but what, if:
  - no infrastructure becomes available? (e.g., disaster areas, emergency operations)
    - e.g., hurricane Cathrina (2005) destroyed huge parts of New Orleans including communication networks
  - it is too expensive to set it up? (e.g., remote/large places, construction areas)
  - there is no time to set it up? (e.g., military operations)
- $\Rightarrow$ **Wireless Ad-hoc Networks**
  - try to construct a network without infrastructure, using *networking abilities of the participants*
  - *ad-hoc network* = a network constructed on demand "for a special purpose"
    - the term ad-hoc is Latin meaning "for this purpose"

Wireless Ad-hoc Networks

Wireless Ad-hoc Network

- a collection of autonomous nodes that communicate with each other by forming a multihop radio network and maintaining connectivity in a decentralized manner
  - each node functions as both a *host* and a *router*
  - the control of the network is distributed among the nodes
  - the network topology is (in general) dynamic
    - the connectivity among the nodes may vary in time due to node departures, new node arrivals, and the nodes' mobility
    - $\Rightarrow$ a need for efficient routing protocols that allow the nodes to communicate over multihop paths in an efficient way
- these networks pose many complex issues $\Rightarrow$ there are many open problems for research
  - without a central infrastructure, things become much more difficult

Wireless Ad-hoc Networks

Simple example

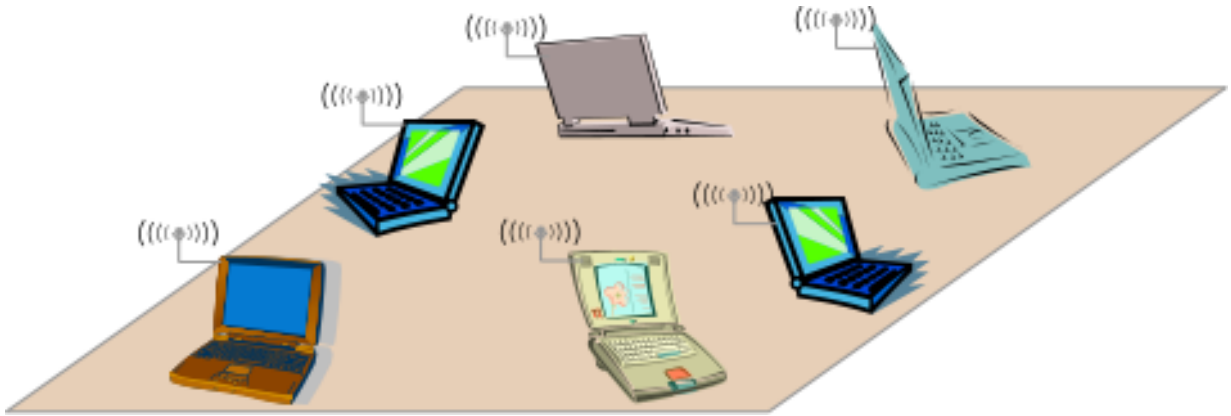


Figure: Simple example: laptops in a conference room – a single-hop ad-hoc network (all the networking nodes are in a direct communication range of each other node).

Wireless Ad-hoc Networks

Multihop Network example

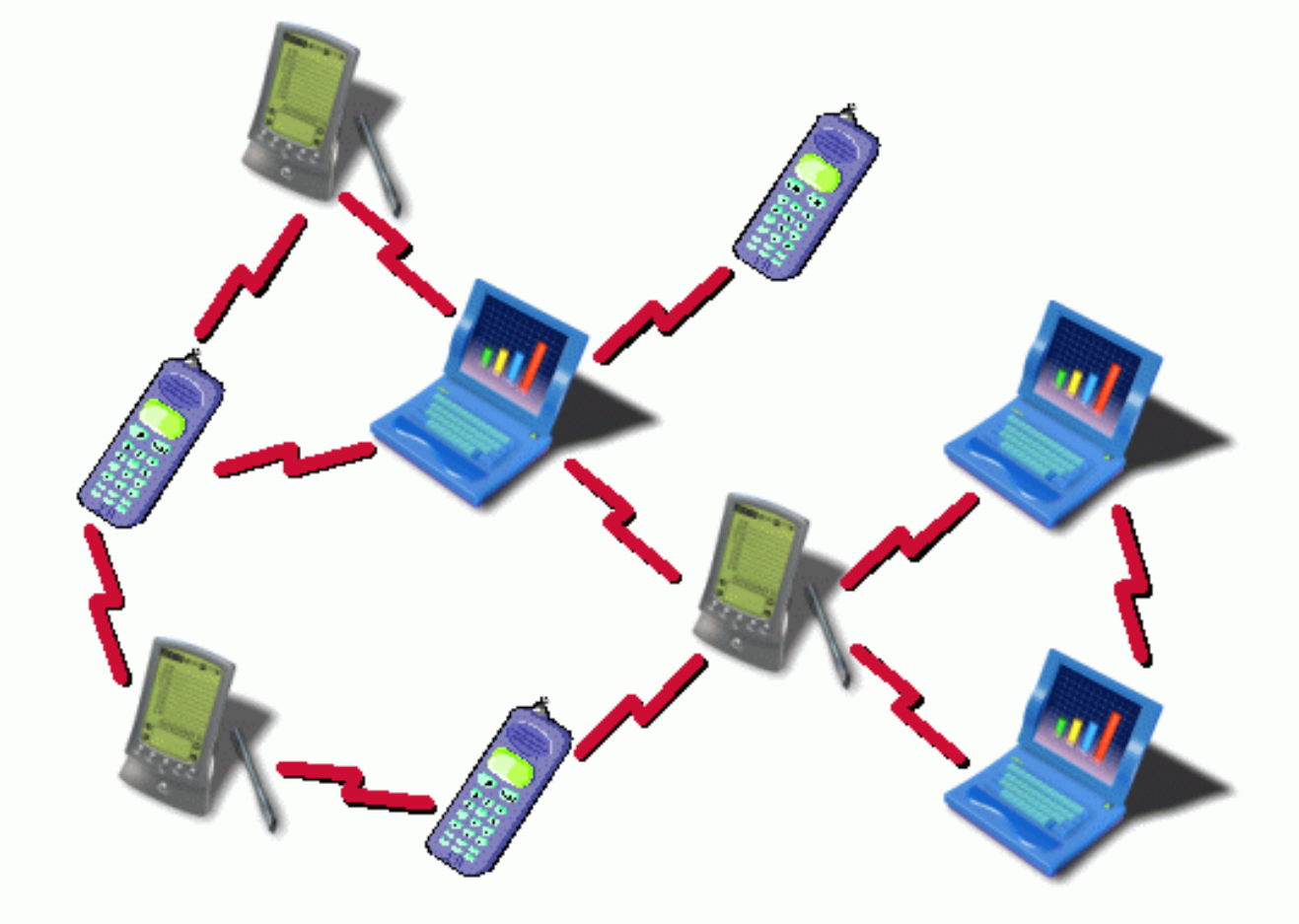


Figure: Multihop (mobile) ad-hoc network example.

Wireless Ad-hoc Networks

Advantages

- very fast construction
  - no need to establish wired connections
- resilient
  - no single point of failure, such as a base station
- spectrally more efficient than cellular networks
  - every node can communicate with any other node (sometimes even simultaneously), so nodes can make better use of the channel

Wireless Ad-hoc Networks

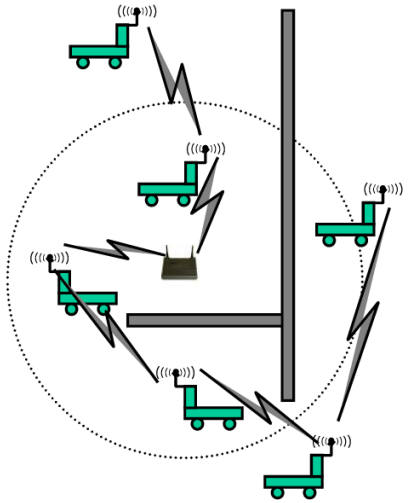
Problems/Challenges

- problems arise due to:
  - lack of a central entity for network organization
    - the participating nodes must organize themselves into a network
    - *self-organization* is a must
  - limited range of wireless communication
    - data have to be delivered over a path involving multiple nodes
    - $\Rightarrow$ mechanisms for dynamic path identification and management are required
  - mobility of participants
    - the network nodes may be allowed to move in time and space
    - the network quality depends on the speed to adapt to new topologies
    - $\Rightarrow$ **Mobile Ad-hoc Networks (MANETs)**
- among others, the following issues have to be addressed:
  - *medium access control* – no base station can assign transmission resources (it must be decided in a distributed fashion)
  - *routing* – finding a route from one participant to another

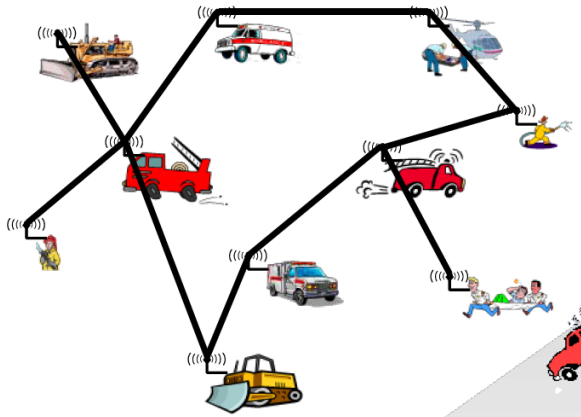
(Mobile) Wireless Ad-hoc Networks

Possible Applications

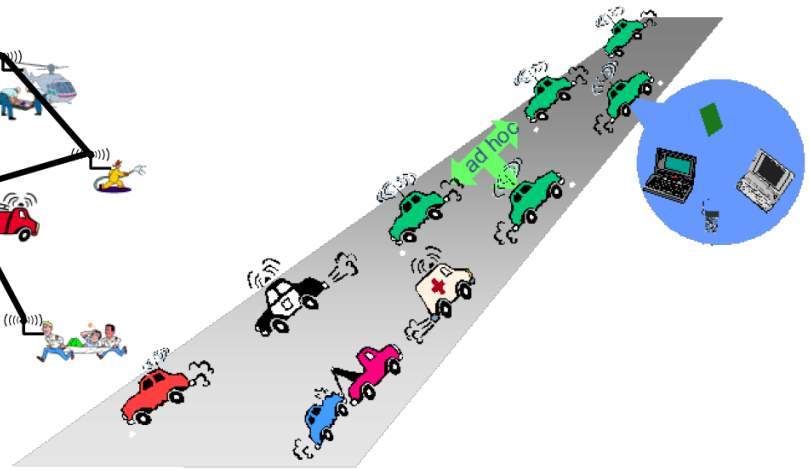
Factory floor automation



Disaster recovery



Car-to-car communication



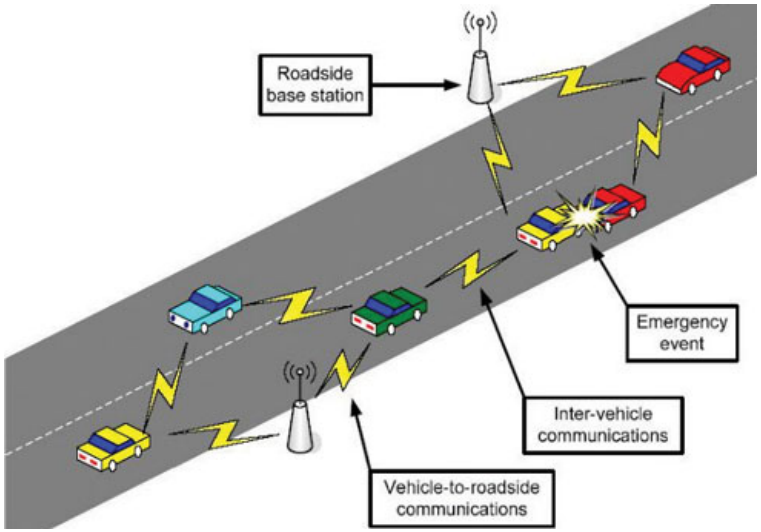
- finding out empty parking lots in a city (without asking a server), avoiding traffic jams/congestions, etc. (= VANETs)
- search-and-rescue in an avalanche
- personal area networking (watch, glasses, PDA, medical appliance, . . .)
- military networking: tanks, soldiers, . . .
- collaborative and distributed computing
- . . .

(Mobile) Wireless Ad-hoc Networks

Vehicular Ad-hoc Networks (VANETs)

Vehicular Ad-hoc Networks (VANETs)

- a technology that uses moving cars as nodes/routers to create a mobile network
  - the cars are allowed to connect to each other (if being in a wireless range) and thus to create a network with a wide range
- in comparison with MANETs, where the nodes move in a random way, the cars tend to move in an organized fashion
  - moreover, the interactions with roadside equipment can be characterized fairly accurately
  - $\Rightarrow$ more specialized routing protocols may be employed



(Mobile) Wireless Ad-hoc Networks

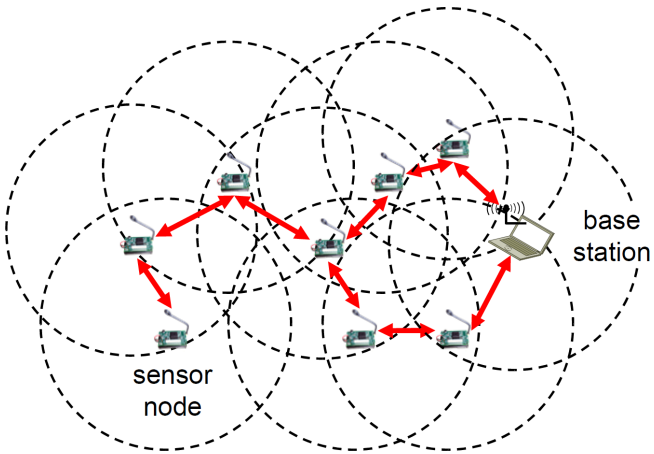
Comparison with Infrastructure-based networks

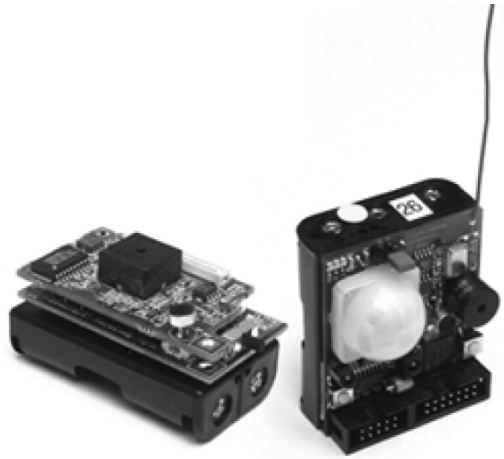
	Infrastructure-based network	**Ad hoc network**
Prerequisites	Pre-deployed infrastructure, e.g. routers, switches, base stations, servers	None
Node properties	End system only	Duality of end system and network functions
Connections	Wired or wireless	Usually wireless
Topology	Outlined by the pre-deployed infrastructure	Self-organized topology maintained by the nodes
Network functions	Provided by the infrastructure	Distributed to all participating nodes

Figure: Comparison between infrastructure-based and infrastructure-less (ad-hoc) networks.

Wireless Sensor Networks

- so far, the participants were devices close to a *human user* (i.e., interacting with humans)
- alternative concept:
  - instead of focusing interaction on humans, focus on interacting with an **environment**
    - network is embedded in an environment (in a random or regular fashion)
    - nodes in such a network are equipped with sensing/actuation to measure/influence the environment
    - the nodes process information and communicate it wirelessly
  - $\Rightarrow$ *Wireless Sensor Networks (WSNs)*
    - or *Wireless Sensor & Actuator Networks (WSANs)*



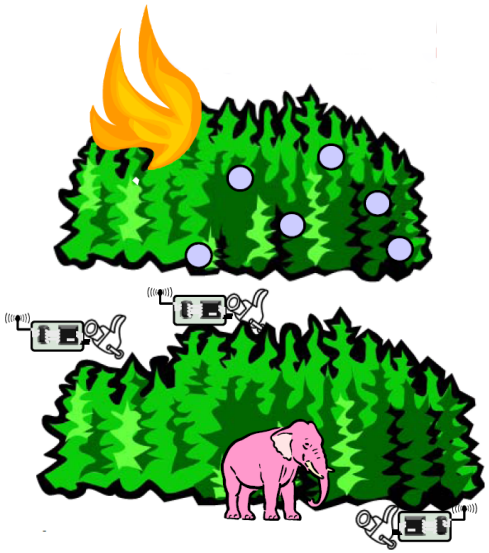


Wireless Sensor Networks

Application Examples

Emergency operations

- e.g., dropping sensor nodes over a wildfire
  - each node measures temperature
  - possible to derive a "temperature map"



Habitat monitoring

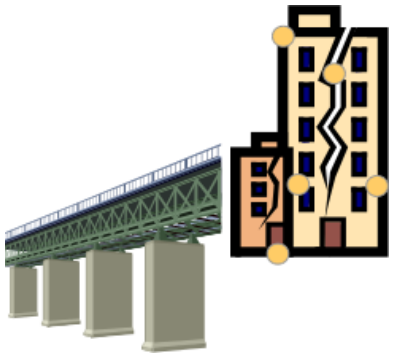
- e.g., sensor nodes to observe wildlife
  - Great Duck Island, ZebraNet, etc.

Precise agriculture

- bringing out fertilizer/pesticides/irrigation only where needed

Intelligent buildings, bridges

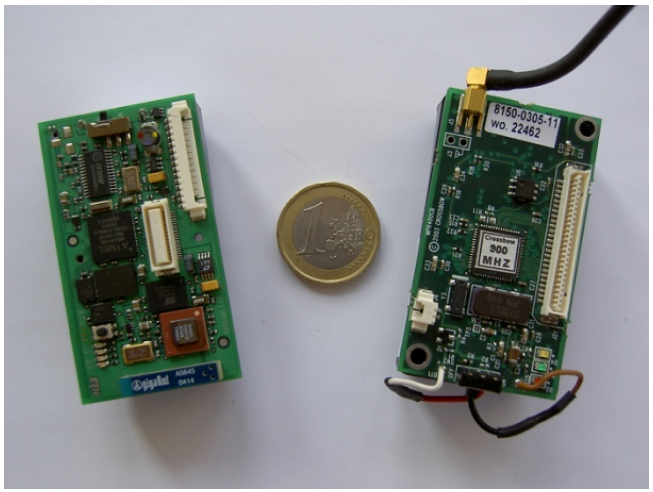
- reducing energy wastage by proper humidity, ventilation, air conditioning
  - needs measurements about room occupancy, temperature, air flow
- monitoring mechanical stress after earthquakes

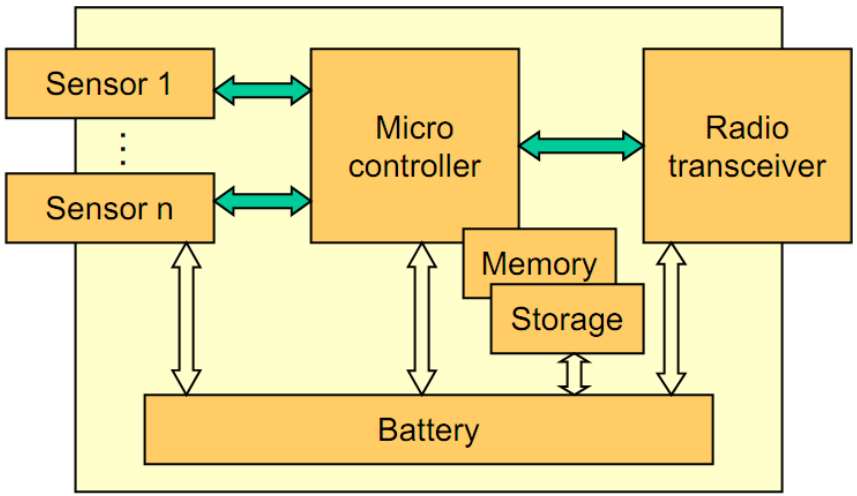


Wireless Sensor Networks

Sensors – HW

- *sensor HW*
  - processor (and memory)
    - e.g., Atmel ATmega128 microcontroller, 16 MHz, 128 kByte flash
  - radio transceiver
    - e.g., Chipcon CC1000 (315/433/868/915 MHz), CC2400 (2.4 GHz)
  - battery
    - possibly in combination with energy harvesting
  - sensors
    - light, temperature, motion, ...

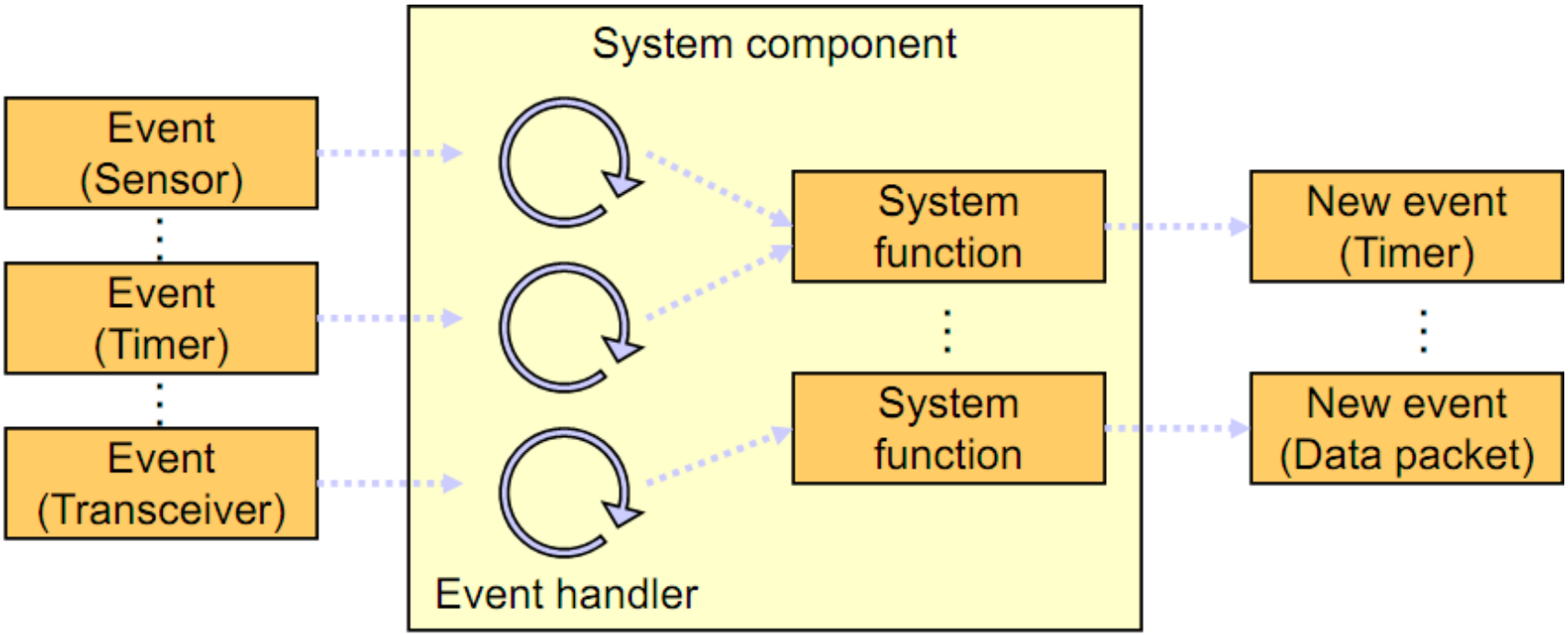




Wireless Sensor Networks

Sensors – SW

- *sensor software*
  - event-driven operating principle
    - e.g., TinyOS



Wireless Sensor Networks

Importance of an Energy-efficient Operation

- often (but not always), the participants in an ad-hoc network (not only sensor network) draw energy from batteries
- it is desirable to sustain a long run time for:
  - individual nodes/devices
  - the network as a whole
    - usually, application demands do not bother with individual nodes, as long as the global application-dependent objective can still be fulfilled
- employed networking protocols have to take the limited energy into account and behave in an energy-efficient way
  - e.g., use routes with low energy consumption (energy/bit)
  - e.g., take available battery capacity of devices into account
  - How to resolve conflicts between different optimizations?
- some form of recharging or energy scavenging from the environment is often used in order to increase the available energy

Wireless Sensor Networks

Required functionality and constraints

- *Available energy*
  - sensor nodes are operated by batteries that provide limited energy for the node
- *Processing power*
  - employed micro controllers usually provide very limited processing performance (due to size and energy restrictions)
- *Memory and storage*
  - the characteristics of the available memory usually correlate with the size of the micro controller
- *Bandwidth and throughput*
  - wireless radio transceivers are optimized for low-energy operation $\Rightarrow$ they provide a relatively small bandwidth to the application
- *Reliability*
  - depending on the application scenario, the demands for the reliability (both communication reliability and error-proneness of the hardware) can strongly differ
- *Addressing*
  - typically, off-the-shelf sensor nodes do not have a globally unique address pre-programmed $\Rightarrow$ networking mechanisms must either dynamically allocate unique addresses or even abandon address-based techniques
- *Scalability*
  - a primary constraint – the scalability of employed methods and algorithms

MANETs (VANETs) vs. WSNs

Many similarities:

- both networks strongly rely on self-organization mechanisms (neighborship relations and network topology maintenance)
- both networks have to cope with limited energy in the devices
  - the energy efficiency of employed algorithms and methods is of the highest importance
- both networks often use wireless multi-hop communications

Many differences:

Resources and properties	MANET	WSN
Available energy	High	Low
Processing power	High	Low
Memory and storage	High	Low
Density and scale	Low	High
Mobility	High	Limited*
Heterogeneity	Medium*	Low*
Varying user demands	High	Low

* Depending on the application scenario

MANETs vs. P2P Systems I.

Wireless ad-hoc networks have also many similarities with P2P systems:

- same paradigm
- self-organizing network
- dynamic topology
- responsible for routing queries in a distributed environment
- lack managing and centralizing units

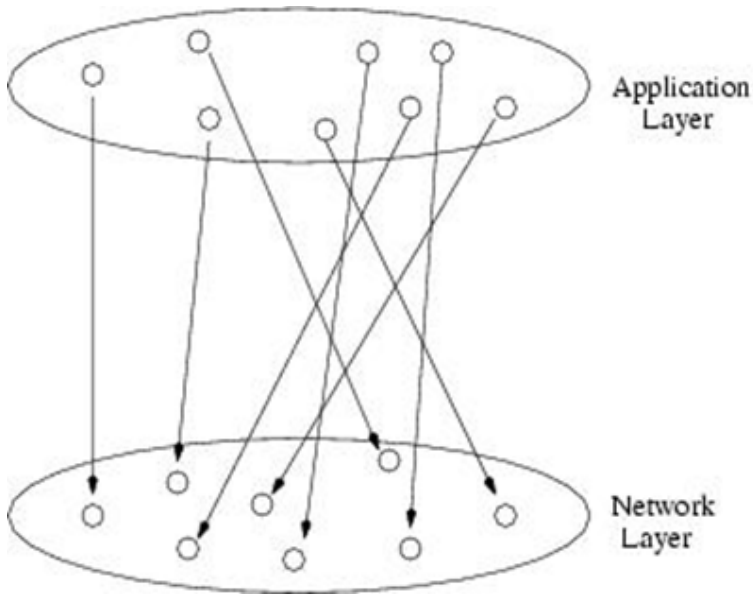
However, there are also great differences $\rightarrow$

MANETs vs. P2P Systems II.

Difference	P2P Network	MANET
Motivation for creating the network	Logical infra structure to provide a service	A physical infra-structure to provide connectivity
Connection Between two nodes	Fixed medium and direct	Wireless and indirect
Connection confidence	High (physical connections)	Low (wireless connections)
Peer location	Any Internet point	Restricted area
Structure	Physical apart from logical structure	Physical structure corresponds to logical structure
Routing	reactive	Proactive, reactive
Peer behavior	Fixed	Mobile
Broadcast	Virtual, multiple unicasts	Physical, to all nodes in transmission range area

MANETs vs. P2P Systems III.

- $\Rightarrow$ MANET rather is a *platform for P2P applications*
- however, existing solutions for wireline Internet cannot be applied directly on MANET for P2P communication, mainly because:
  - neighbors at the application layer (P2P view) may not necessarily be neighbors at the network layer (MANET view)
- $\Rightarrow$ in order to deploy P2P applications **efficiently** in MANETs, existing P2P solutions must be subjected to considerable modifications to take many MANET's specifics into account



Lecture Overview

Medium Access Control in Ad-hoc and Sensor Networks I.

- *Medium Access Control (MAC)*
  - responsible for coordination of nodes' access to a shared transmission media
  - the goal is to minimize collisions
    - i.e., simultaneous transmissions, which lead to signal corruptions
- medium access in (infrastructure, ad-hoc) wireless networks is difficult mainly because of:
  - it is impossible (or very difficult) to send and to receive at the same time
  - from the sender's point of view, it is hard to estimate the interference situation at the receiver's side
  - high error rates make it rather hard to establish a well coordinated communication link among nodes over the wireless medium
- requirements for ad-hoc/sensor networks' MAC protocols:
  - *as usually:* high throughput, low overhead, low error rates, ...
  - *additionally:* **energy-efficiency**

Medium Access Control in Ad-hoc and Sensor Networks II.

- effects, that contribute to **energy wastage**:
  - *collisions*
    - wasted effort when two packets (transmissions) collide – the detection of and reaction to collisions, and data retransmissions require additional energy
  - *overhearing*
    - if a node is receiving a packet that is destined for another receiver in the same wireless transmission range, the required energy for receiving the packet (or at least parts of it) and the detection that it is destined to another node are waste efforts
  - *idle listening*
    - since the receiving node has no knowledge when a sender may begin a transmission, it must be idle, waiting for a possible packet reception (energy is wasted for doing nothing)
  - *protocol overhead*
- another issue is a **mobility of the nodes**:
  - it can essentially affect the performance (throughput) of the protocol
    - e.g., bandwidth reservations or exchanged control information may become useless if nodes are moving quickly
  - $\Rightarrow$ protocol design must take this mobility factor into consideration

Classification of MAC Protocols for Wireless Radio Nets

MAC protocols for wireless radio networks can be distinguished into the following classes:

- **Contention-based protocols** – description follows
- **Contention-based protocols with reservation mechanisms**
  - support for real-time traffic using QoS guarantees
  - use mechanisms for reserving bandwidth a priori
  - *synchronous* (require time synchronization among all nodes in the network) and *asynchronous* (usually rely on relative time information)
  - e.g., MACA/PR (MACA with Piggy-Backed Reservation)
- **Contention-based protocols with scheduling mechanisms**
  - focus on packet scheduling at nodes and also scheduling nodes for access to the channel
  - used to enforce priorities among flows (i.e., QoS support is available)
  - sometimes battery characteristics (e.g., remaining battery power) are considered while scheduling nodes for access to the channel
  - e.g., LEACH (Low-Energy Adaptive Clustering Hierarchy), SMACS, TRAMA

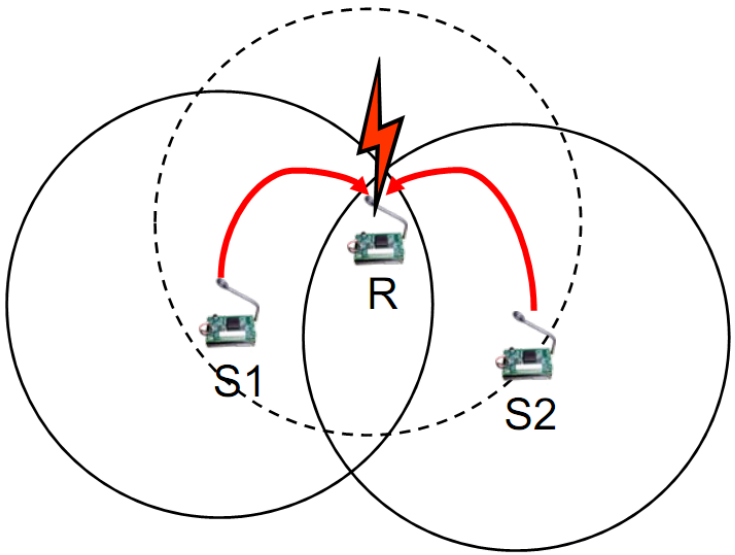
Contention-based protocols

- no a priori resource reservation
- whenever a packet should be transmitted, the node contends with its neighbors for access to the shared channel
  - if multiple nodes want to access the channel at the very same time, collisions cannot be avoided
  - $\Rightarrow$ contention resolution has to be provided by the protocols
- cannot provide QoS guarantees
- two approaches:
  - *sender-initiated protocols* – the packet transmissions are initiated by the sender node
  - *receiver-initiated protocols* – the receiver node initiates the contention-resolution protocol
- have to cope with two fundamental problems:
  - hidden and exposed terminals

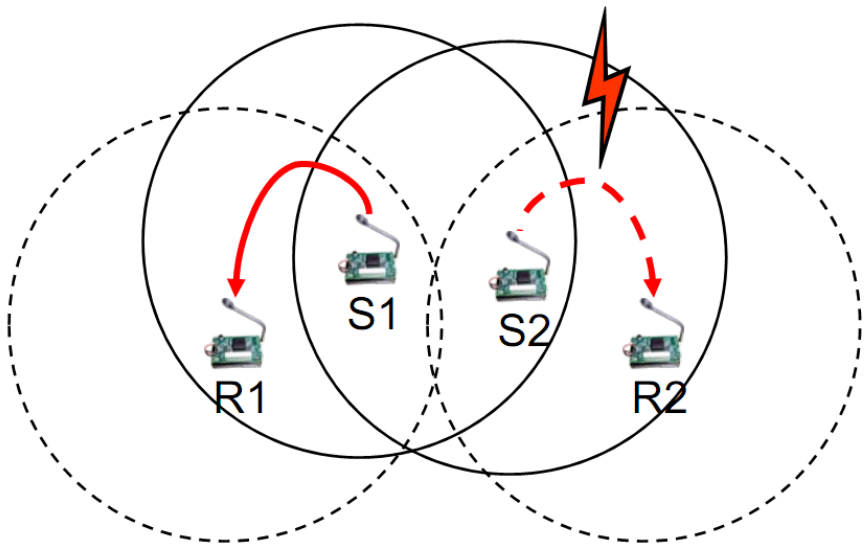
Contention-based protocols

Hidden and Exposed Terminals Problems

- *Hidden terminal problem* – collision of packets due to simultaneous transmission of those nodes that are not within the direct transmission range of the sender but are within the transmission range of the receiver
- *Exposed terminal problem* – inability of a node, which is blocked due to transmission by a nearby transmitting node, to transmit to another node



Hidden terminal



Exposed terminal

Contention-based protocols

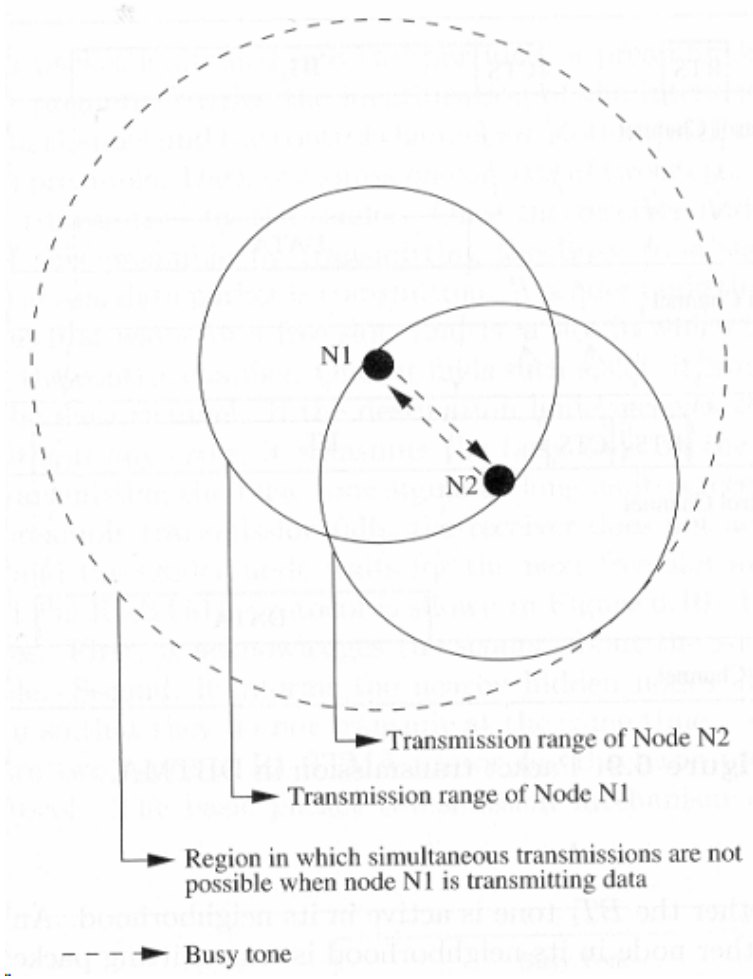
Main Options to Shut Up Senders

To reserve a channel during/for a transmission, two basic options are possible:

- receiver informs potential interferers **while** a reception is on-going
  - by sending out a signal indicating just that
  - problem: cannot use the same channel on which actual reception takes place
    - $\Rightarrow$ necessary to use a separate channel for signaling
  - e.g., *Busy tone protocol*
- receiver informs potential interferers **before** a reception is on-going
  - can use same channel
  - receiver itself needs to be informed, by sender, about impending transmission
  - potential interferers need to be aware of such information
  - e.g., *MACA protocol*

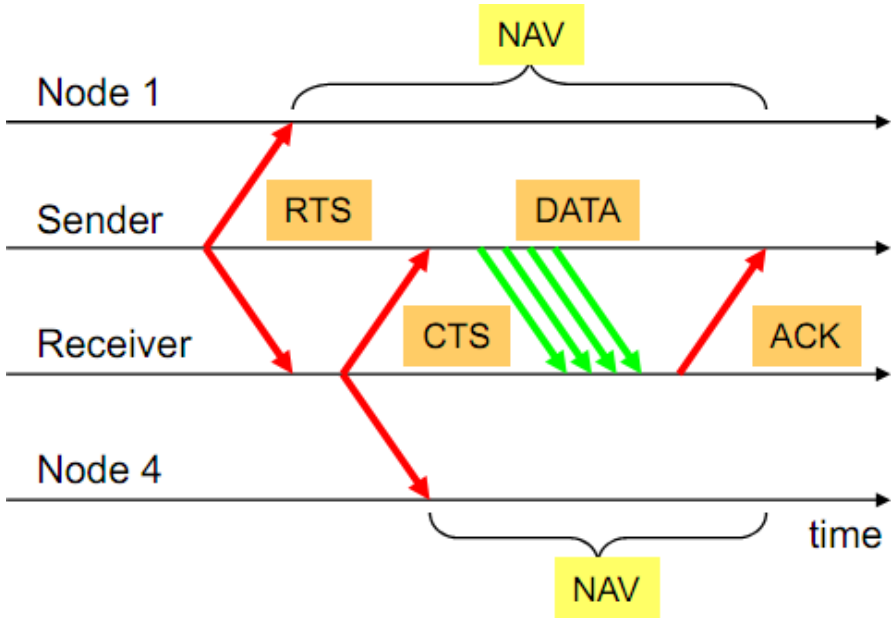
BTMA – Busy Tone Multiple Access

- the transmission channel is split into data and control channel
- general behavior:
  - when a node wants to transmit a packet, it senses the channel to check whether the busy tone is active
  - if not, it turns on the busy tone signal and starts transmission
- problem: very poor bandwidth utilization



MACA — Multiple Access Collision Avoidance

- well-established MAC protocols in the ad-hoc domain
- use of additional signaling packets:
  - sender asks receiver whether it is able to receive a transmission – *Request to Send (RTS)*
  - if receiver agrees, it sends out a *Clear to Send (CTS)*
  - sender sends, receiver acks
- potential interferers overhear RTS/CTS
  - RTS/CTS packets carry the expected duration of the data transmission
  - store this information in a *Network Allocation Vector (NAV)*



Power-Control MAC (PCM) protocol I.

- PCM provides a MAC layer solution for power control by varying the transmission power to reduce the overall energy consumption
- *the idea:*
  - RTS/CTS handshake messages should be transmitted with the maximum available power p_{max}
  - the handshake is used to determine the required transmission power $p_{desired}$ that is used for the subsequent DATA/ACK transfer
  - the calculation of $p_{desired}$ is performed from the signal level of the received RTS in combination with some well known minimum threshold for the received signal strength Rx_{thresh} that is necessary for correctly decoding the messages
- *the calculation:*
  - $p_{desired} = \frac{p_{max}}{p_r} Rx_{thresh} \times c$
  - where p_r denotes the received power level and a constant parameter c is used to increase $p_{desired}$ according to environmental conditions
- can be combined with any RTS/CTS based MAC protocol (i.e., including MACA)

MACA — Energy Consumption Reduce II.

Power-Control MAC (PCM) protocol II.

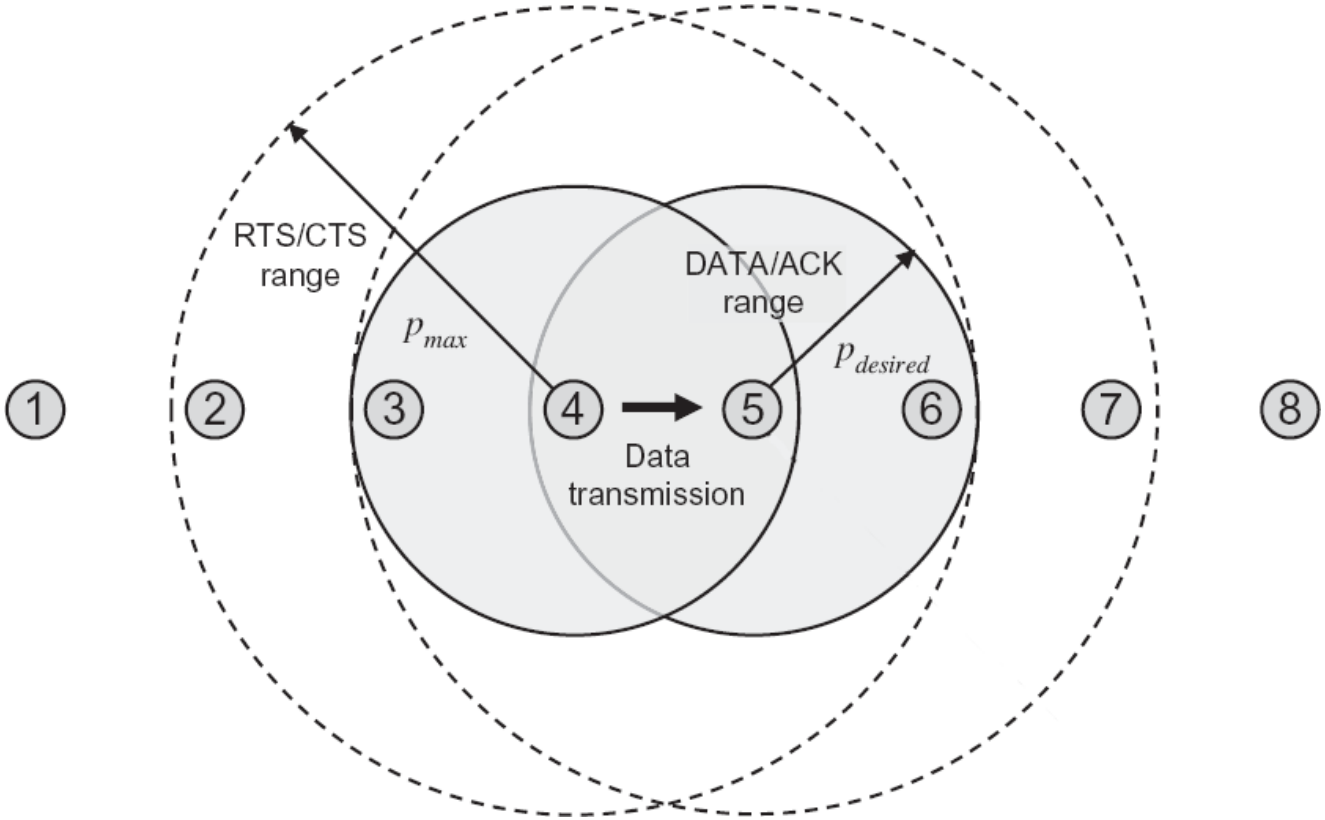
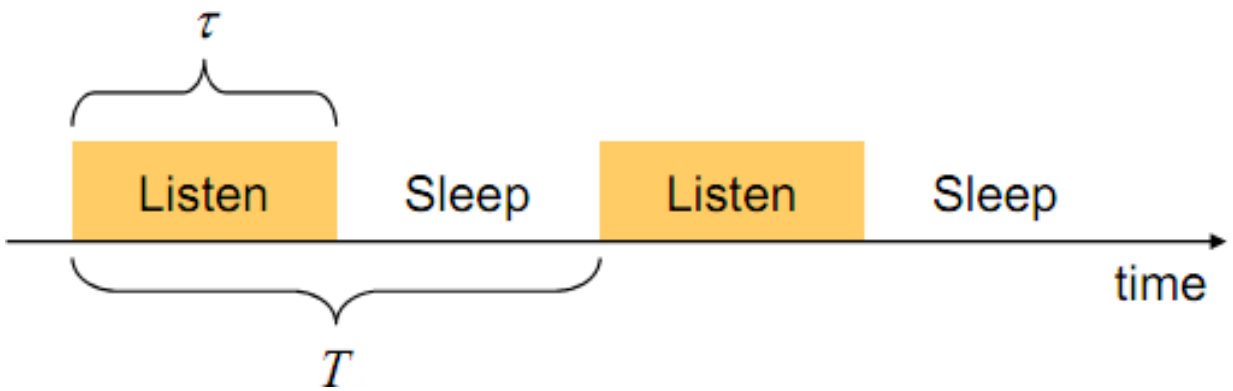


Figure: Transmission ranges used by PCM for RTS/CTS and DATA/ACK, respectively.

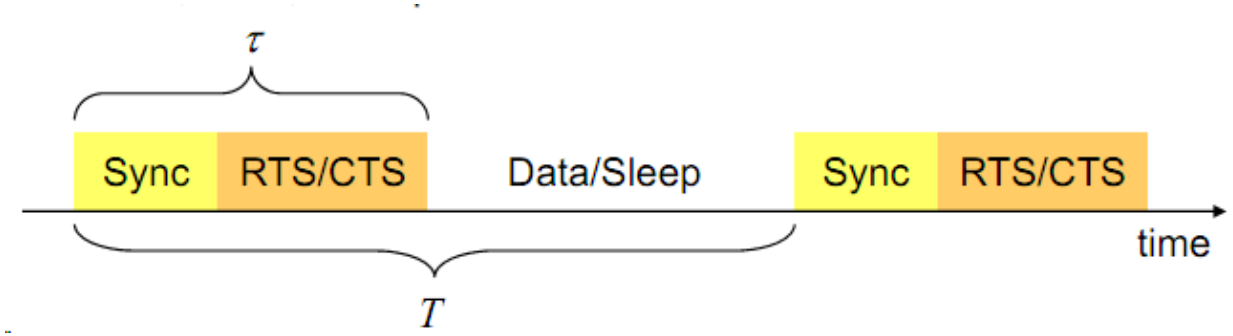
Sensor-MAC (S-MAC) I.

- new protocol improving the energy efficiency in multi-hop radio networks
- *primary goal:* to retain flexibility of contention-based protocols while improving energy efficiency in multi-hop networks
  - MACA's idle listening is particularly unsuitable if average data rate is low (most of the time, nothing happens)
- *the idea*: switch nodes off and ensure that neighboring nodes turn on simultaneously to allow packet exchange ("rendez-vous")
  - only in these active periods packet exchanges can happen
  - requires to exchange a wakeup schedule between neighbors
  - when awake, essentially perform RTS/CTS
  - it introduces coarse-grained listen/sleep cycle with a *duty-cycle* $D = \frac{\tau}{T}$
    - duty-cycle = a measure for the energy efficiency of a node



Sensor-MAC (S-MAC) II.

- in fact, the listen period is divided to support synchronization between neighboring nodes as well as the contention for the wireless channel using the RTS/CTS handshake mechanism

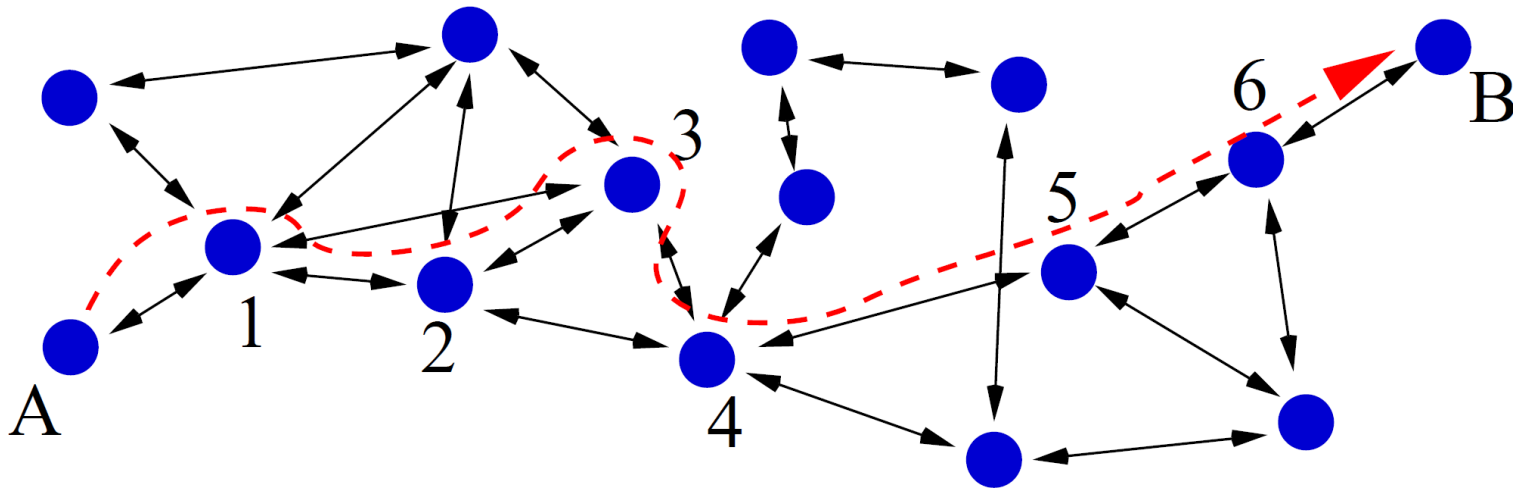


- the explicit (time) synchronization was introduced to support low duty-cycle operations of 1 – 10 %
- all nodes choose their own listen/sleep schedules
  - these schedules are shared with their neighbors to make communication between all neighboring nodes possible
- each node periodically broadcasts its schedule in a SYNC packet, which provides simple time synchronization
- to reduce overhead, S-MAC encourages neighboring nodes to adopt identical schedules
- many other variants exist: T-MAC, B-MAC, P-MAC, Z-MAC, etc.

Lecture Overview

Ad-hoc Routing

- typically, nodes are not within the direct communication range of all other nodes
- nodes need to discover routes (consisting of intermediate nodes) through which they can deliver their packets to their distant destinations
  - = a task of a **routing protocol**
  - complicated by the presence of node mobility, and the lack of centralized control
- the routing protocol must be coupled with a medium access control (MAC) protocol
  - the routing protocol specifies to whom a node should transmit the packet
  - the MAC protocol specifies when it should transmit the packet



Ad-hoc Routing

Address-based routing vs. data-centric forwarding I.

Address-based routing

- the first routing approaches for ad-hoc and sensor networks
- messages are directed towards a well-specified particular destination (sink)
  - $\Rightarrow$ these routing protocols require each node to have a network-wide unique address or identifier
- provide support for unicast, multicast, and broadcast messages
- *obvious advantage:* the possibility of identifying specific (unique) nodes and sending messages to them

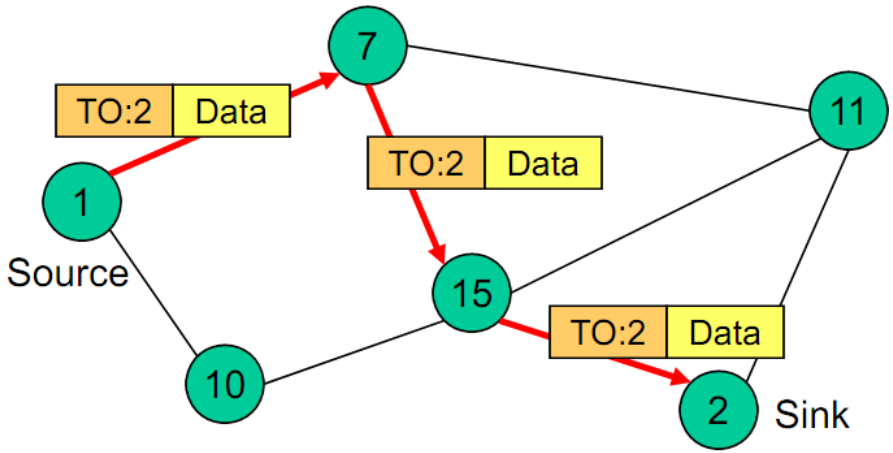


Figure: Principles of address-based routing: a data packet carrying the destination address "TO:2" is forwarded along an established path towards its final destination: node 2.

Ad-hoc Routing

Address-based routing vs. Data-centric forwarding II.

Data-centric forwarding

- sometimes (especially in WSNs), the unique addresses are not demanded by the application requirements but only by the employed routing protocols
  - $\Rightarrow$ the addressing scheme can be removed and replaced with the specific semantics of the transmitted messages
    - node addresses are replaced by a kind of interest of particular nodes
    - payload information (data) is used to forward messages towards an appropriate destination

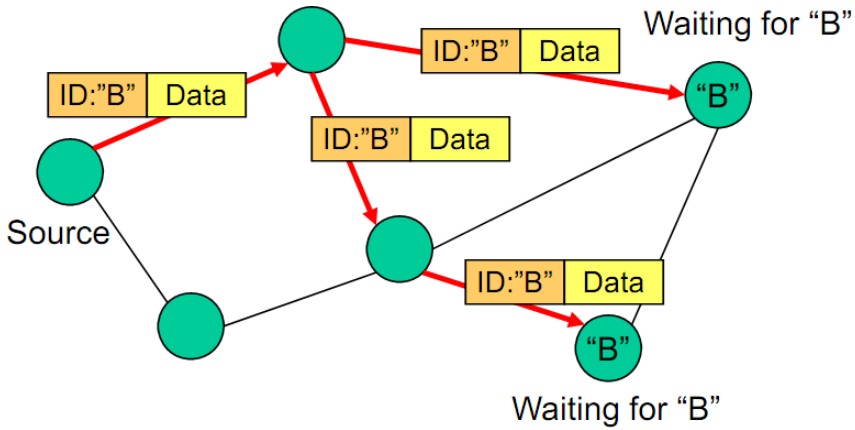


Figure: Principles of data-centric forwarding: messages are forwarded according to their internal meaning – messages of type "B" are transmitted to two sinks, which requested exactly messages of type "B".

Ad-hoc Routing

Address-based routing vs. Data-centric forwarding III.

	Address-based routing	Data-centric forwarding
Routing approach	Identification of a path according to the destination address of the data message	Determination of the destination of a data message according to the content of the packet
Prerequisites	Network-wide unique addresses	Pre-defined message types and semantics
Routing techniques	Proactive routing (continuous state maintenance) or reactive routing (on-demand path finding)	(probabilistic) flooding schemes or interest-based reverse routing
Advantages	Usually low delays in connection setup and data dissemination	No address information required and simplified self-management and redundancy
Disadvantages	Network-wide unique address identifiers required	Increased overhead for single transmissions

Address-based Ad-hoc Routing

Classification of Routing Protocols I.

Many different classifications of routing protocols exist:

- **proactive** vs. **reactive** protocols:
  - *Proactive protocols*
    - discover routes before they are needed
    - provide small latency, but large routing overheads
  - *Reactive protocols*
    - discover routes only when they are needed
    - provide small routing overhead, but higher latency
- **table-driven** vs. **source-routing** protocols:
  - *Table-driven protocols*
    - each node only knows the next hop to a destination
    - the routing overhead is small, but routing loops may be formed
  - *Source-routing protocols*
    - nodes know the complete route to a destination
    - routing loops are easy to avoid, but the routing overhead is larger

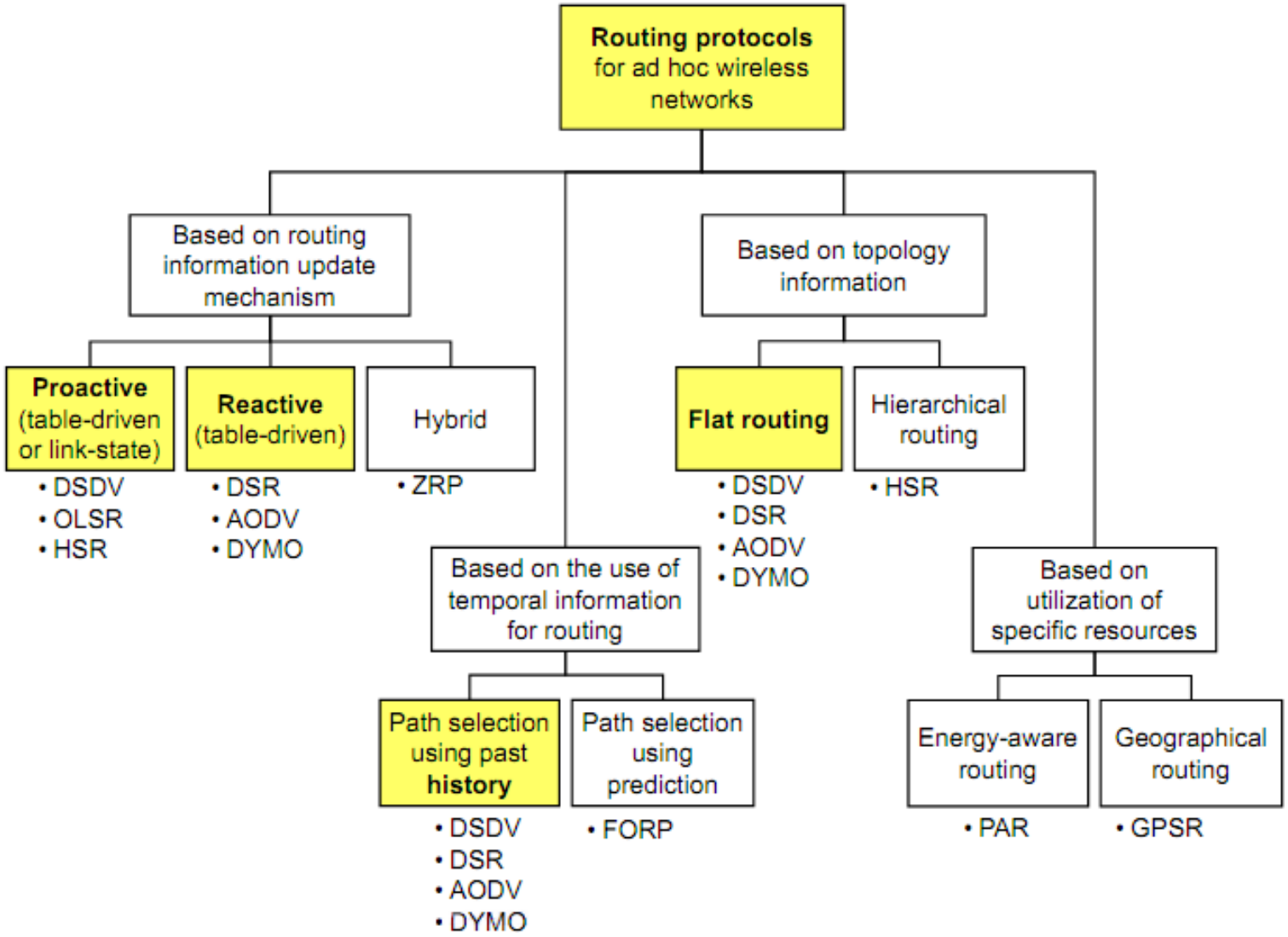
Address-based Ad-hoc Routing

Classification of Routing Protocols II.

- **flat** vs. **hierarchical** protocols:
  - *Flat protocols*
    - all nodes run identical algorithms (⇒ the protocols are relatively simple)
    - the routing overhead may increase very fast as the number of nodes increases
  - *Hierarchical protocols*
    - some nodes have added responsibilities (⇒ the algorithms are more complicated)
    - the performance scales better with network size
- **location-based** vs. **non-location-based** protocols:
  - *Location-based protocols*
    - make use of the nodes' physical location (⇒ reduce routing overhead)
    - nodes need to be equipped with GPS or something equivalent
  - *Non-location-based protocols*
    - oblivious to the physical location of nodes (⇒ simpler)
    - routing overhead is typically greater
- and many other classifications also exist

Address-based Ad-hoc Routing

Classification of Routing Protocols II.



Proactive Ad-hoc Routing

Proactive ad-hoc routing protocols:

- rely on a periodic collection and exchange of topology information
  - either *table-driven (distance-vector)* or *link-state* mechanisms for topology maintenance
    - *table-driven (distance-vector)* protocols periodically exchange routing tables between neighboring nodes
    - *link-state* distribute topology information (updates) so that each node can calculate optimal paths on their own

– high network overhead for state (topology) maintenance

\+ data packets can be forwarded at any time to any destination within the network

Proactive Ad-hoc Routing

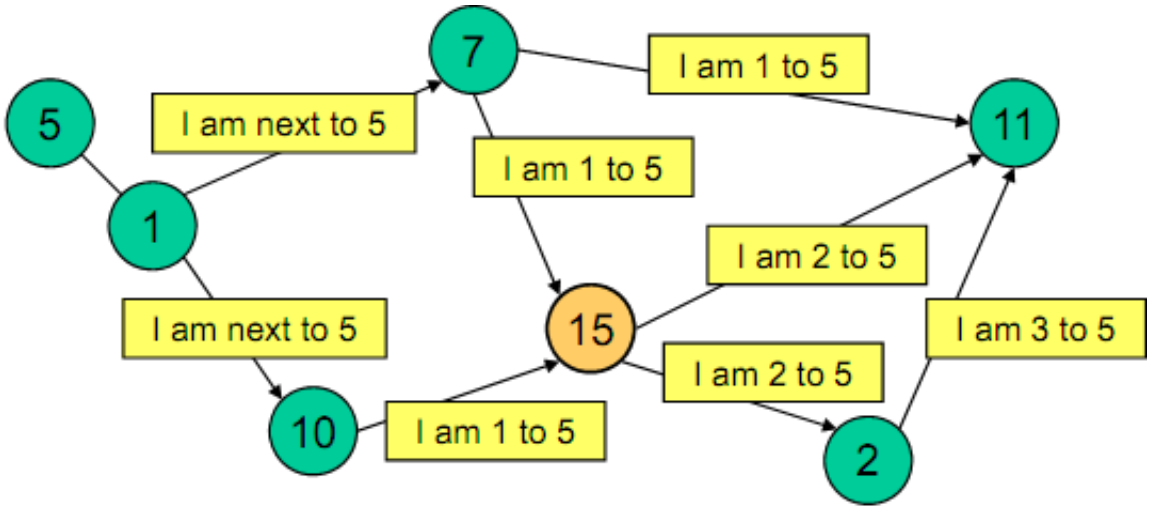
Destination Sequence Distance Vector (DSDV)

Destination Sequence Distance Vector (DSDV):

- a distance vector routing protocol inspired by RIP protocol
- based on distributed Bellman Ford procedure
  - nodes periodically exchange whole routing tables between neighbors
  - on topology change, incremental route updates are possible
- every node knows "where" everybody else is
  - $\Rightarrow$ routing table maintains $O(N)$ items
- aging information is used for maintaining fresh routes and avoiding loops
- simple, but does not scale (high overhead)

Dest	Next	Dist	Seq
7	7	1	12
1	7	2	26
5	7	3	26
...	...	...	...

Routing table at node 15



Proactive Ad-hoc Routing

Optimized Link State Routing (OLSR) Protocol

Optimized Link State Routing (OLSR) Protocol:

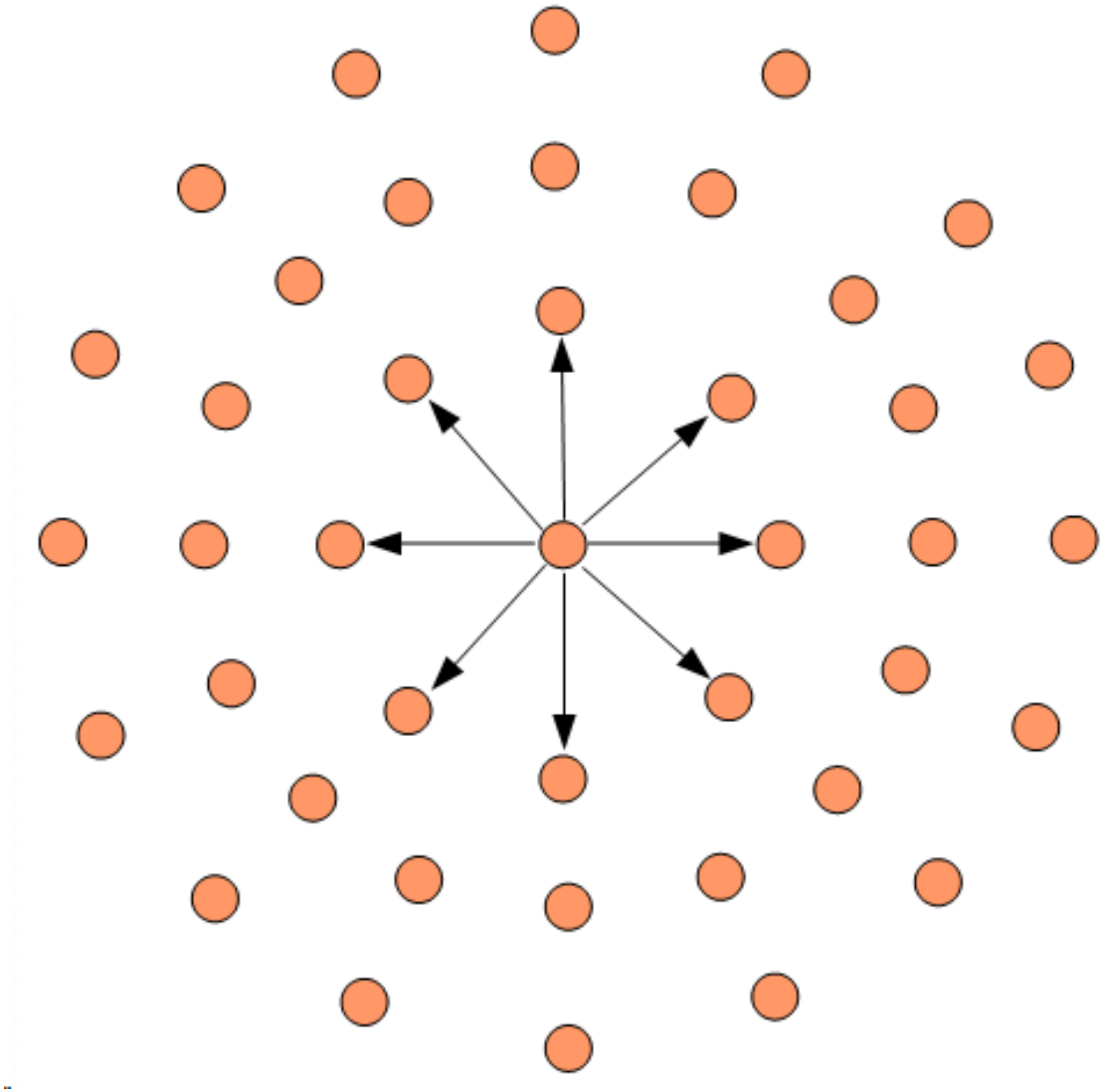
- link-state based routing protocol
  - links' state information is flooded through the network
  - $\Rightarrow$ nodes keep track of the whole topology and compute the shortest paths on their own
- broadcasts (topology information distribution) are optimized through *MultiPoint Relays (MPRS)*
  - instead of regular flooding, which introduces high overhead
  - each node selects and maintains its own MPR
    - the rule: *"For all 2-hop neighbors there must exist a MPR through which they can contact each other."*
  - MPRs further allow to *aggregate* link-state information

\+ suitable for large and dense networks

– lack of security, no support for multicast

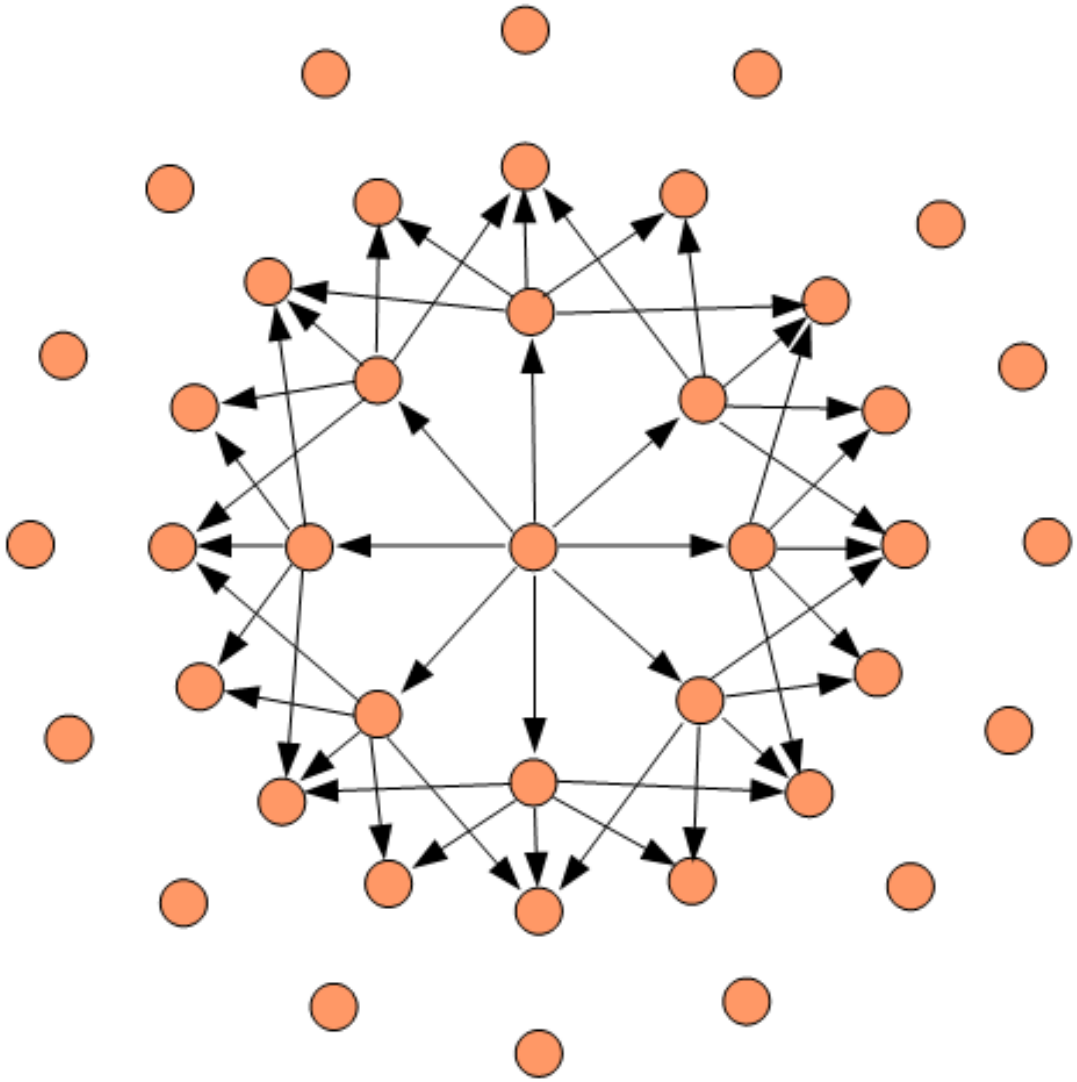
Proactive Ad-hoc Routing

Optimized Link State Routing (OLSR) Protocol – Regular Flooding



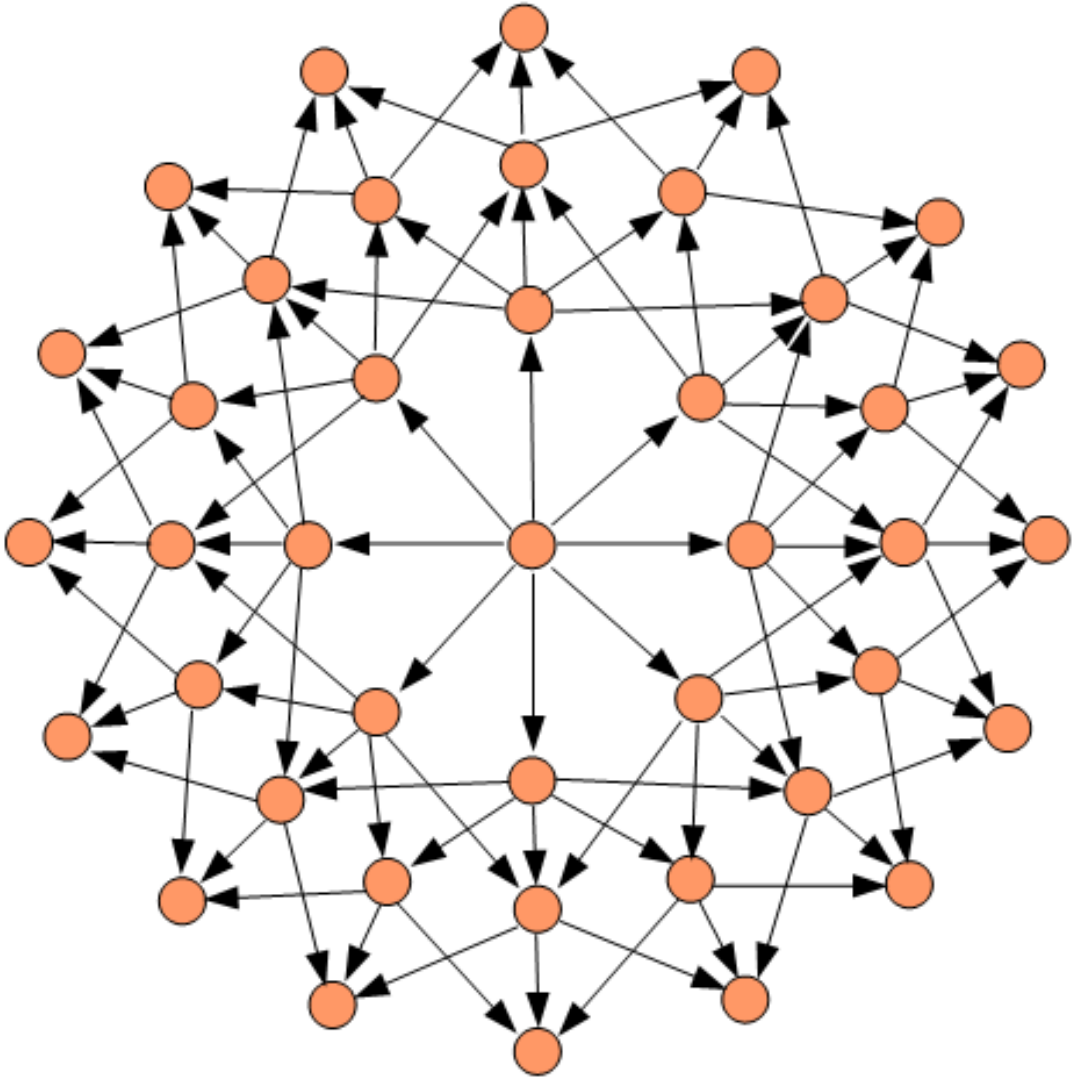
Proactive Ad-hoc Routing

Optimized Link State Routing (OLSR) Protocol – Regular Flooding



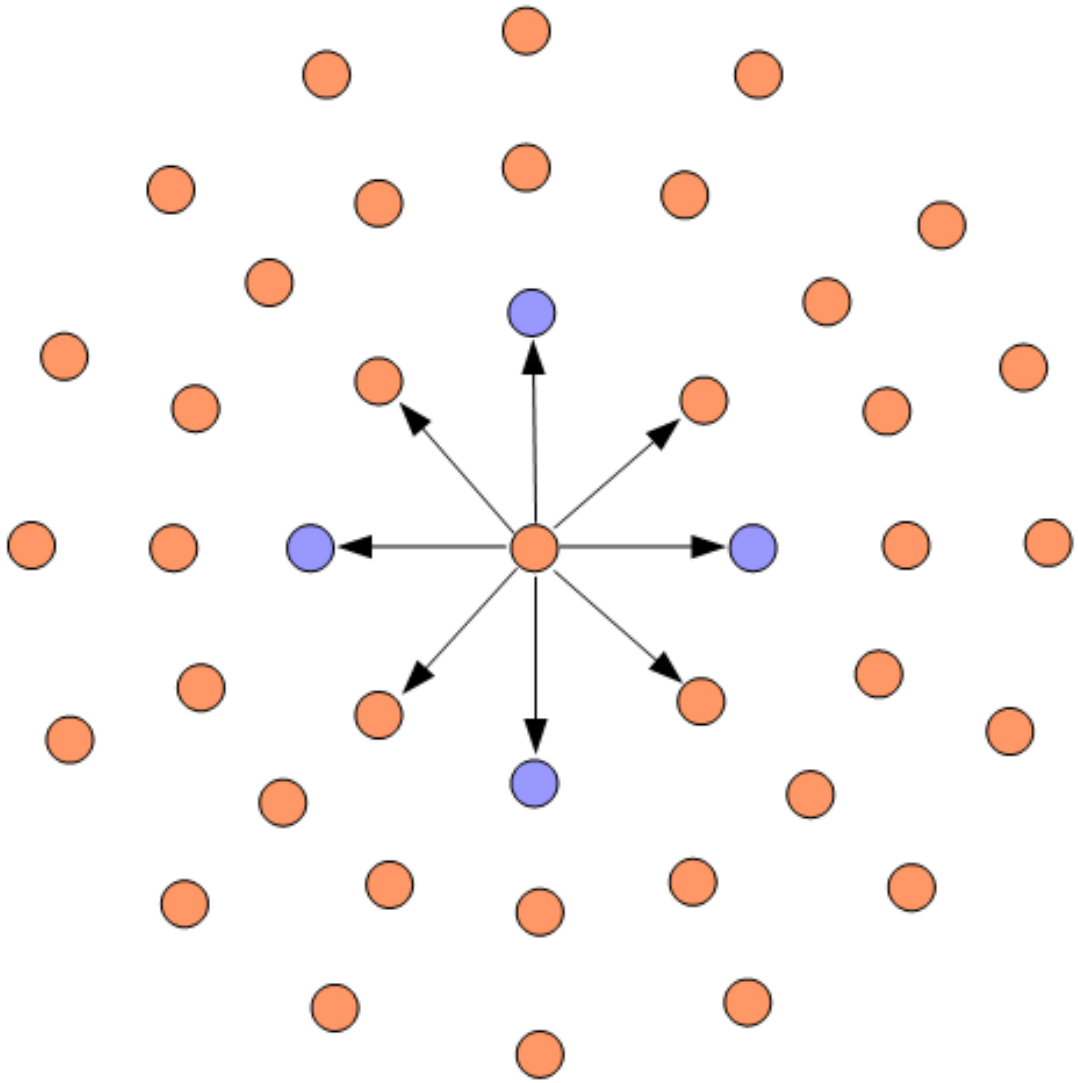
Proactive Ad-hoc Routing

Optimized Link State Routing (OLSR) Protocol – Regular Flooding



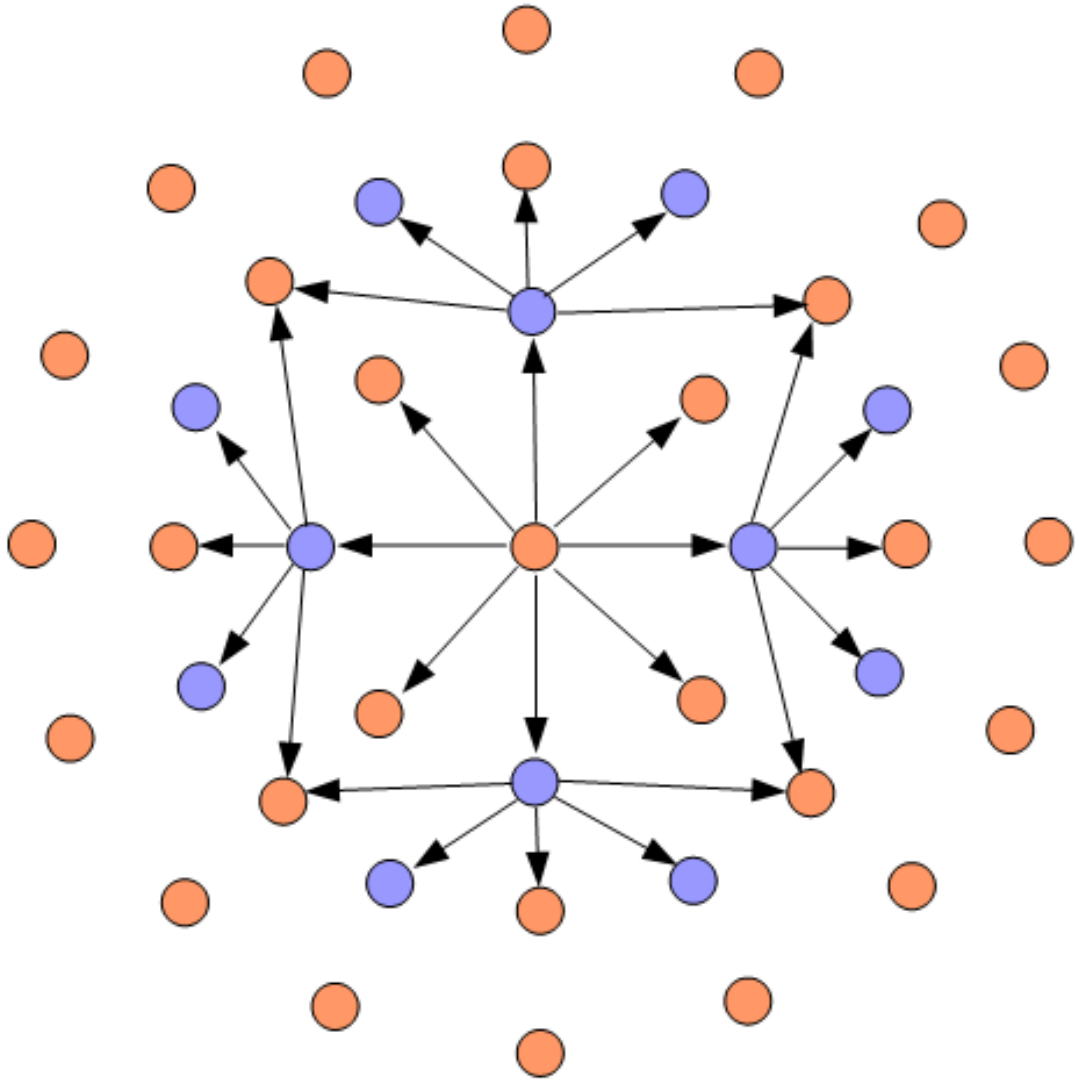
Proactive Ad-hoc Routing

Optimized Link State Routing (OLSR) Protocol – MPR Flooding



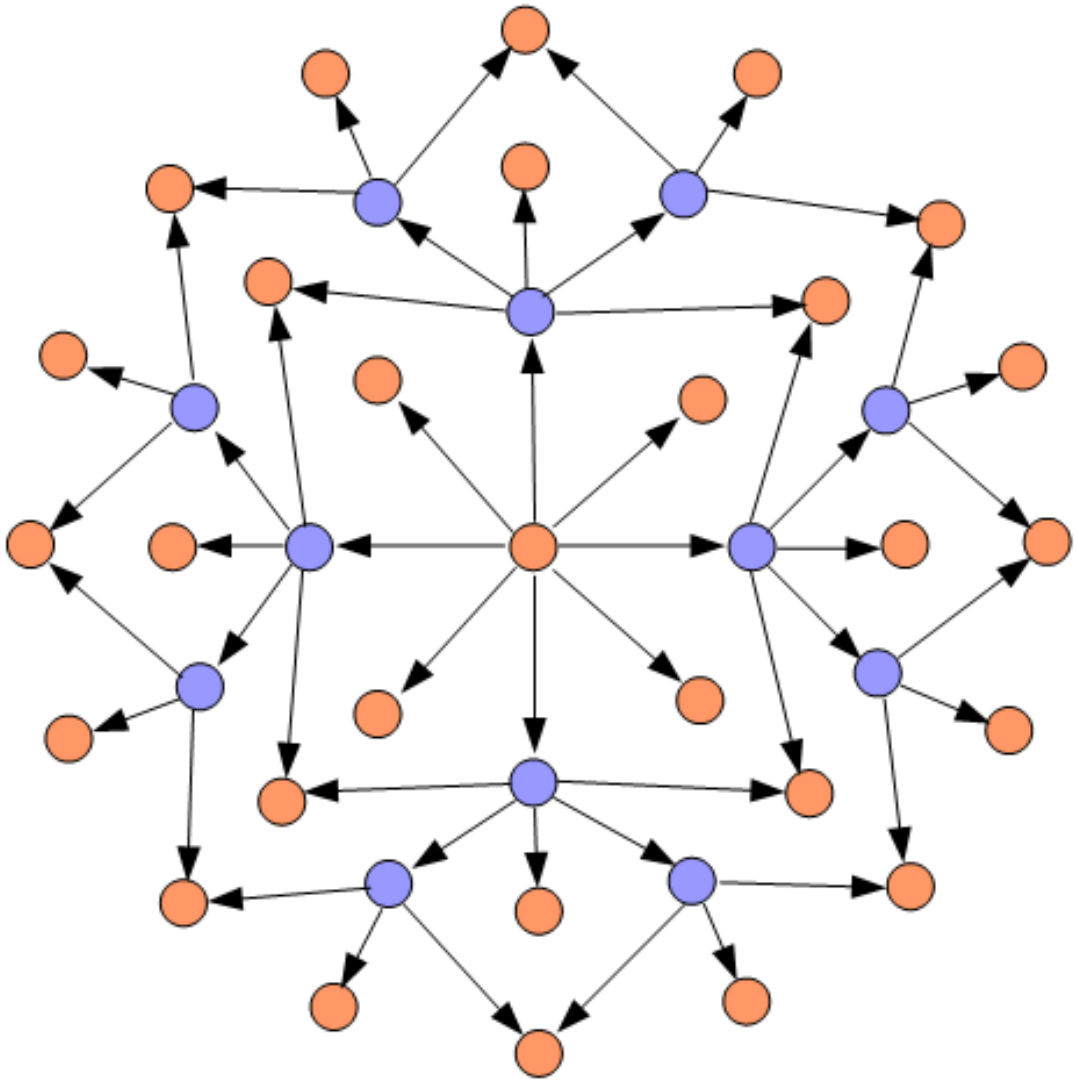
Proactive Ad-hoc Routing

Optimized Link State Routing (OLSR) Protocol – MPR Flooding



Proactive Ad-hoc Routing

Optimized Link State Routing (OLSR) Protocol – MPR Flooding



Reactive (On-Demand) Ad-hoc Routing

- routes are discovered only when needed (when data packets need to be transmitted)
  - \+ saves energy and bandwidth during inactivity
  - – additional delay is introduced for the setup of routing information
- \+ requires no (or very small) routing tables
- – introduces high network overhead in the *flooding process* when querying for routes
- – performance degrades with increasing mobility

Reactive (On-Demand) Ad-hoc Routing

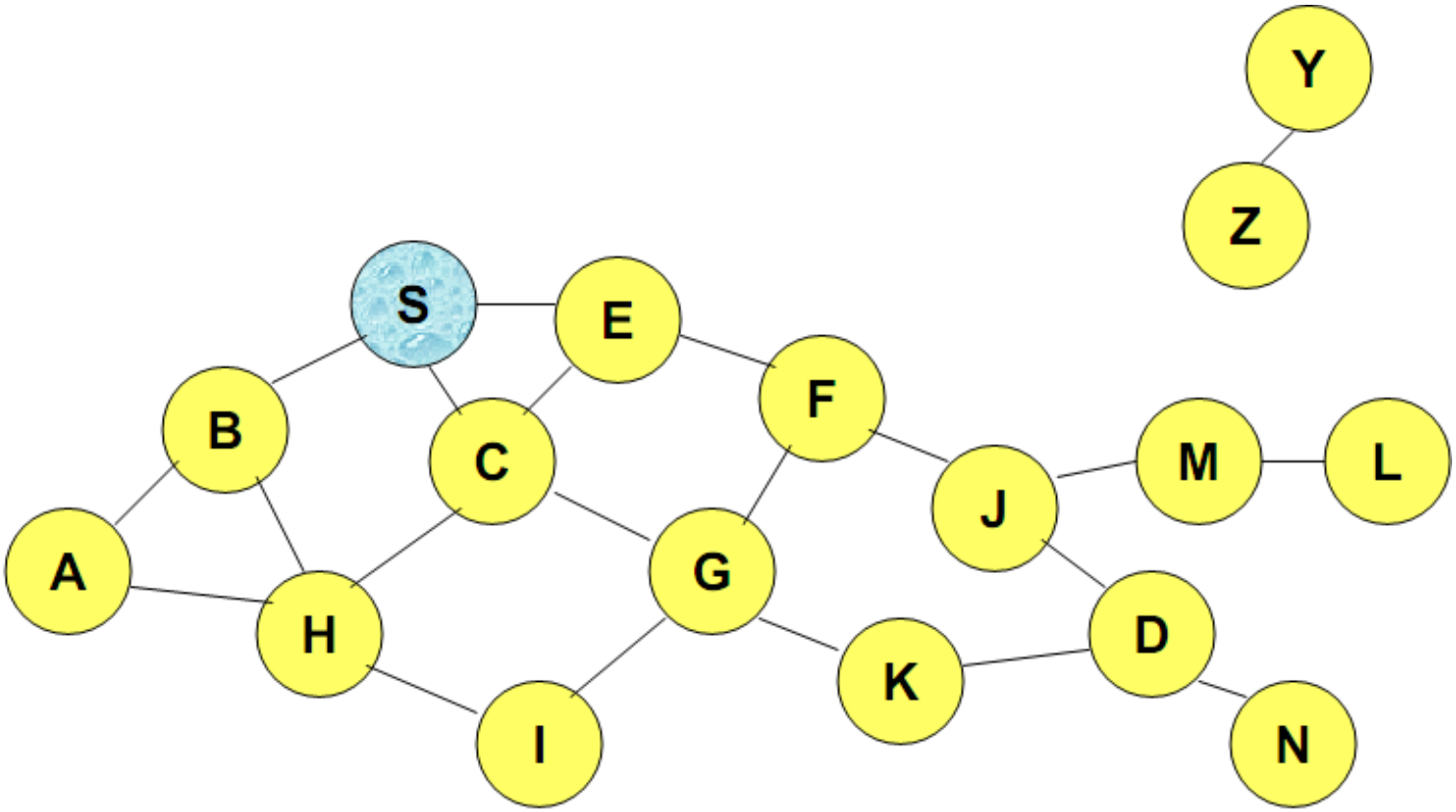
Dynamic Source Routing (DSR)

Dynamic Source Routing (DSR)

- source-based routing protocol
- uses separate *Route Request (RREQ)* and *Route Reply (RREP)* packets to discover a route from the source node to the destination
  - sender floods RREQ through the network
  - nodes forward RREQs after appending their identification
  - destination node receives RREQ and unicasts a RREP back to the sender node
- the routing information is stored in the discovery packets
  - there is no need to maintain globally valid routing tables and state information in each node
- data packets are sent once a route has been established
- behaves well for smaller, less saturated wireless networks
- *optimization:* route caching by observing RREQs and RREPs of other nodes

Reactive (On-Demand) Ad-hoc Routing

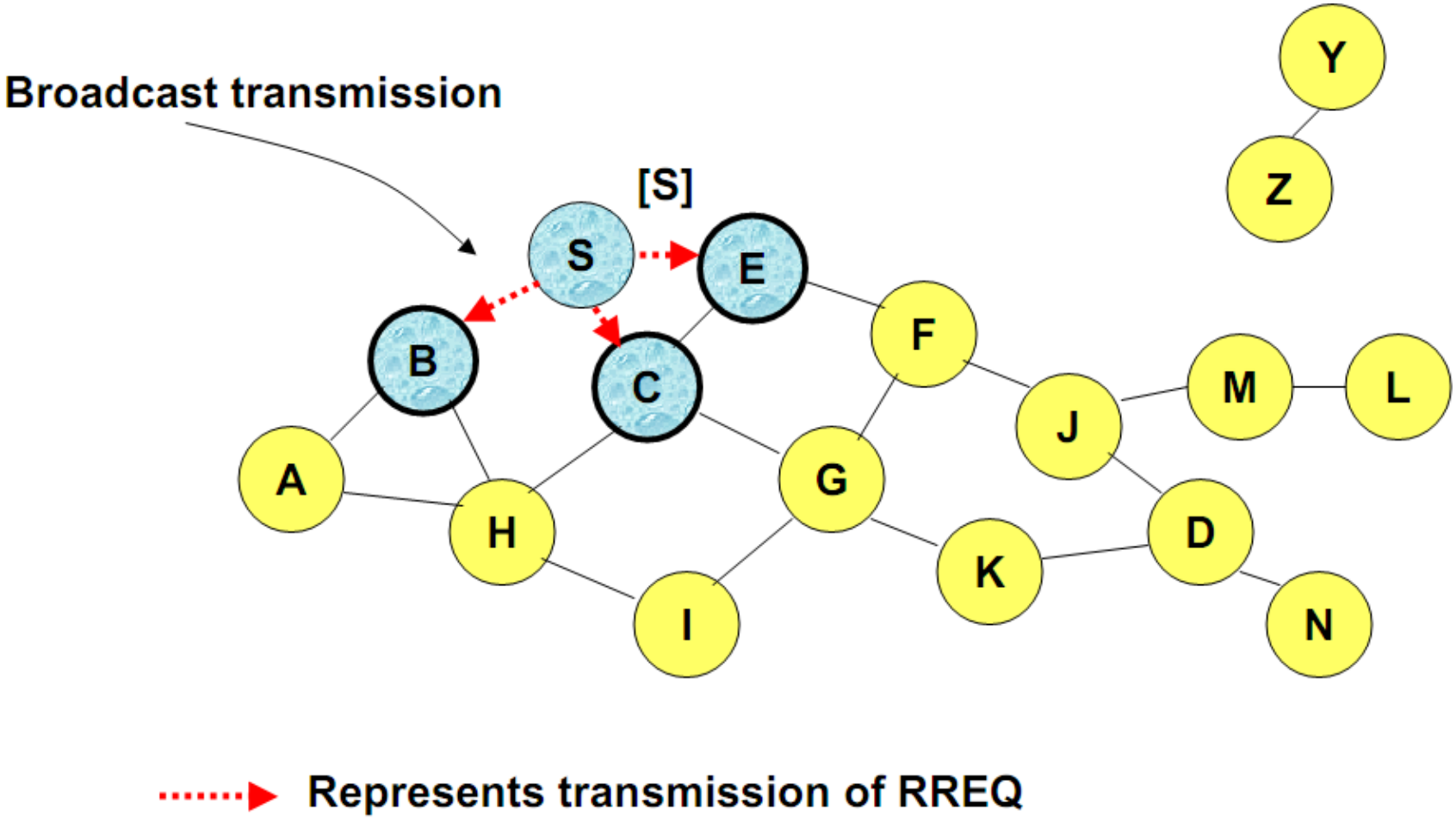
Dynamic Source Routing (DSR) – Route Discovery I.



Represents a node that has received RREQ for D from S

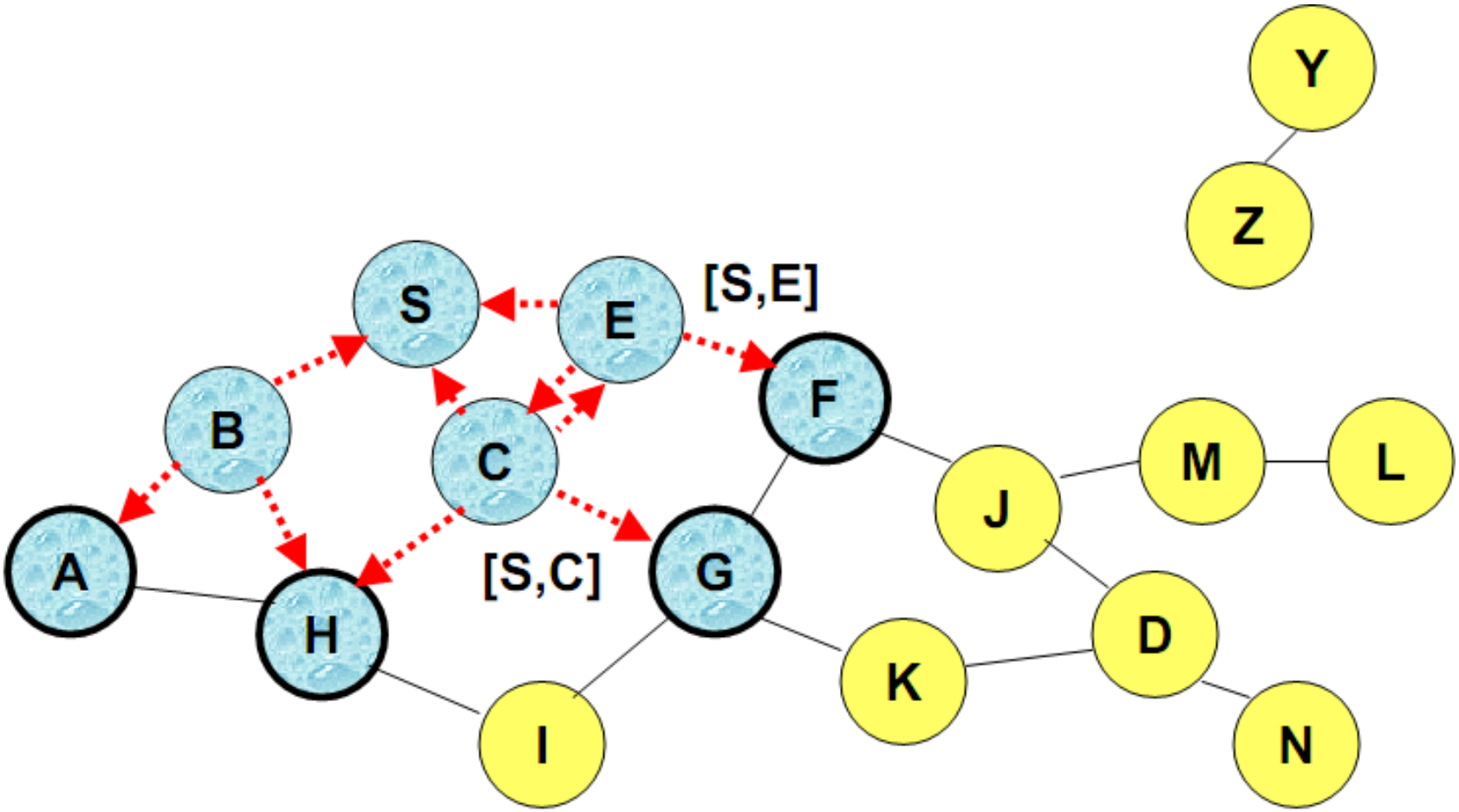
Reactive (On-Demand) Ad-hoc Routing

Dynamic Source Routing (DSR) – Route Discovery II.



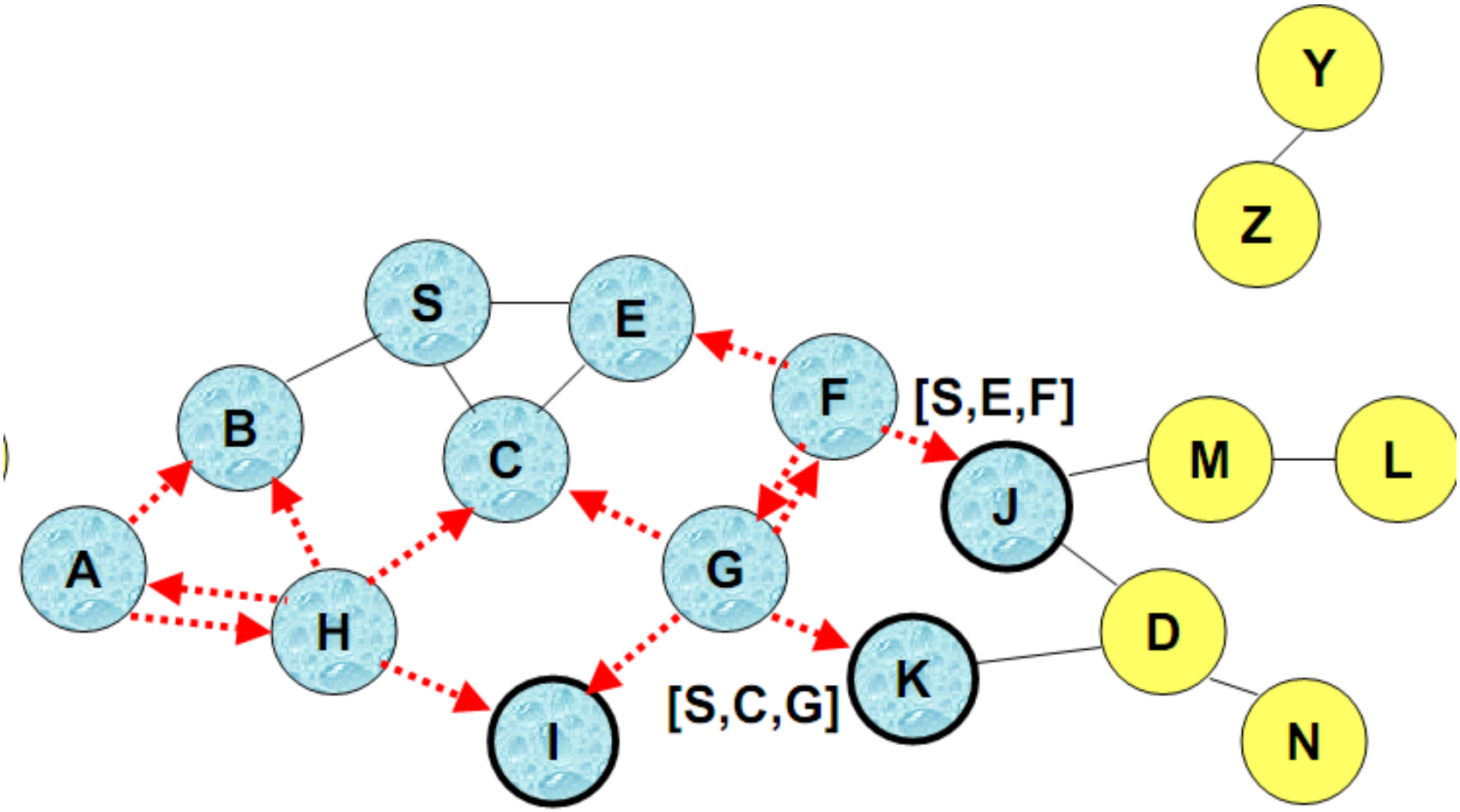
Reactive (On-Demand) Ad-hoc Routing

Dynamic Source Routing (DSR) – Route Discovery III.



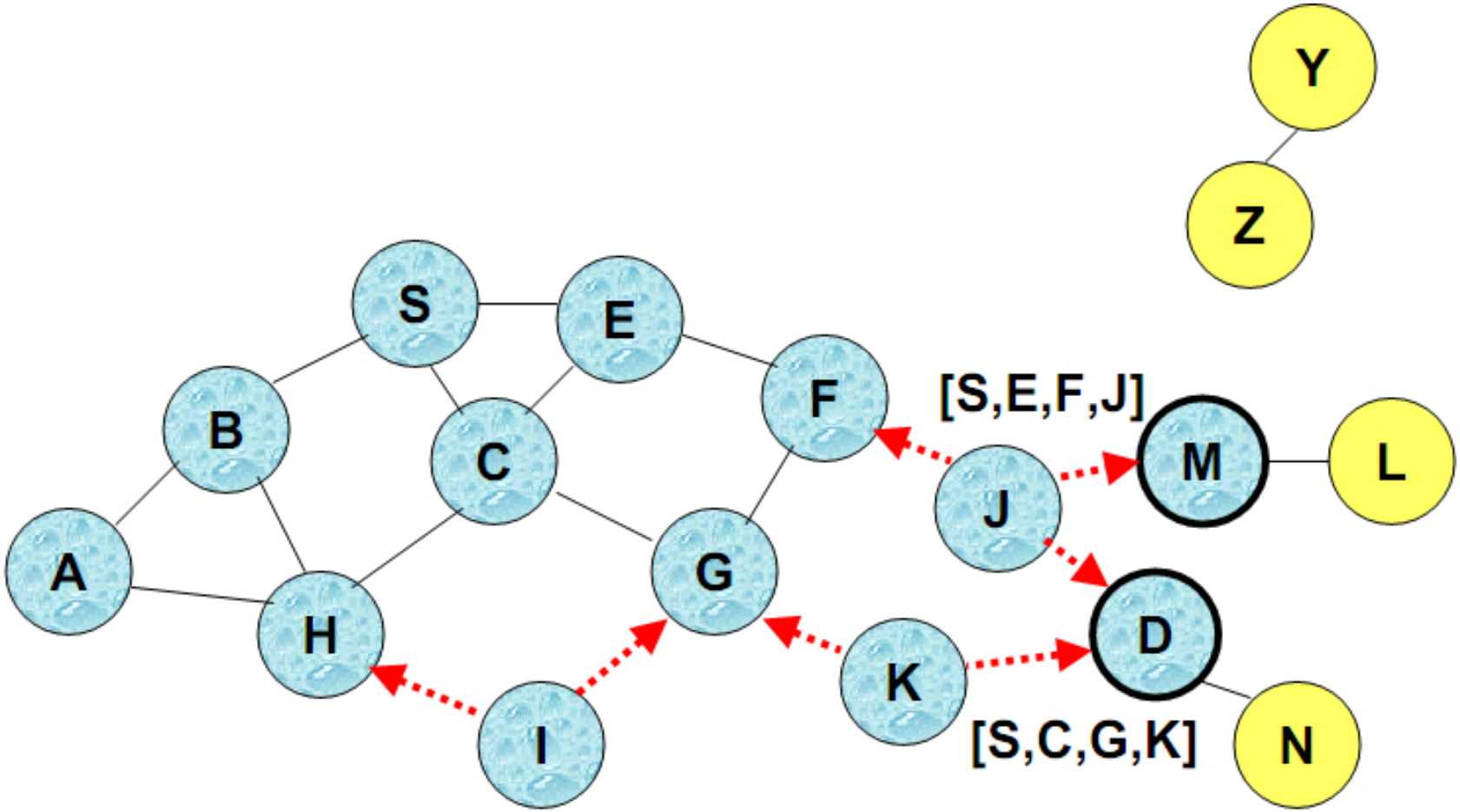
Reactive (On-Demand) Ad-hoc Routing

Dynamic Source Routing (DSR) – Route Discovery IV.



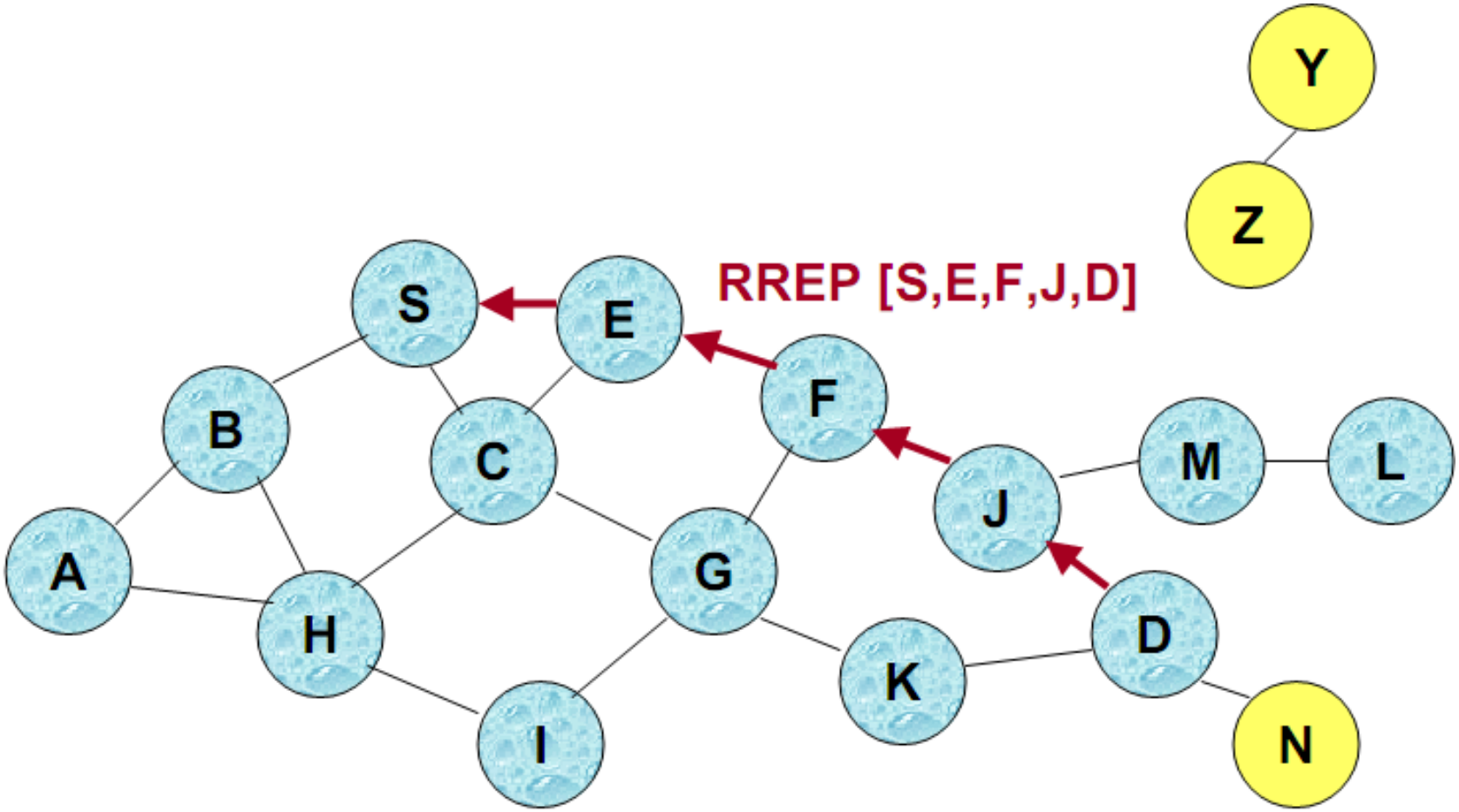
Reactive (On-Demand) Ad-hoc Routing

Dynamic Source Routing (DSR) – Route Discovery V.



Reactive (On-Demand) Ad-hoc Routing

Dynamic Source Routing (DSR) – Route Reply



Reactive (On-Demand) Ad-hoc Routing

Ad Hoc on Demand Distance Vector (AODV)

Ad Hoc on Demand Distance Vector (AODV)

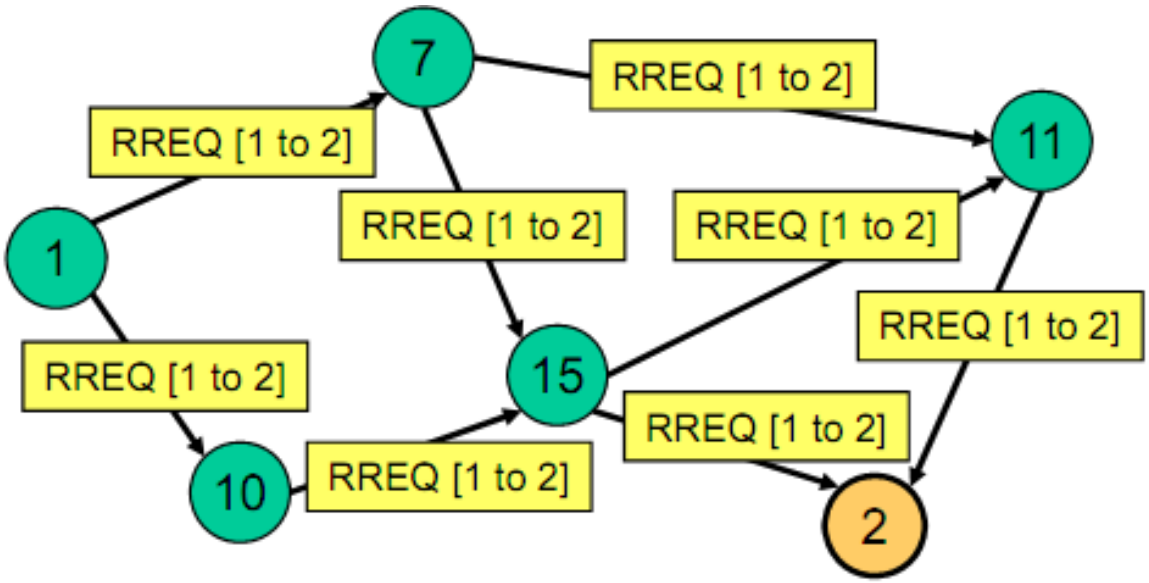
- another reactive routing protocol, searching paths between the source and the destination on demand
- basically, the same route discovery procedure is used as in DSR
  - however, it copes with the per-packet overhead introduced by DSR
    - (source-routing – the whole route has to be stored in each packet)
  - in AODV, all nodes remember from where a packet came and populate their routing tables with that information
    - i.e., intermediate nodes in a given path maintain routing tables instead of using source routing
    - when an intermediate node knows a route to destination from previous communication, it may answer to RREQ instead of the destination node

\+ lower connection setup delay (compared to DSR)

Reactive (On-Demand) Ad-hoc Routing

Ad Hoc on Demand Distance Vector (AODV) – Route Setup

RREQs are flooded through the entire network (limited by a TTL describing the maximum network diameter)



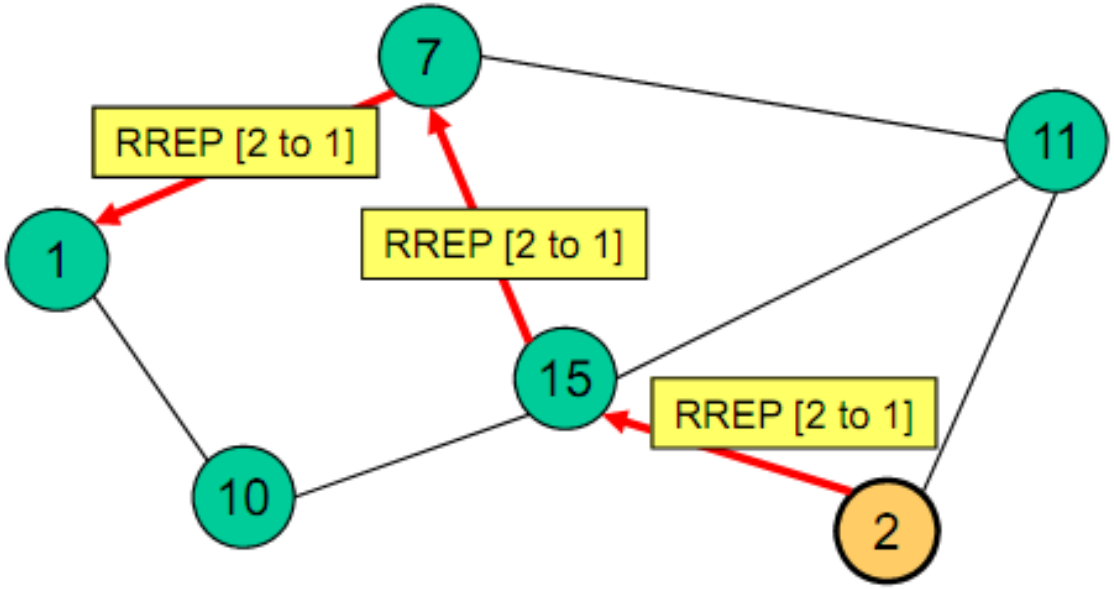
Node	Dest	Next	Dist
7	1	1	1
11	1	7	2
15	1	7	2
...	...	...	...
2	1	15	3

Routing tables after flooding the RREQ [1 to 2]

Reactive (On-Demand) Ad-hoc Routing

Ad Hoc on Demand Distance Vector (AODV) – Route Reply

The RouteReply (RREP) is unicasted towards the source



Node	Dest	Next	Dist
7	1	1	1
7	2	15	2
11	1	7	2
15	1	7	2
15	2	2	1
…	…	…	…
2	1	15	3

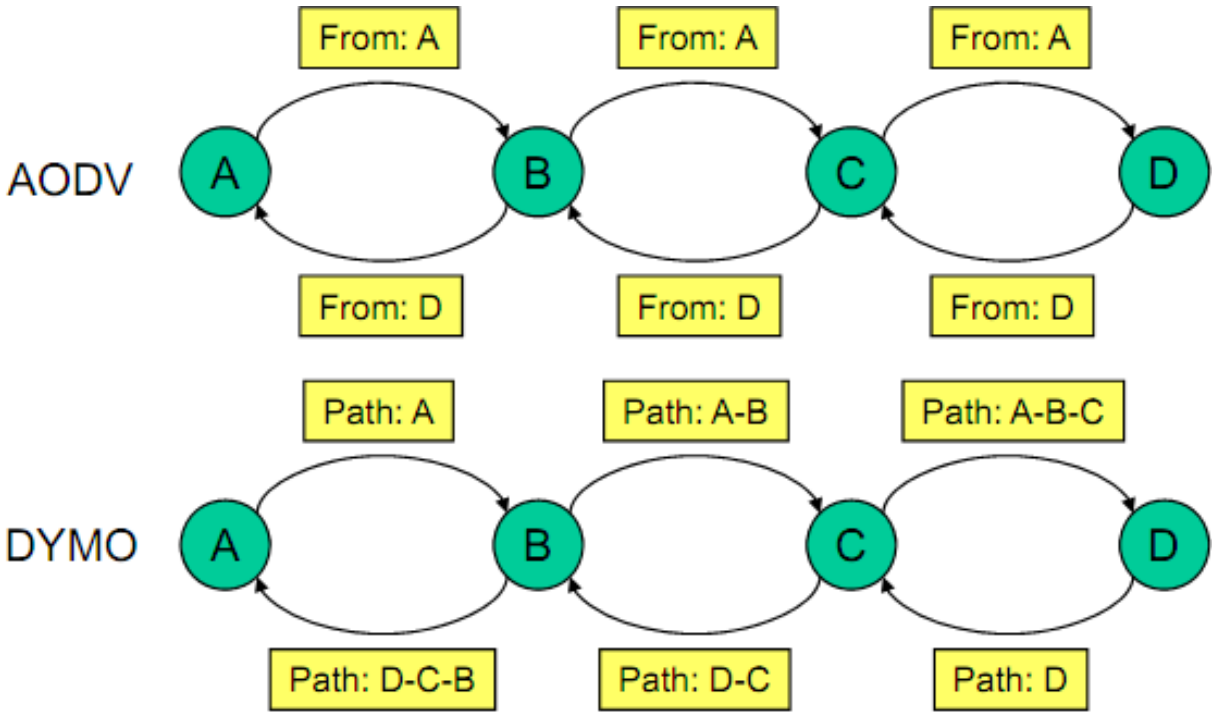
Routing tables after sending the RREP [2 to 1]

Reactive (On-Demand) Ad-hoc Routing

Dynamic MANET On Demand (DYMO)

Dynamic MANET On Demand (DYMO)

- successor of AODV
- reduces the overhead in route setup and route maintenance



Specialized Routing Protocols

Geographic Routing

- instead of maintaining routing tables (to know nodes' positions), infer this information from physical placement of nodes
  - nodes know their geo coordinates (GPS, location service mapping node ID to node position, etc.)
  - send a message to a neighbor in the right direction as next hop
- e.g., DREAM, GPSR, LAR

Energy-Aware Routing Protocols

- take the nodes' energy capacity into account
- several metrics can be employed:
  - minimize the energy consumption per packet (selecting paths with minimum transmission energy)
  - minimize the variance in node power levels (preffering nodes with higher energy level)
  - etc.

Lecture Overview

Conclusions

- (mobile) ad-hoc networks appear to be a good solution not only for temporary networks
  - but for fixed installations as well (buildings, cities, etc.)
  - provide many useful features as compared to infrastructure-based wireless networks
- alive and well-researched area
- still many challenges & research objectives:
  - *network lifetime*
  - *robustness & fault-tolerance*
  - *in-network processing*
  - *quality of service*
  - *software management* (i.e., nodes' reprogramming)
  - etc.

Information Sources

FI Courses:

- PA151: Advanced Computer Networks (doc. Staudek)
- PV169: Communication Systems Basics (doc. Staudek)

Literature:

- Falko Dressler: *Self-Organization in Sensor and Actor Networks.* John Wiley & Sons, 2007.
- Jon S. Wilson: *Sensor technology handbook.* Newnes, 2005.
- Ananthram Swami: *Wireless sensor networks: signal processing and communications perspectives.* John Wiley & Sons, 2007.
- Holger Karl, Andreas Willig: *Protocols and Architectures for Wireless Sensor Networks.* Wiley-Interscience, 2007.
- Amiya Nayak, Ivan Stojmenović: *Wireless Sensor and Actuator Networks: Algorithms and Protocols for Scalable Coordination and Data Communication.* Wiley-Interscience, 2009.
- ...