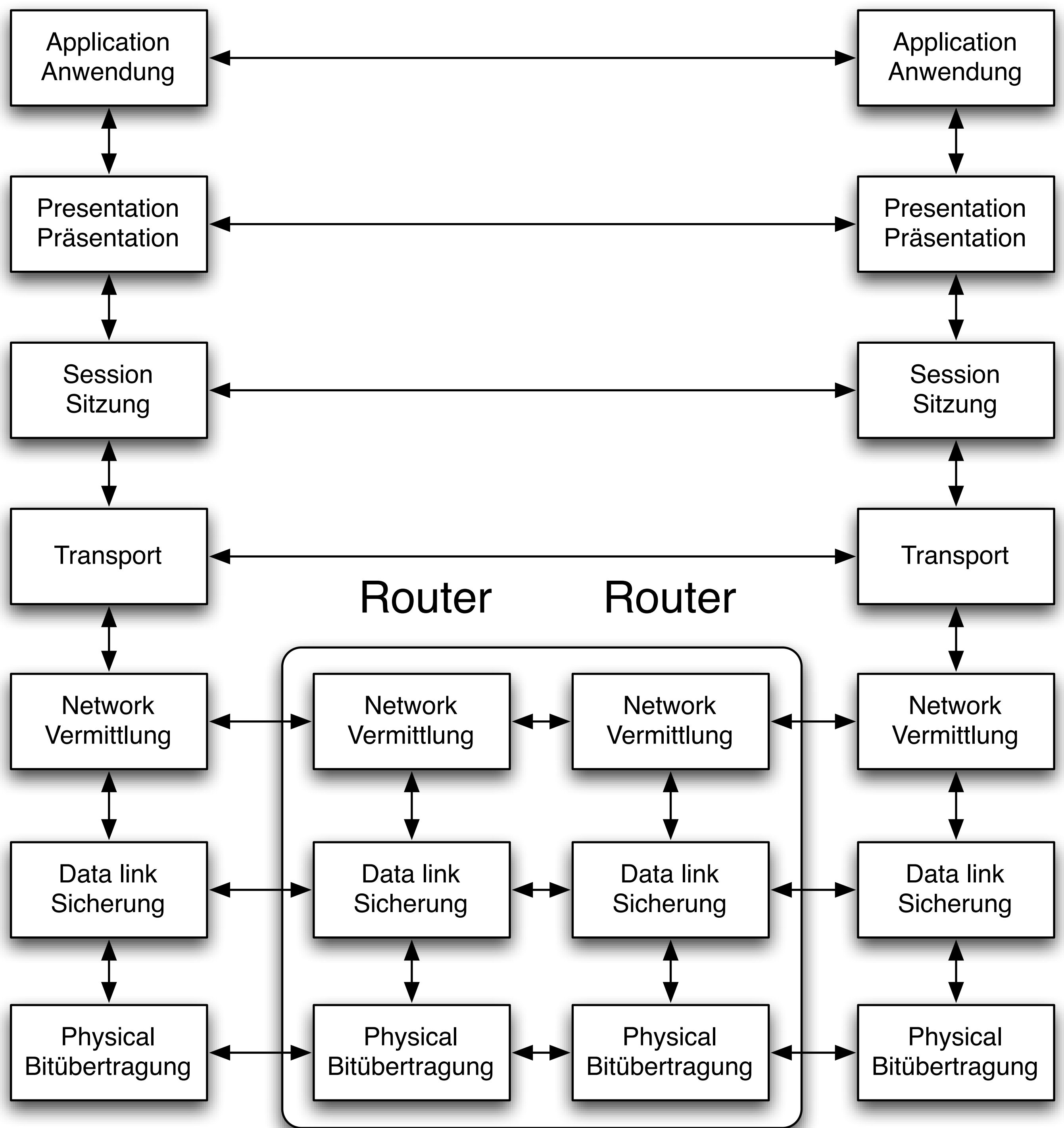
Wireless Sensor Networks
5. Routing

Christian Schindelhauer
Technische Fakultät
Rechnernetze und Telematik
Albert-Ludwigs-Universität Freiburg
Version 30.05.2016

ISO/OSI Reference model

- 7. Application
  - Data transmission, e-mail, terminal, remote login
- 6. Presentation
  - System-dependent presentation of the data (EBCDIC / ASCII)
- 5. Session
  - start, end, restart
- 4. Transport
  - Segmentation, congestion
- 3. Network
  - Routing
- 2. Data Link
  - Checksums, flow control
- 1. Physical
  - Mechanics, electrics



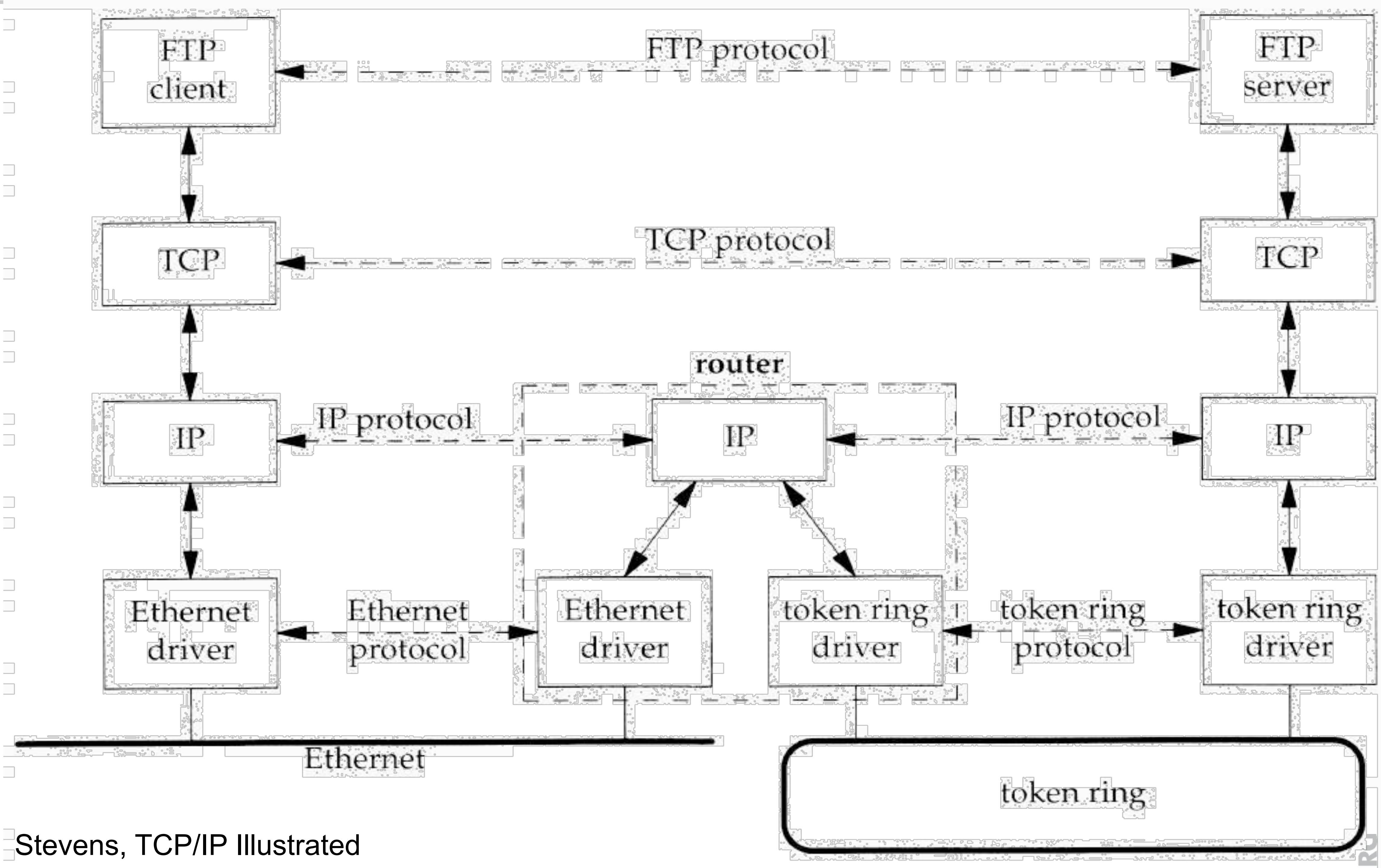
Protocols of the Internet

Application	Telnet, FTP, HTTP, SMTP (E-Mail), ...
Transport	TCP (Transmission Control Protocol) UDP (User Datagram Protocol)
Network	IP **(Internet Protocol)** + ICMP **(Internet Control Message Protocol)** + IGMP **(Internet Group Management Protocol)**
Host-to-Network	LAN **(e.g. Ethernet, Token Ring etc.)**

TCP/IP Layers

- 1. Host-to-Network
  - Not specified, depends on the local network,k e.g. Ethernet, WLAN 802.11, PPP, DSL
- 2. Routing Layer/Network Layer
  (IP - Internet Protocol)
  - Defined packet format and protocol
  - Routing
  - Forwarding
- 3. Transport Layer
  - TCP (Transmission Control Protocol)
    - Reliable, connection-oriented transmission
    - Fragmentation, Flow Control, Multiplexing
  - UDP (User Datagram Protocol)
    - hands packets over to IP
    - unreliable, no flow control
- 4. Application Layer
  - Services such as TELNET, FTP, SMTP, HTTP, NNTP (for DNS), ...

Example: Routing between LANs



Stevens, TCP/IP Illustrated

Routing Tables and Packet Forwarding

- IP Routing Table
  - contains for each destination the address of the next gateway
  - destination: host computer or sub-network
  - default gateway
- Packet Forwarding
  - IP packet (datagram) contains start IP address and destination IP address
    - if destination = my address then hand over to higher layer
    - if destination in routing table then forward packet to corresponding gateway
    - if destination IP subnet in routing table then forward packet to corresponding gateway
    - otherwise, use the default gateway

IP Packet Forwarding

- IP -Packet (datagram) contains...
  - TTL (Time-to-Live): Hop count limit
  - Start IP Address
  - Destination IP Address
- Packet Handling
  - Reduce TTL (Time to Live) by 1
  - If TTL ≠ 0 then forward packet according to routing table
  - If TTL = 0 or forwarding error (buffer full etc.):
    - delete packet
    - if packet is not an ICMP Packet then
      - send ICMP Packet with
      - start = current IP Address
      - destination = original start IP Address

Static and Dynamic Routing

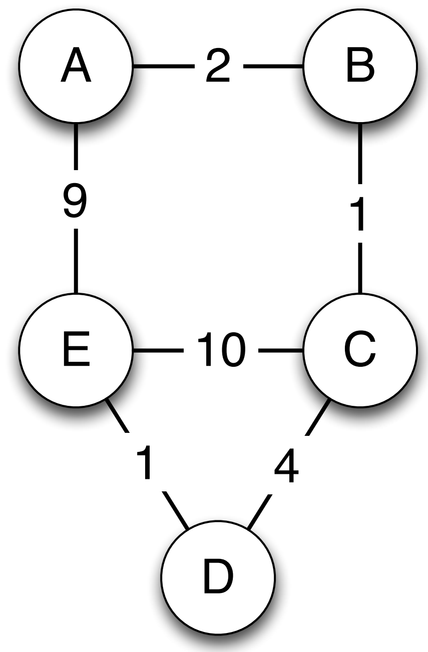
- Static Routing
  - Routing table created manually
  - used in small LANs
- Dynamic Routing
  - Routing table created by Routing Algorithm
  - Centralized, e.g. Link State
    - Router knows the complete network topology
  - Decentralized, e.g. Distance Vector
    - Router knows gateways in its local neighborhood

Intra-AS Routing

- Routing Information Protocol (RIP)
  - Distance Vector Algorithmus
  - Metric = hop count
  - exchange of distance vectors (by UDP)
- Interior Gateway Routing Protocol (IGRP)
  - successor of RIP
  - different routing metrics (delay, bandwidth)
- Open Shortest Path First (OSPF)
  - Link State Routing (every router knows the topology)
  - Route calculation by Dijkstra’s shortest path algorithm

Distance Vector Routing Protocol

- Distance Table data structure
  - Each node has a
    - Line for each possible destination
    - Column for any direct neighbors
- Distributed algorithm
  - each node communicates only with its neighbors
- Asynchronous operation
  - Nodes do not need to exchange information in each round
- Self-terminating
  - exchange unless no update is available



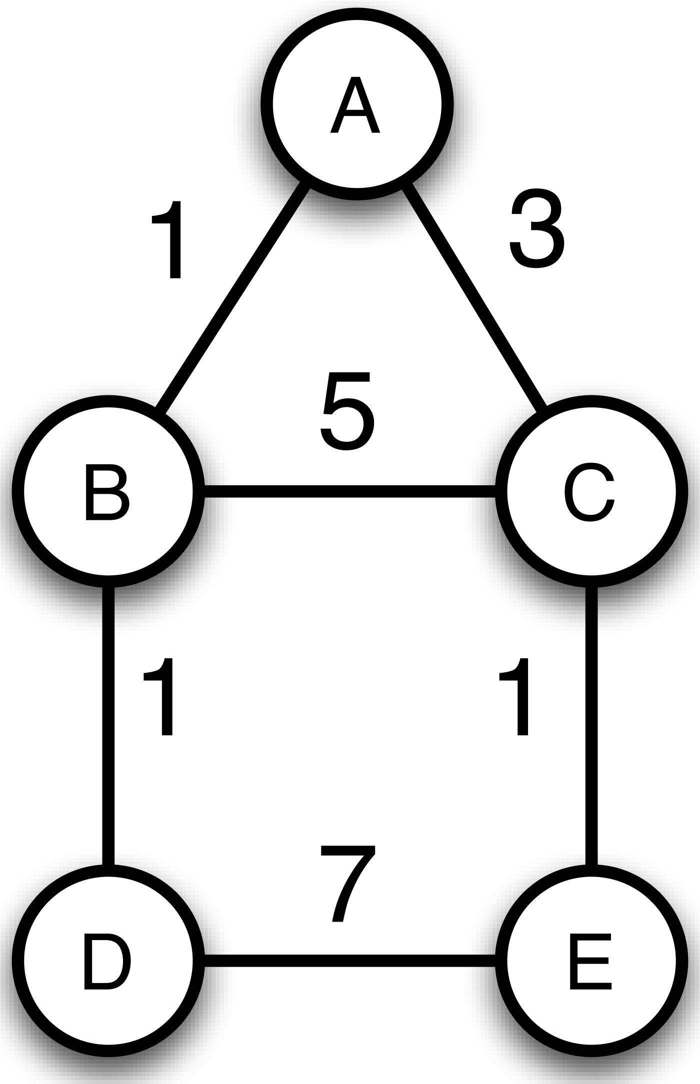
Distance Table for A

		via		Routing Table
from A		B	E	entry
to	B	**2**	15	B
	C	**3**	14	B
	D	**7**	10	B
	E	**8**	9	E

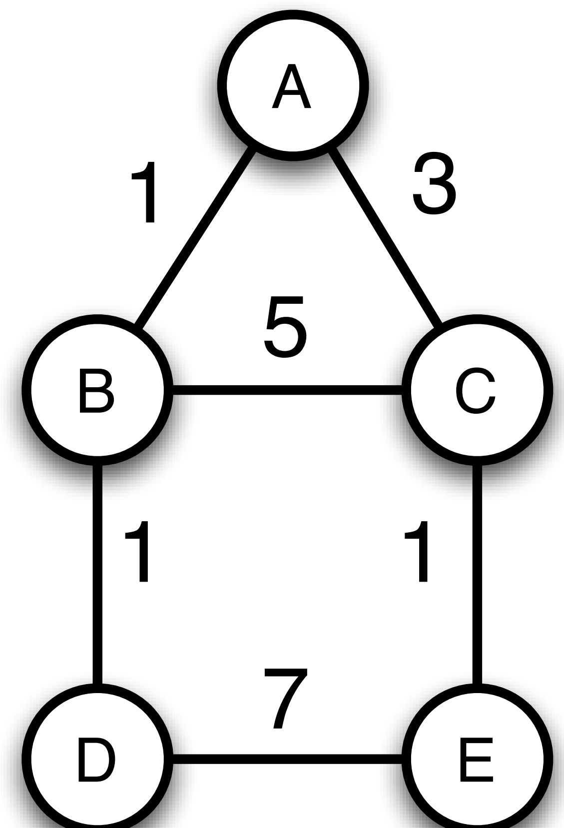
Distance Table for C

			via		Routing Table
from C		B	D	E	entry
to	A	**3**	11	18	B
	B	**1**	9	21	B
	D	6	**4**	11	D
	E	7	**5**	10	D

Distance Vector Routing Example



from A to	via B	via C	entry
B	**1**	8	**B**
C	6	**3**	**C**
D	**2**	9	**B**
E	7	**4**	**C**



from A to	via		entry
	B	C	
B	1	-	B
C	-	3	C
D	-	-	-
E	-	-	-

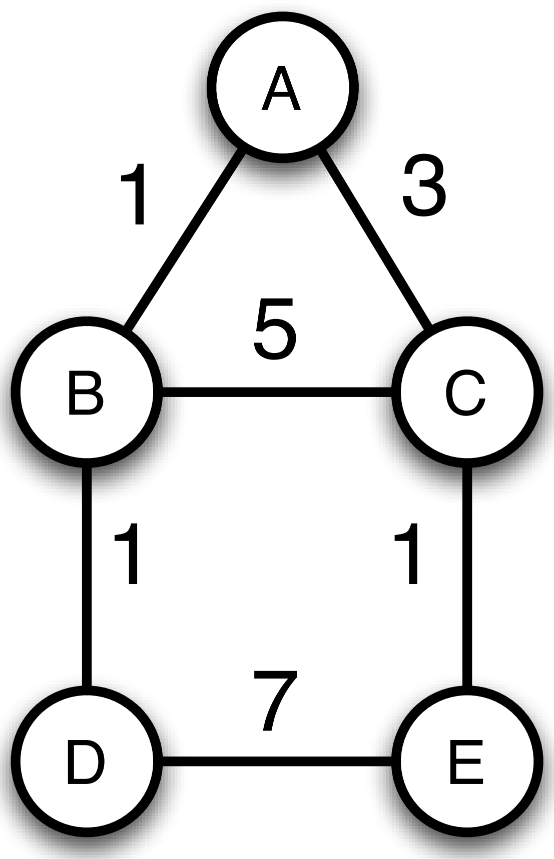
from B to	via			entry
	A	C	D	
A	1	-	-	A
C	-	3	-	C
D	-	-	1	C
E	-	-	8	D

from C to	via			entry
	A	B	E	
A	3	-	-	A
B	-	5	-	B
D	-	-	8	E
E	-	-	1	E

from B to	via			Entry
	A	C	D	
A	1	-	-	A
C	-	5	-	C
D	-	-	1	D
E	-	-	8	D

from C to	via			Entry
	A	B	E	
A	3	-	-	A
B	-	5	-	B
D	-	-	8	E
E	-	-	1	E

from B to	via			Entry
	A	C	D	
A	1	8	-	A
C	-	5	-	C
D	-	13	1	D
E	-	6	8	C

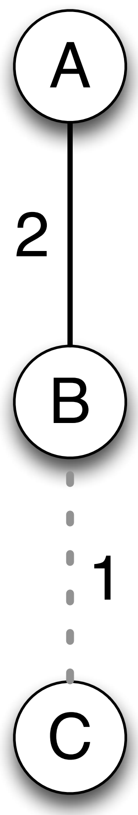


from C to	via			Entry
	A	B	E	
A	3	6	-	A
B	-	5	-	B
D	-	6	8	B
E	-	13	1	E

“Count to Infinity” - Problem

- Good news travels fast
  - A new connection is quickly at hand
- Bad news travels slowly
  - Connection fails
  - Neighbors increase their distance mutally
  - "Count to Infinity" Problem

"Count to Infinity" - Problem



from A		via B	Routing Table entry
to	B	2	B
	C	3	B

from B		via A	via C	Routing Table entry
to	A	2	-	A
	C	5	-	A

↓

from A		via B	Routing Table entry
to	B	2	B
	C	7	B

from B		via A	via C	Routing Table entry
to	A	2	-	A
	C	5	-	A

↓

from A		via B	Routing Table entry
to	B	2	B
	C	7	B

from B		via A	via C	Routing Table entry
to	A	2	-	A
	C	9	-	A

Link-State Protocol

- Link state routers
  - exchange information using Link State Packets (LSP)
  - each node uses shortest path algorithm to compute the routing table
- LSP contains
  - ID of the node generating the packet
  - Cost of this node to any direct neighbors
  - Sequence-no. (SEQNO)
  - TTL field for that field (time to live)
- Reliable flooding (Reliable Flooding)
  - current LSP of each node are stored
  - Forward of LSP to all neighbors
    - except to be node where it has been received from
  - Periodically creation of new LSPs
    - with increasing SEQNO
  - Decrement TTL when LSPs are forwarded

Characteristics of routing in mobile ad hoc networks

- Movement of participants
  - Reconnecting and loss of connection is more common than in other wireless networks
  - Especially at high speed
- Other performance criteria
  - Route stability in the face of mobility
  - energy consumption

Unicast Routing

- Variety of protocols
  - Adaptations and new developments
- No protocol dominates the other in all situations
  - Solution: Adaptive protocols?

Routing in MANETs

- Routing
  - Determination of message paths
  - Transport of data
- Protocol types
  - proactive
    - Routing tables with updates
  - reactive
    - repairm of message paths only when necessary
  - hybrid
    - combination of proactive and reactive

Routing Protocols for MANETs

CoNe Freiburg

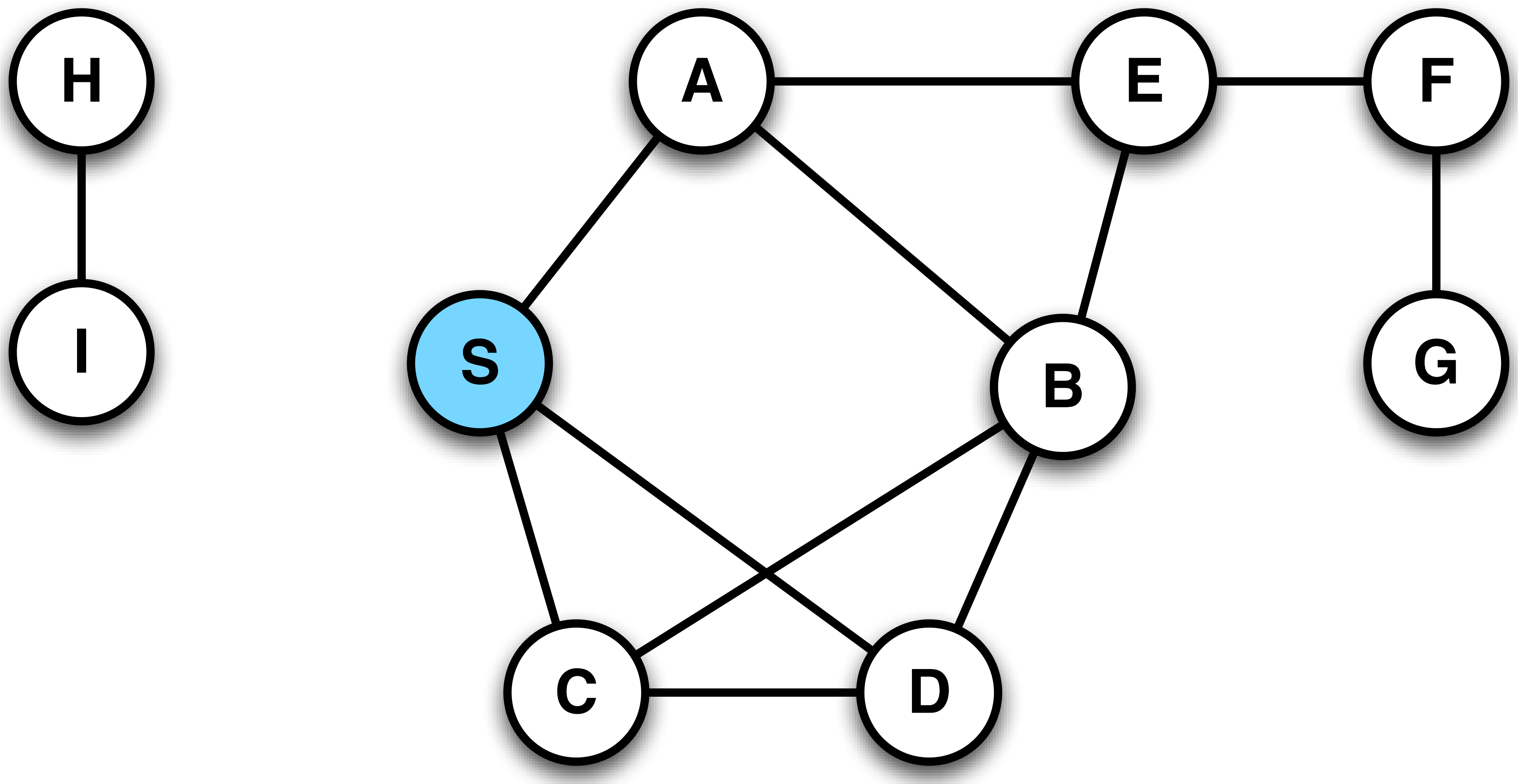
- **Proactive**
  - Routes are **demand independent**
  - Standard Link-State und Distance-Vector Protocols
    - Destination Sequenced Distance Vector (**DSDV**)
    - Optimized Link State Routing (**OLSR**)
- **Reactive**
  - Route are determined when needed
    - Dynamic Source Routing (**DSR**)
    - Ad hoc On-demand Distance Vector (**AODV**)
    - Dynamic MANET On-demand Routing Protocol
    - Temporally Ordered Routing Algorithm (**TORA**)
- **Hybrid**
  - combination of reactive und proactive
    - Zone Routing Protocol (**ZRP**)
    - Greedy Perimeter Stateless Routing (**GPSR**)

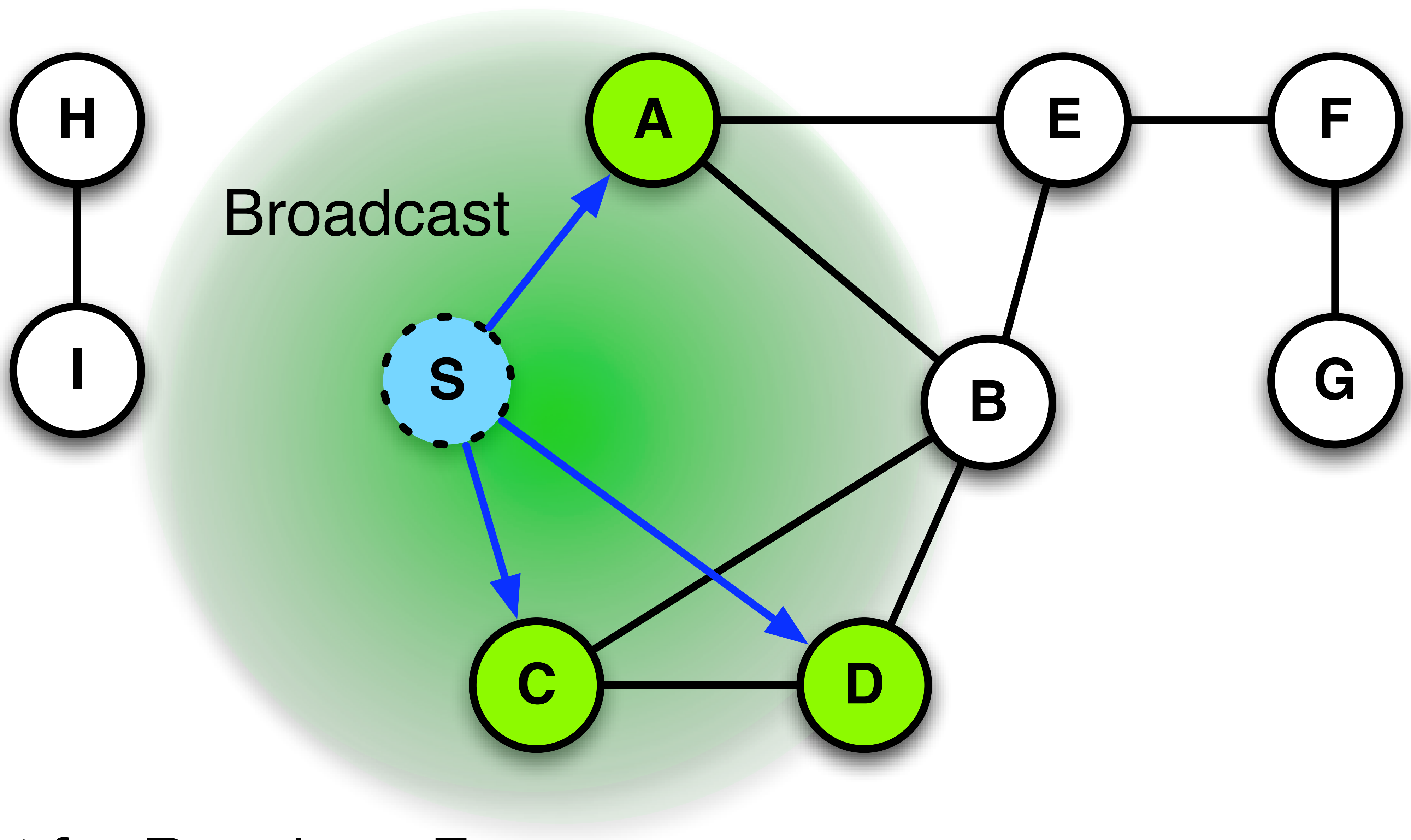
Trade-Off

- Latency because of route discovery
  - Proactive protocols are faster
  - Reactive protocols need to find routes
- Overhead of Route discovery and maintenance
  - Reactive protocols have smaller overhead (number of messages)
  - Proactive protocols may have larger complexity
- Traffic-Pattern and mobility
  - decides which type of protocol is more efficient

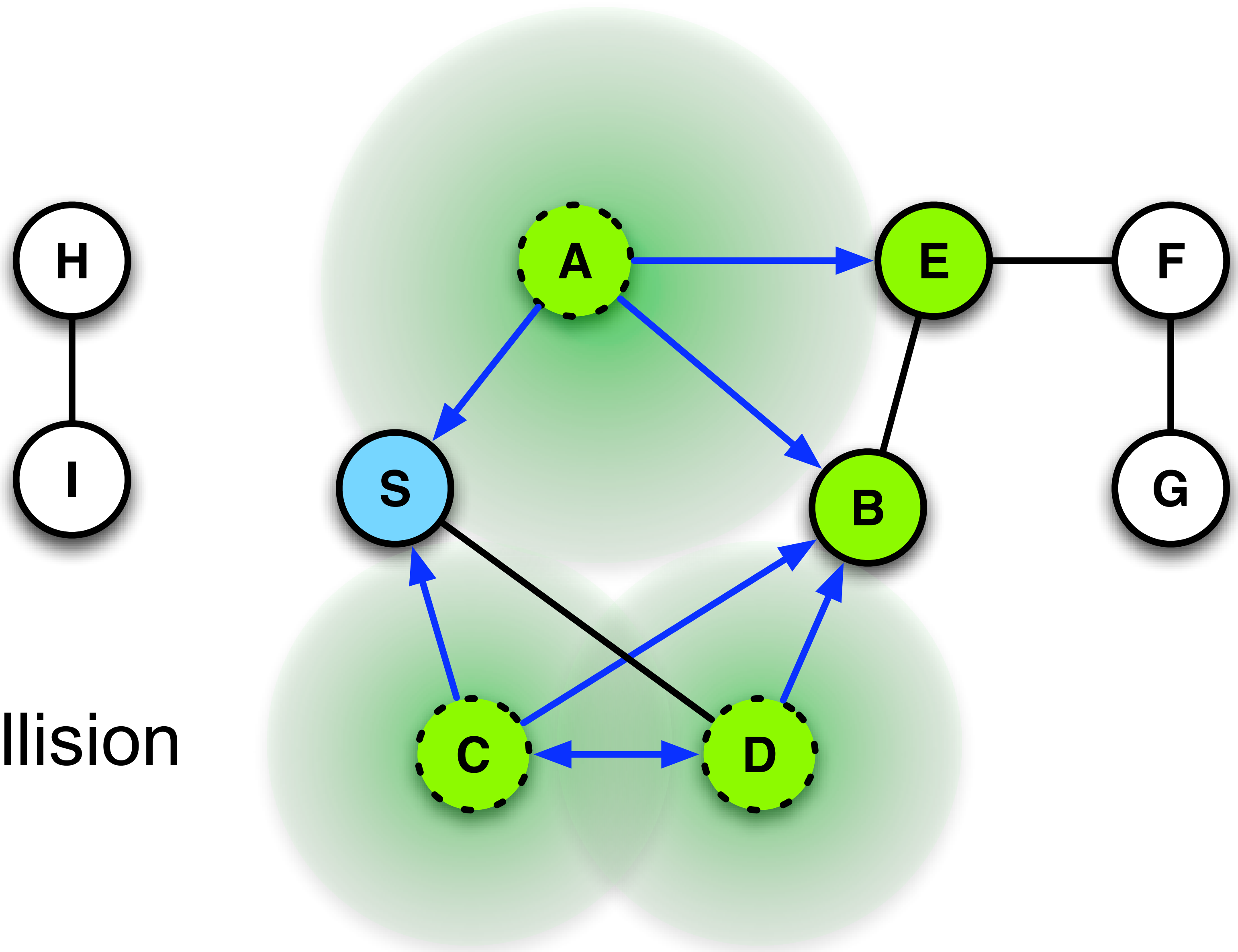
Flooding

- Algorithm
  - Sender S broadcasts data packet to all neighbors
  - Each node receiving a new packet
    - broadcasts this packet
    - if it is not the receiver
- Sequence numbers
  - identifies messages to prevent duplicates
- Packet always reaches the target
  - if possible


H
I
A
E
F
S
B
G
C
D

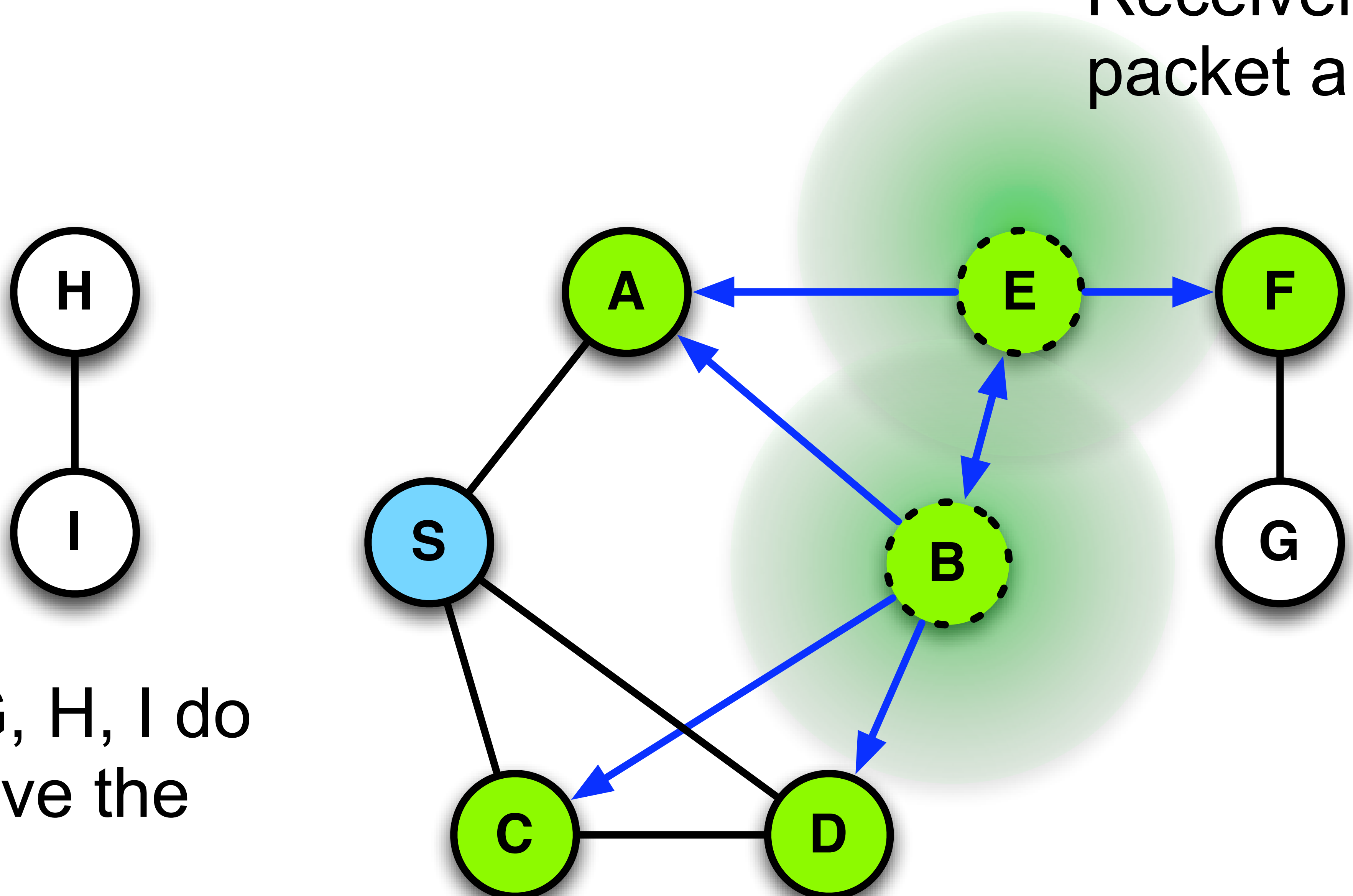


Packet for Receiver F



Possible collision
at B

Receiver F gets packet and stops



Nodes G, H, I do not receive the packet

Flooding

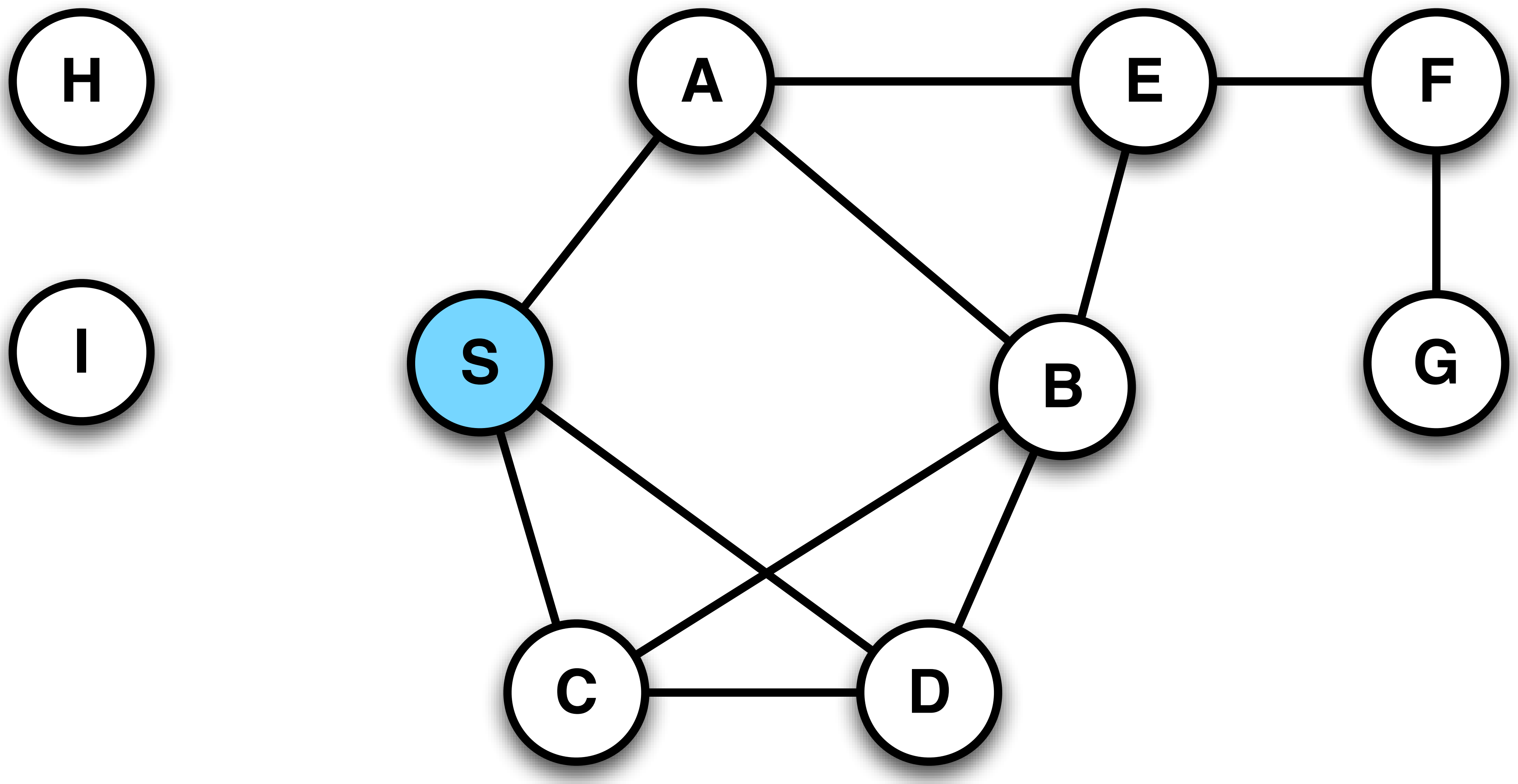
- Advantage
  - simple and robust
  - the best approach for short packet lengths, small number of participants in highly mobile networks with light traffic
- Disadvantage
  - High overhead
  - Broadcasting is unreliable
    - lack of acknowledgements
    - hidden, exposed terminals lead to data loss or delay

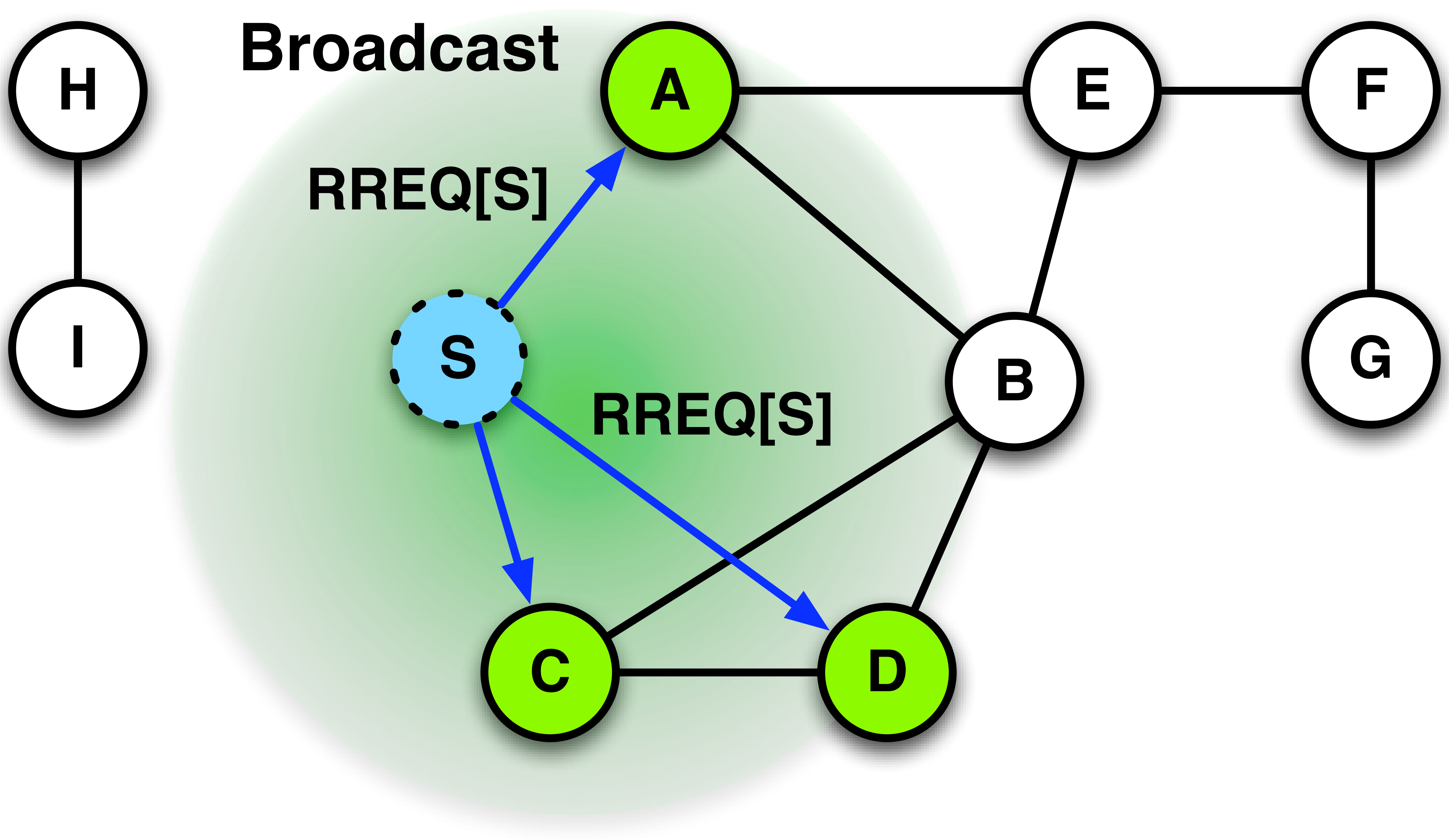
Flooding

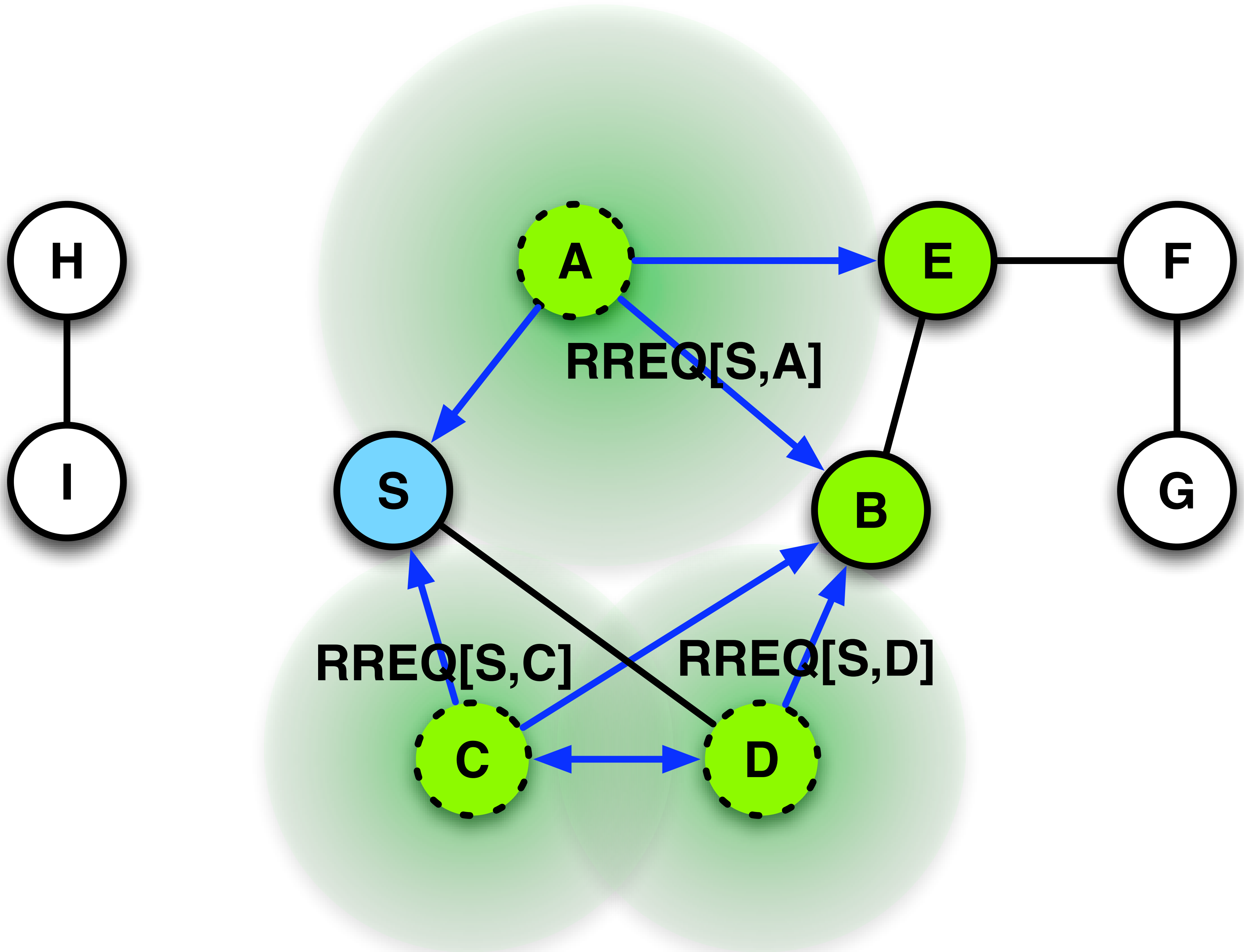
- Produces too many unnecessary (long) data packets
  - in the worst case, each participant sends each packet
  - many long transmissions collisions lead to long waiting times in the medium access
- Better approach:
  - Use of control packets for route determination
  - Flooding of control packet leads to DSR

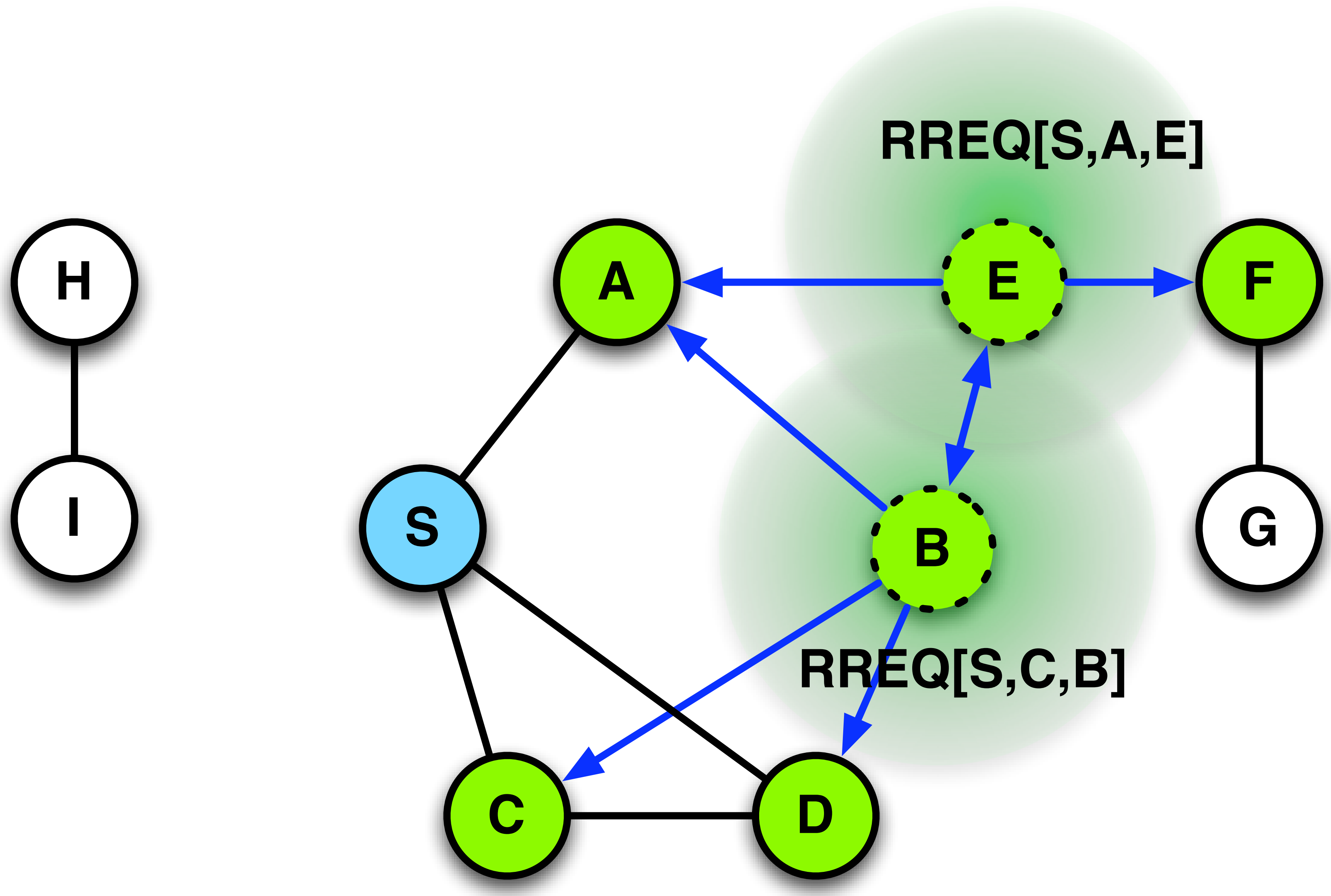
Dynamic Source Routing (DSR)

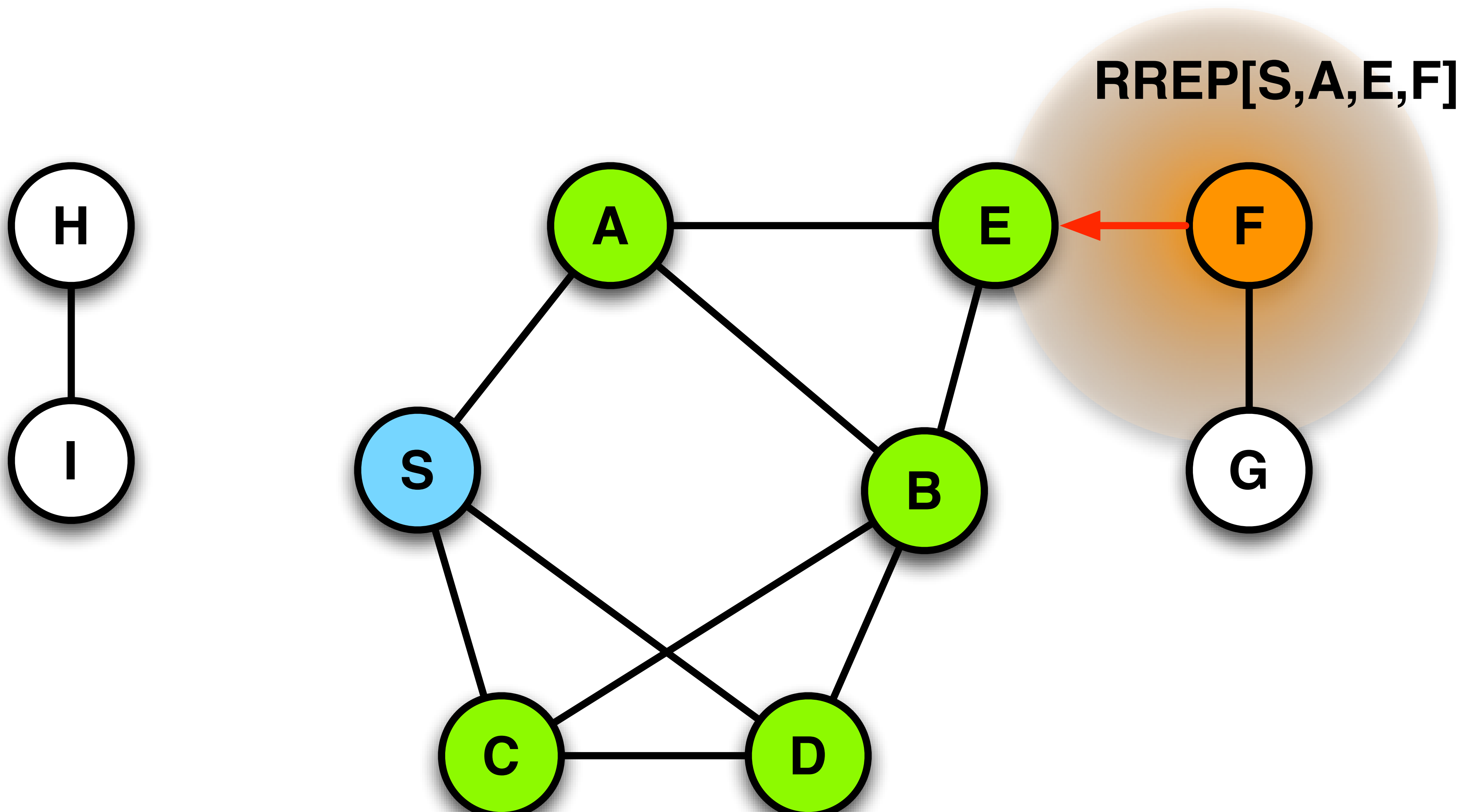
- Johnson, Maltz
  - *Dynamic Source Routing in Ad Hoc Wireless Networks*, Mobile Computing, 1996
- Algorithm
  - Sender initiates route discovery by flooding of **Route-Request (RREQ)**-packets
    - Each forwarding node appends his ID to the RREQ-packet
  - The receiver generates the routing information from the RREQ packet by producing a **Route-Reply (RREP)-**packet
    - using the route information of the packet is sent back to the sender
  - Transmitter sends **data packet** along with route information to the receiver

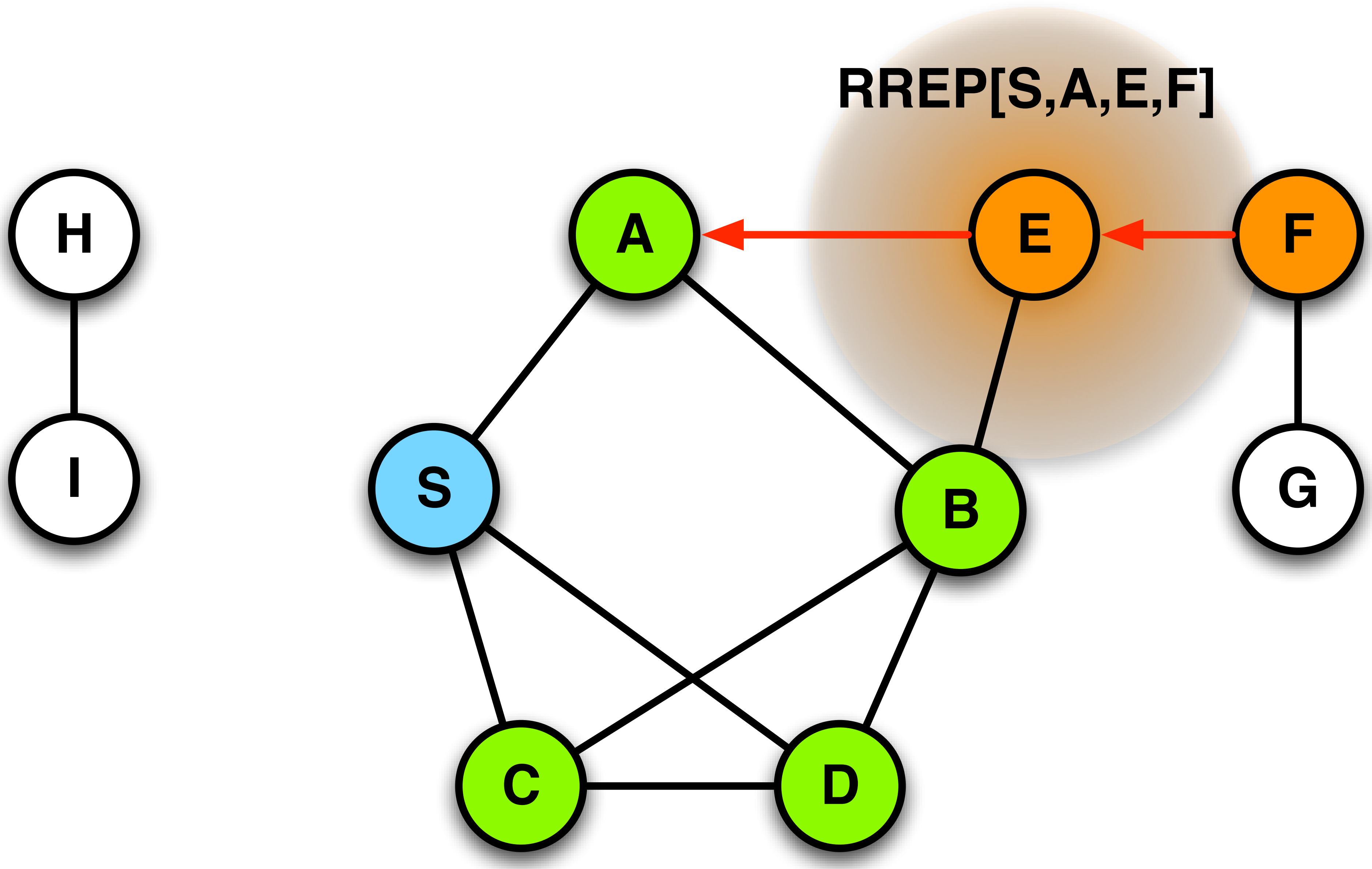

H
A
E
F
I
S
B
G
C
D

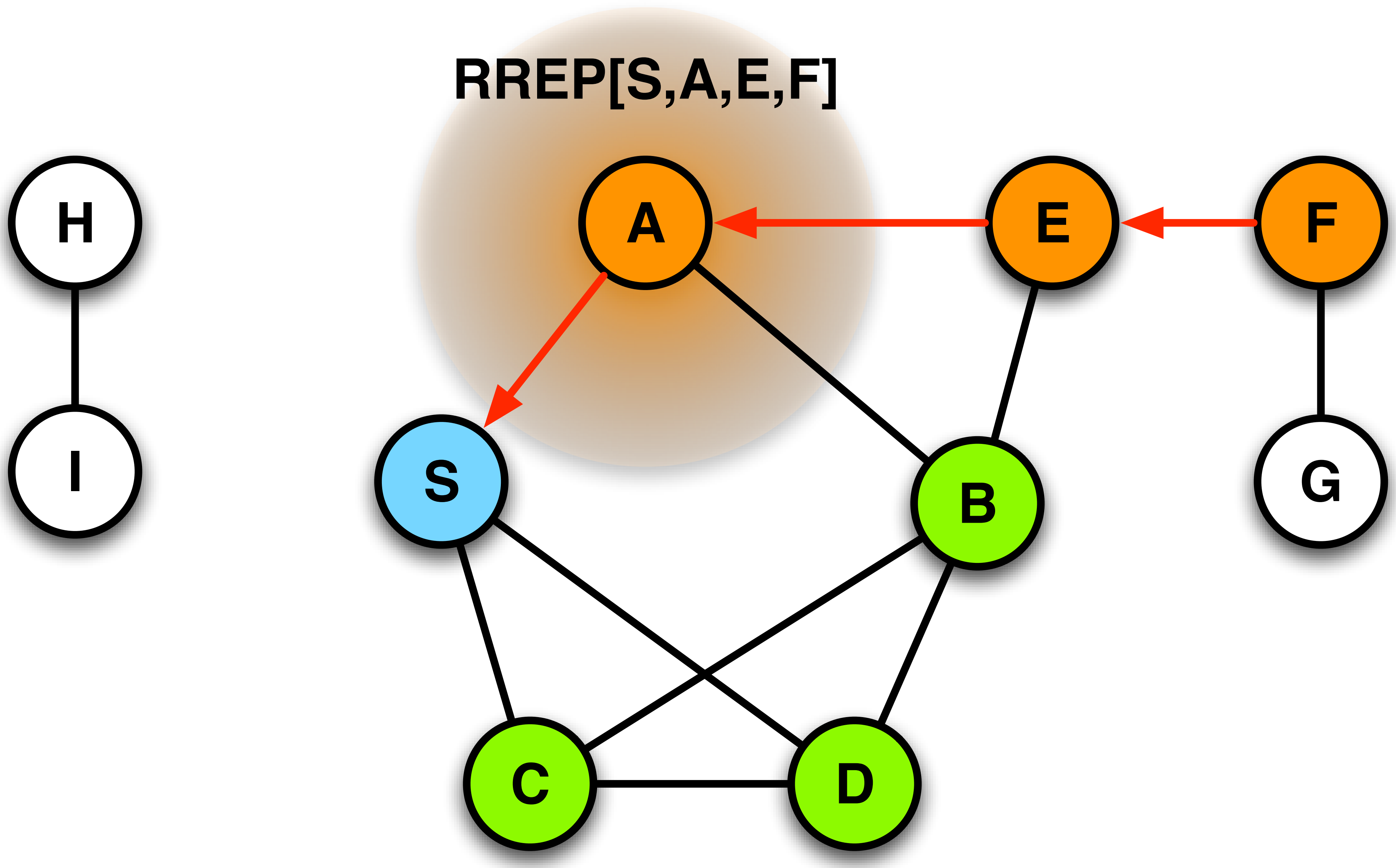

Broadcast
RREQ[S]
RREQ[S]
H
I
S
A
E
F
G
B
C
D

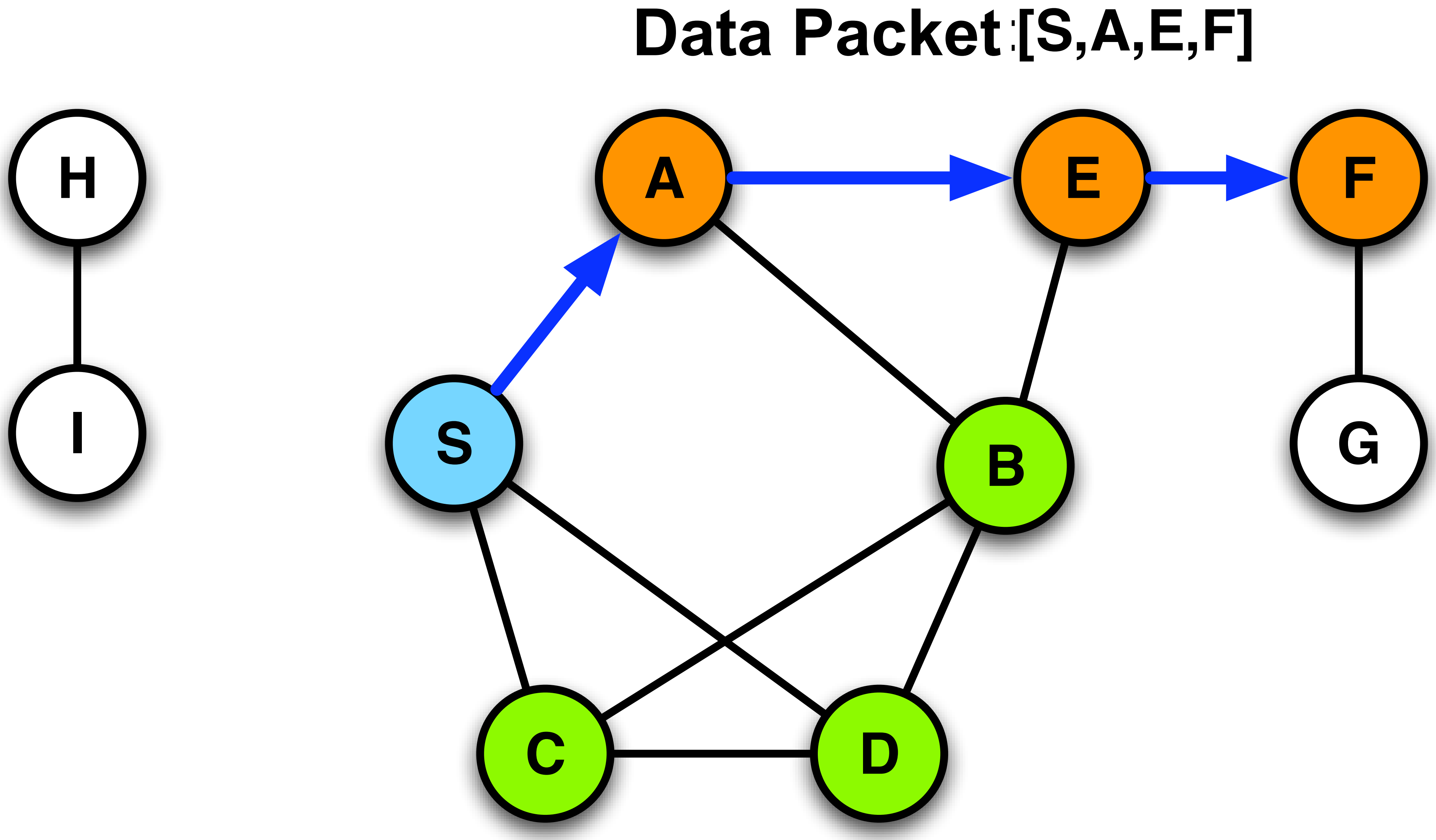

H
I
A
E
F
RREQ[S,A]
S
B
G
RREQ[S,C]
RREQ[S,D]
C
D


RREQ[S,A,E]
H
A
E
F
I
S
B
G
RREQ[S,C,B]
C
D


RREP[S,A,E,F]
H
I
A
E
F
S
B
G
C
D


RREP[S,A,E,F]
H
I
A
E
F
S
B
G
C
D


RREP[S,A,E,F]
H
A
E
F
I
S
B
G
C
D


Data Packet :[S,A,E,F]
H
I
A
E
F
S
B
G
C
D

Requirements

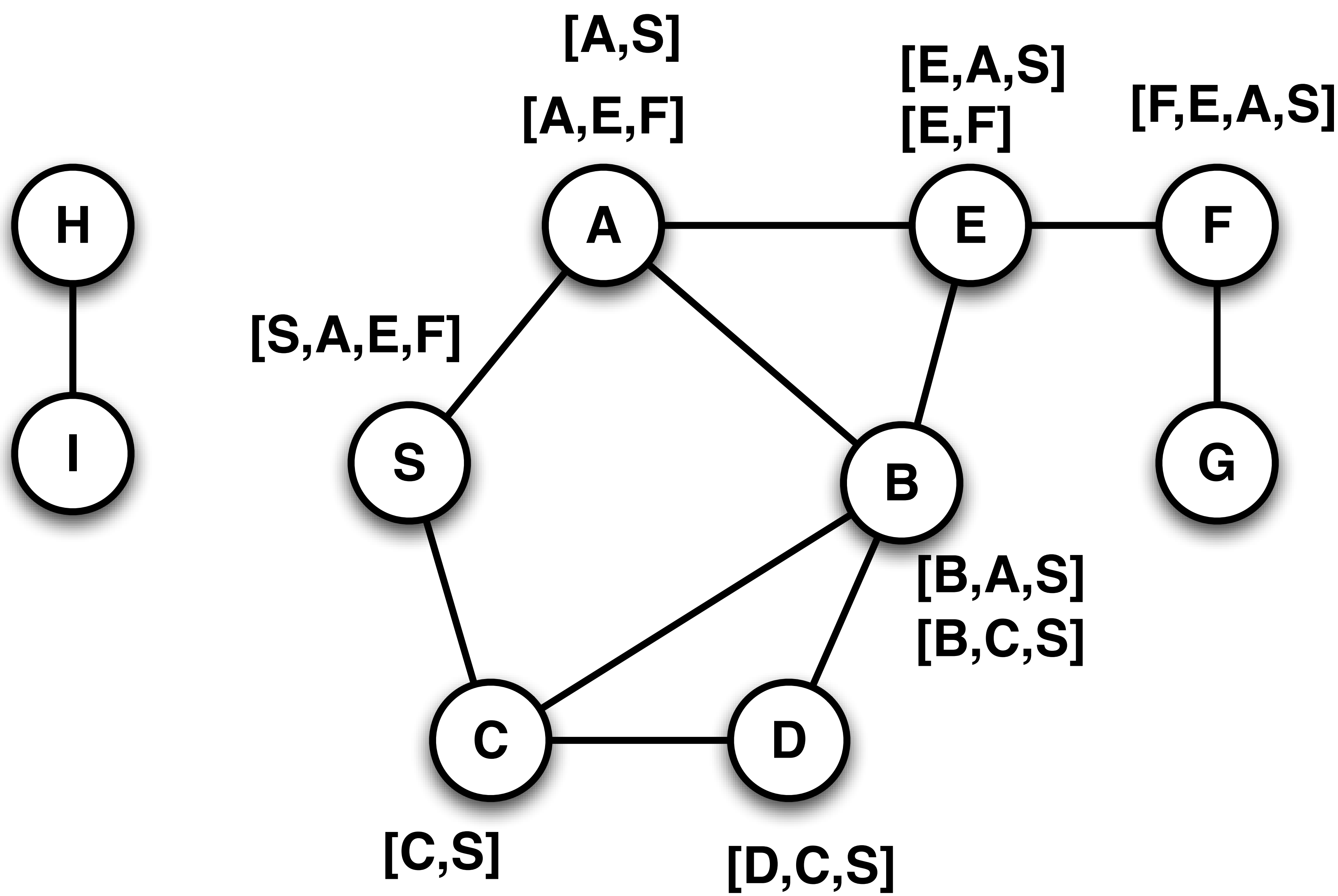
- Route Reply
  - requires bidirectional connections
  - unidirectional links
    - must be tested for symmetry
    - or Route-Reply must trigger its own route-request
- Data packet has all the routing information in the header
  - hence: Source-Routing
- Route determination
  - if no valid route is known

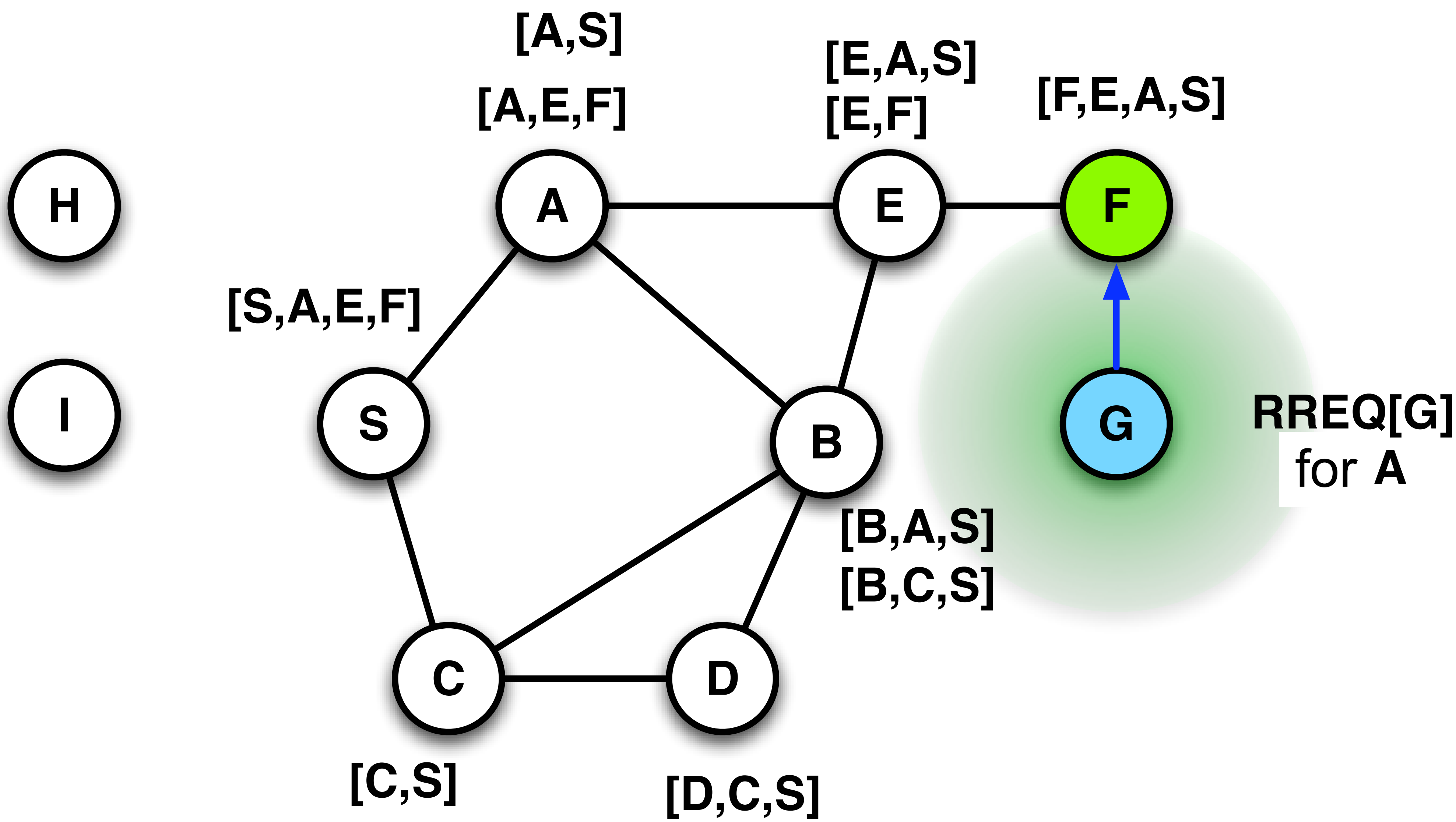
DSR Extensions and Modifications

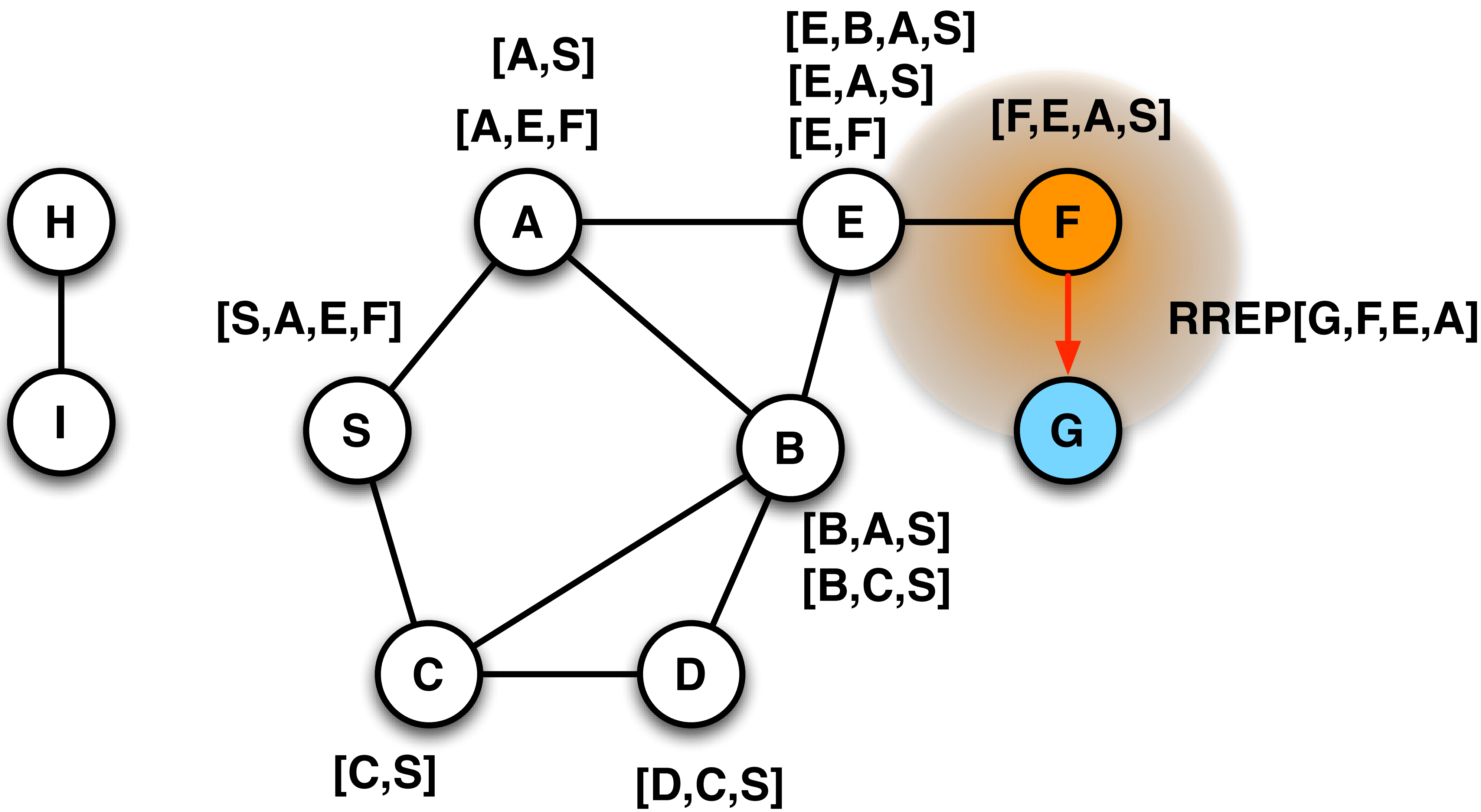
- Intermediate nodes can cache information RREP
  - Problem: stale information
- Listening to control messages
  - can help to identify the topology
- Random delays for answers
  - To prevent many RREP-packets (Reply-Storm)
  - if many nodes know the answer (not for media access)
- Repair
  - If an error is detected then usually: route recalculation
  - Instead: a local change of the source route
- Cache Management
  - Mechanisms for the deletion of outdated cache information

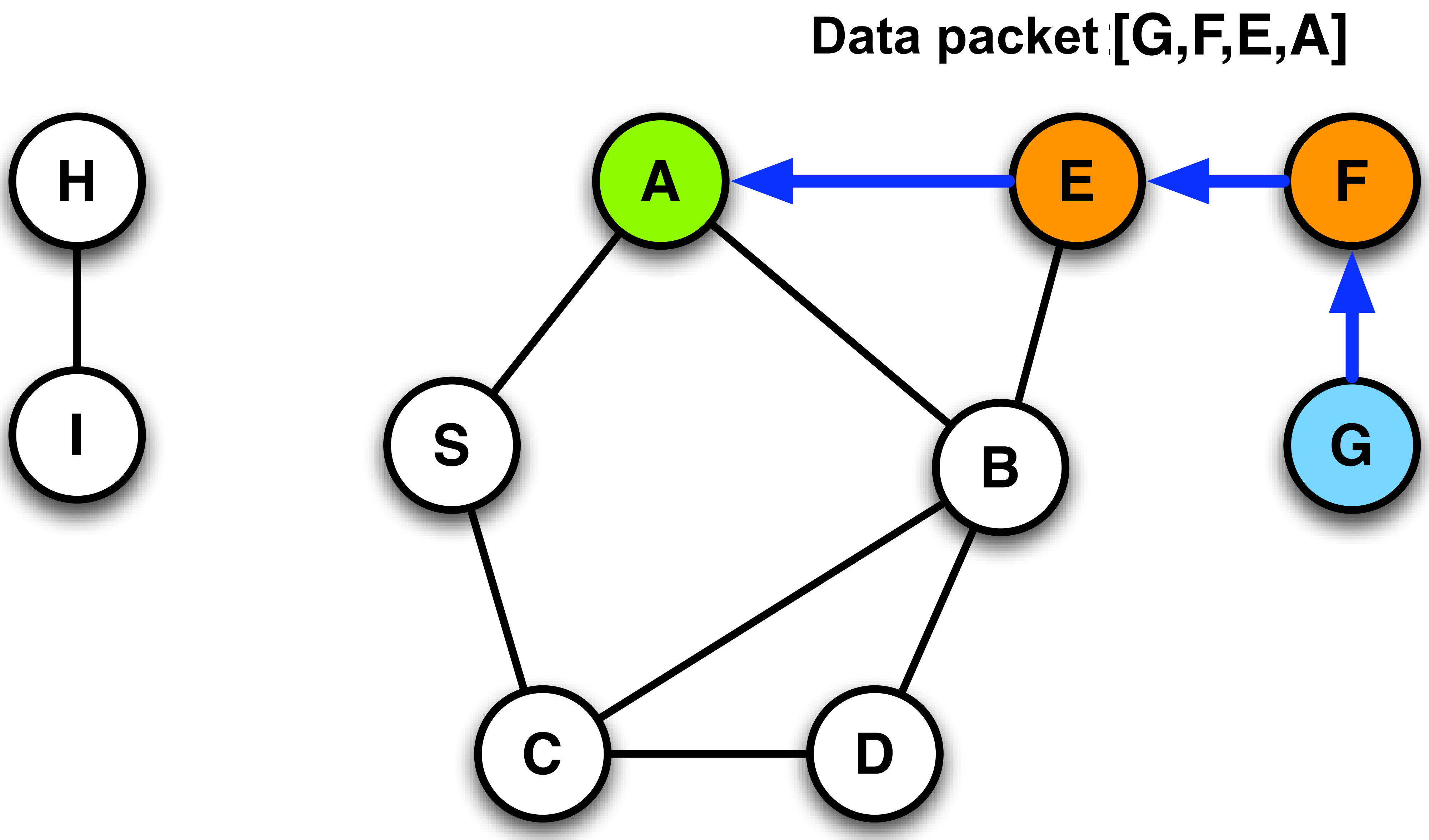
DSR Optimization Route Caching

- Each node stores information from all available
  - Header of data packets
  - Route Request
  - Route-Reply
  - partial paths
- From this information, a route reply is generated


[A,S]
[A,E,F]
[E,A,S]
[E,F]
[F,E,A,S]
H
A
E
F
[S,A,E,F]
I
S
B
G
[B,A,S]
[B,C,S]
C
D
[C,S]
[D,C,S]

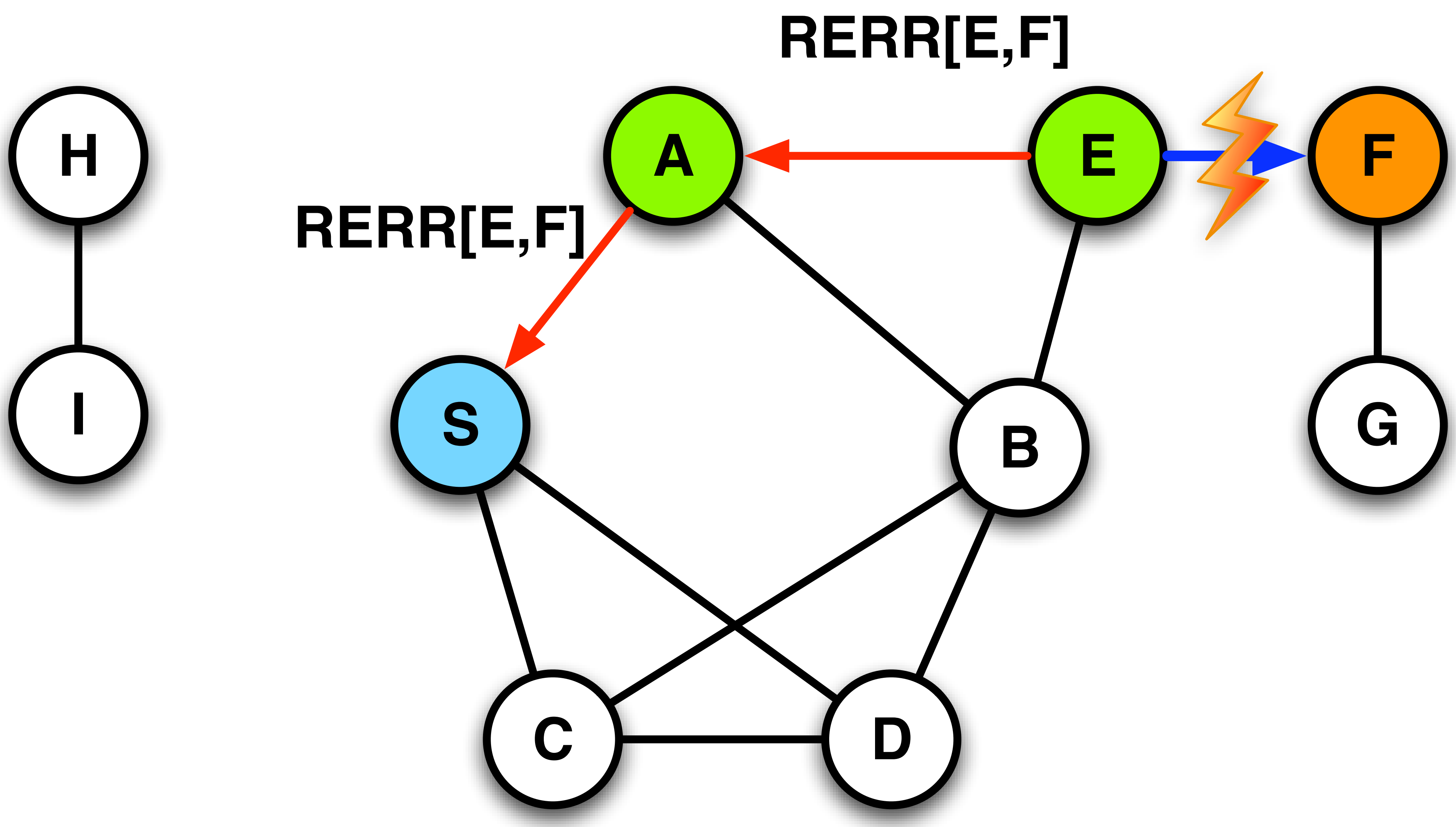

[A,S]
[A,E,F]
[E,A,S]
[E,F]
[F,E,A,S]
H
A
E
F
[S,A,E,F]
I
S
B
G
RREQ[G]
for A
[B,A,S]
[B,C,S]
C
D
[C,S]
[D,C,S]


[A,S]
[A,E,F]
[E,B,A,S]
[E,A,S]
[E,F]
[F,E,A,S]
H
A
E
F
RREP[G,F,E,A]
[S,A,E,F]
I
S
B
G
[B,A,S]
[B,C,S]
C
D
[C,S]
[D,C,S]


Data packet [G,F,E,A]
H
I
A
E
F
S
B
G
C
D

DSR Optimization
Route Caching

- If any information is incorrect
  - because a route no longer exists
  - then this path is deleted from the cache
  - alternative paths are used
  - or RREQ is generated
- **Missing links are distributed by (RERR) packets in the network**


RERR[E,F]
RERR[E,F]
H
A
E
F
I
S
B
G
C
D

DSR Discussion

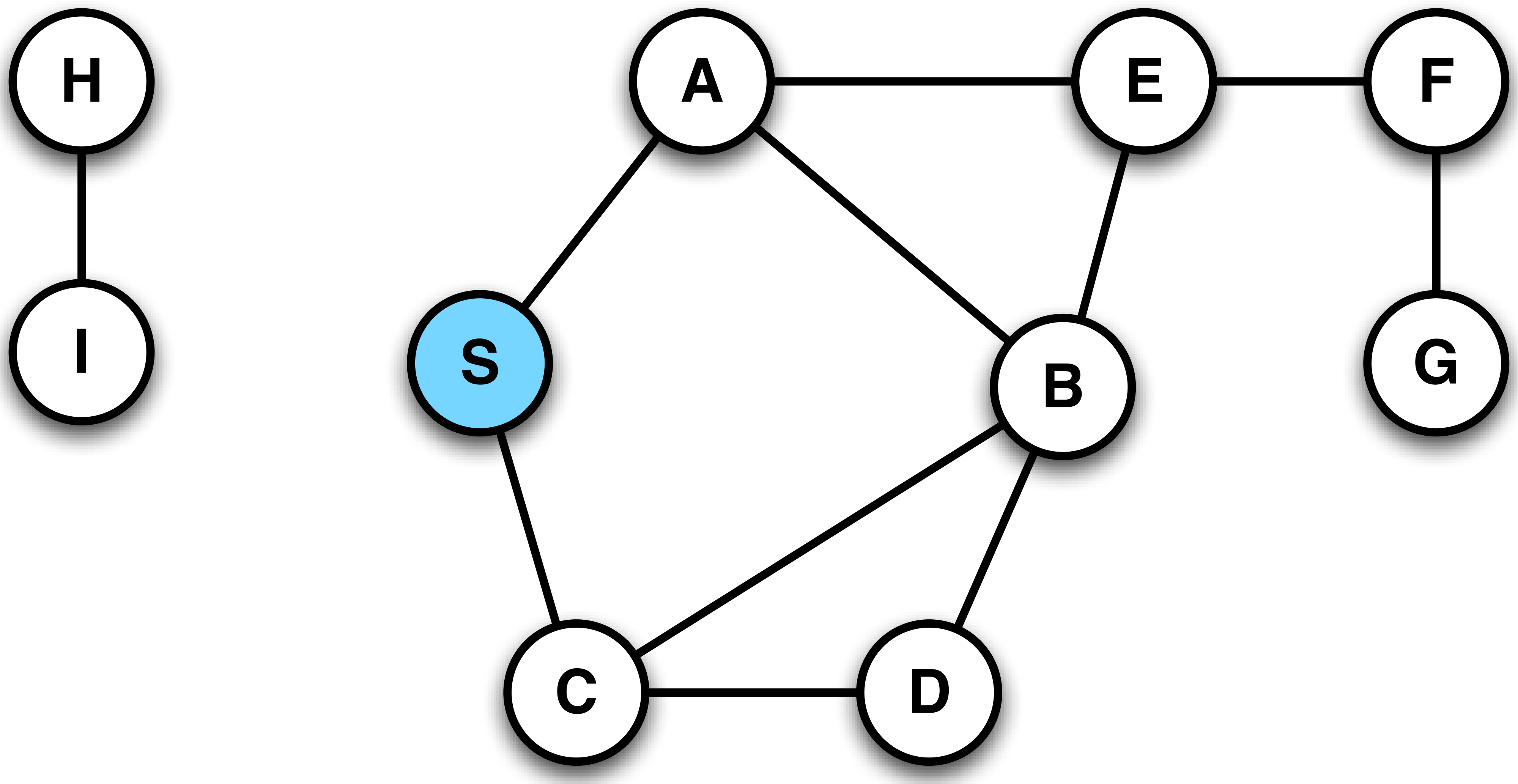
- Benefits
  - Routes are maintained only between communicating nodes
  - Route caching reduces route search
  - Caches help many alternative routes to find
- Disadvantages
  - Header size grows with distance
  - Network may be flooded with route requests
  - Route-Reply-Storm
  - Outdated information may cause cache overhead

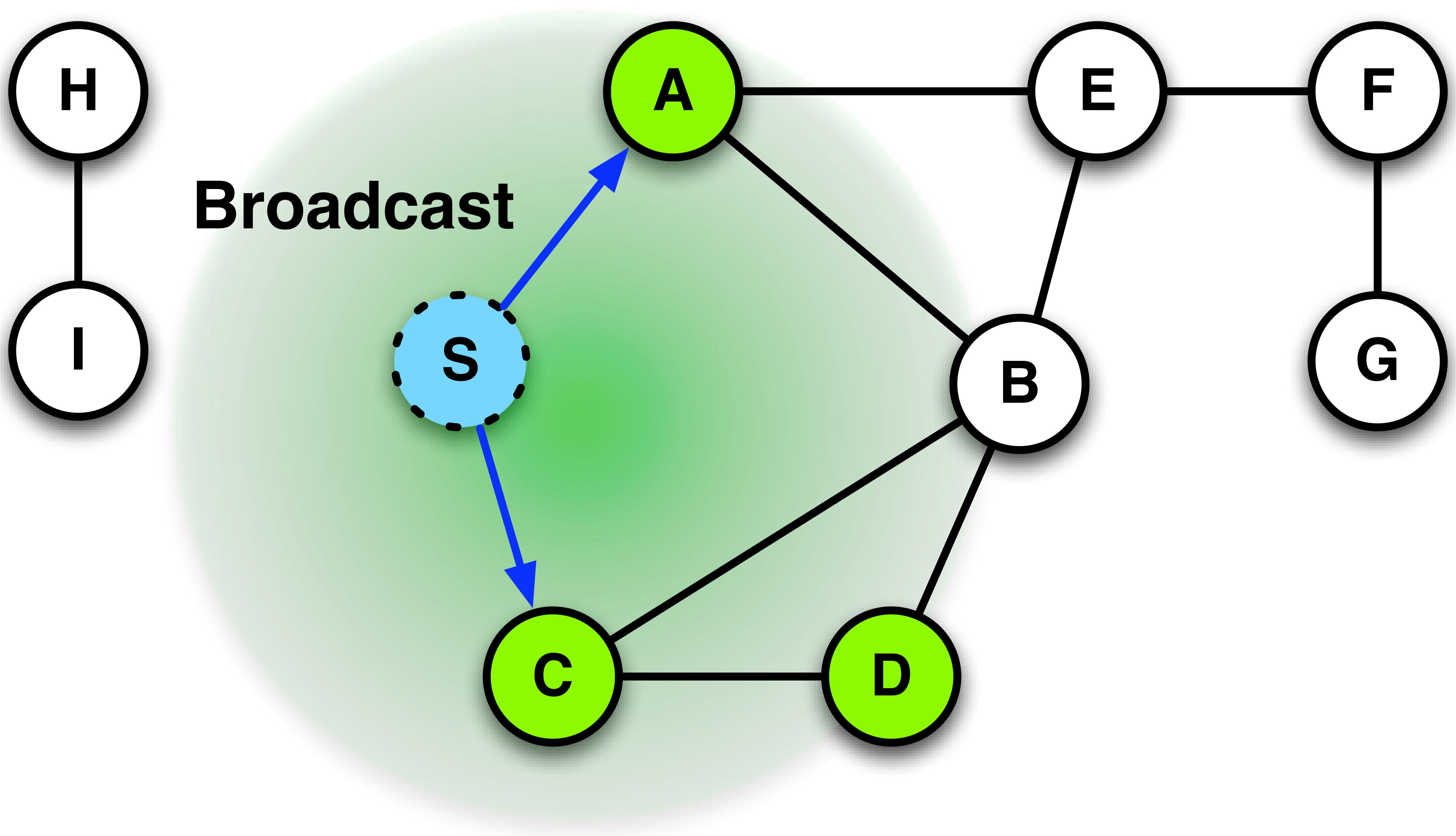
AODV

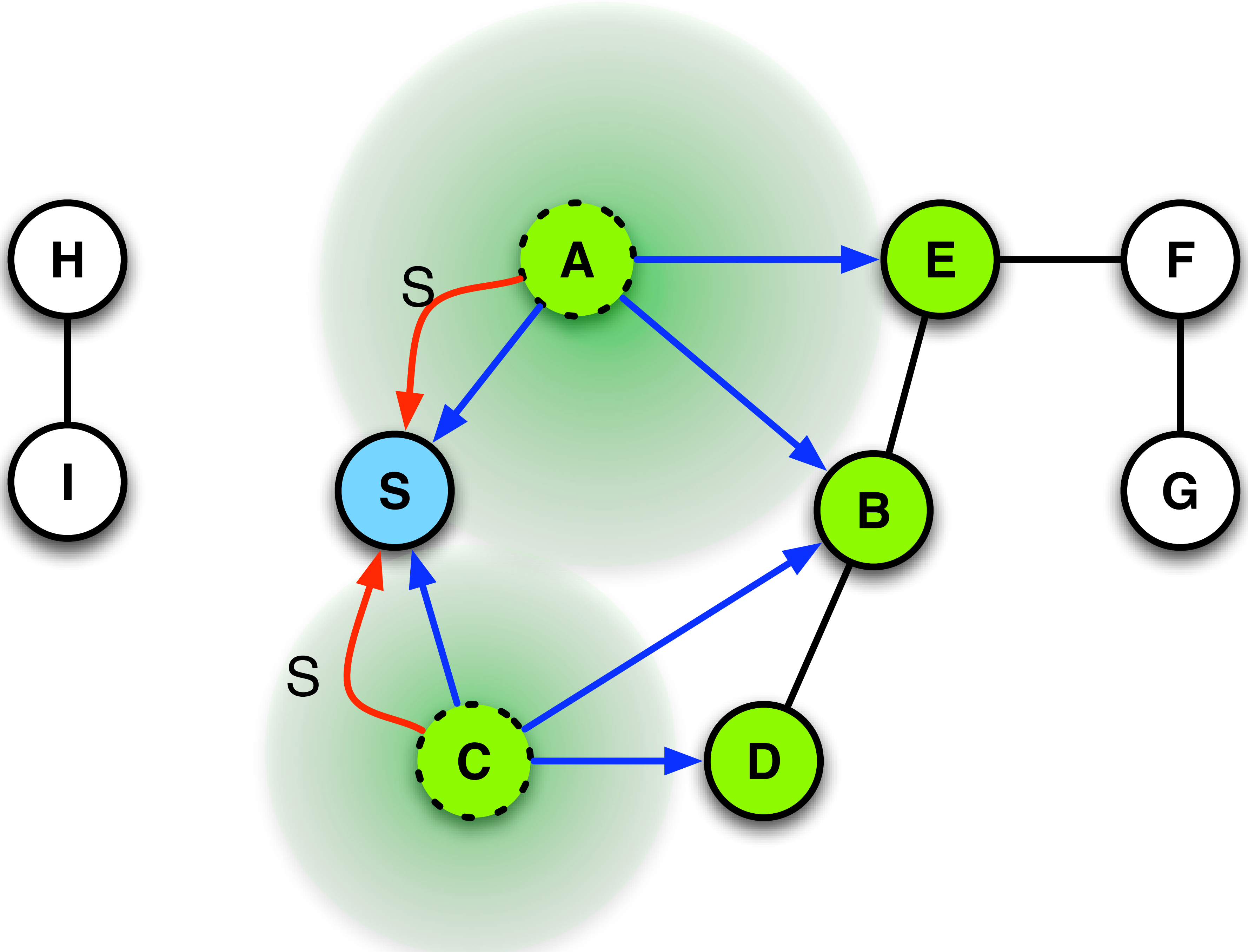
- Perkins, Royer
  - Ad hoc On-Demand Distance Vector Routing, IEEE Workshop on Mobile Computing Systems and Applications,1999
- Reaktives Routing-Protokoll
- Reactive routing protocol
  - Improvement of DSR
  - no source routing
  - Distance Vector Tables
    - but only for nodes with demand
  - Sequence number to help identify outdated cache info
  - Nodes know the origin of a packet and update the routing table

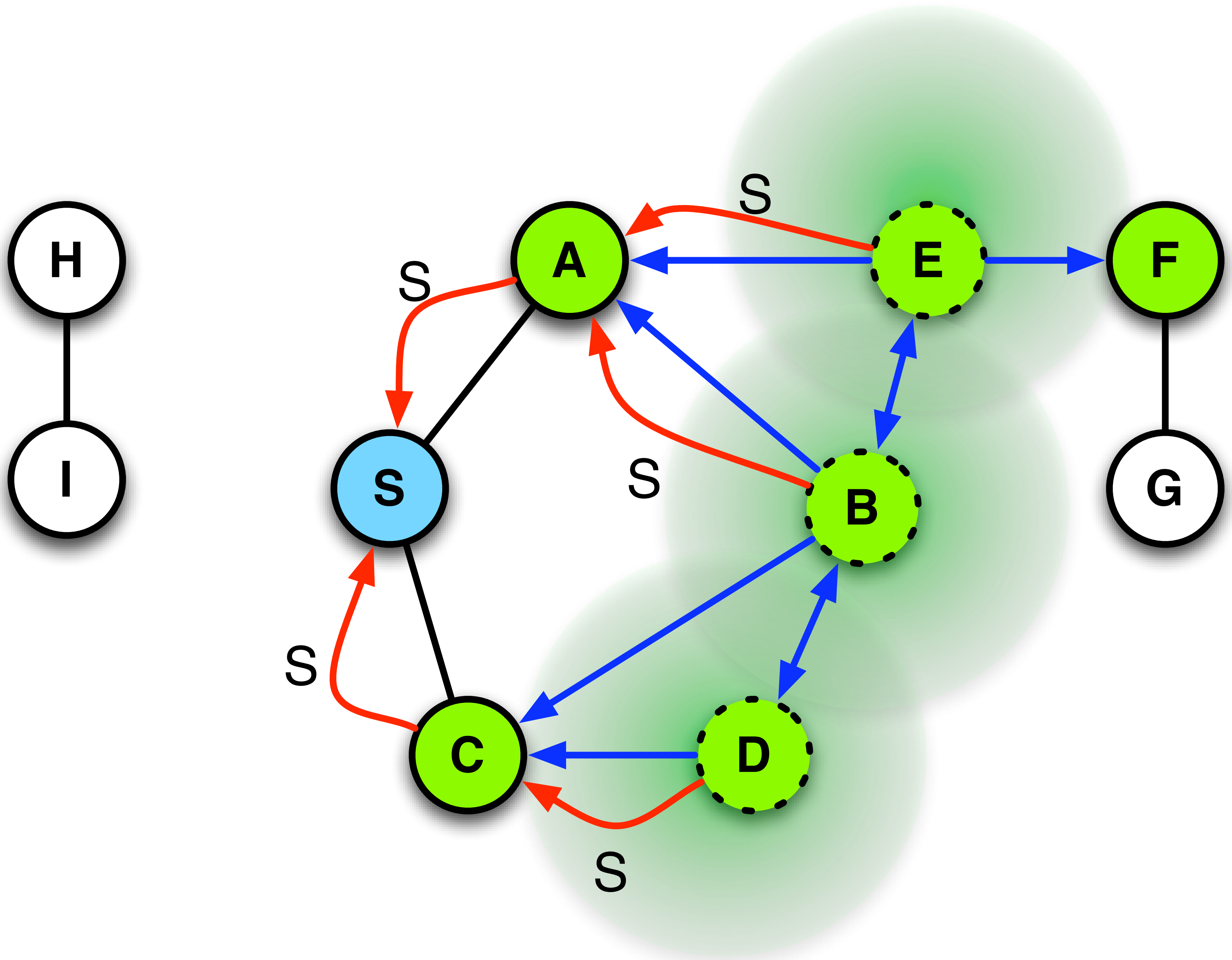
AODV

- Algorithm
  - Route Request (RREQ) like in DSR
  - Intermediate nodes set a reverse pointer towards thesender
  - If the target is reached, a Route Reply (RREP) is sent
  - Route Reply follow the pointers
- Assumption: symmetric connections

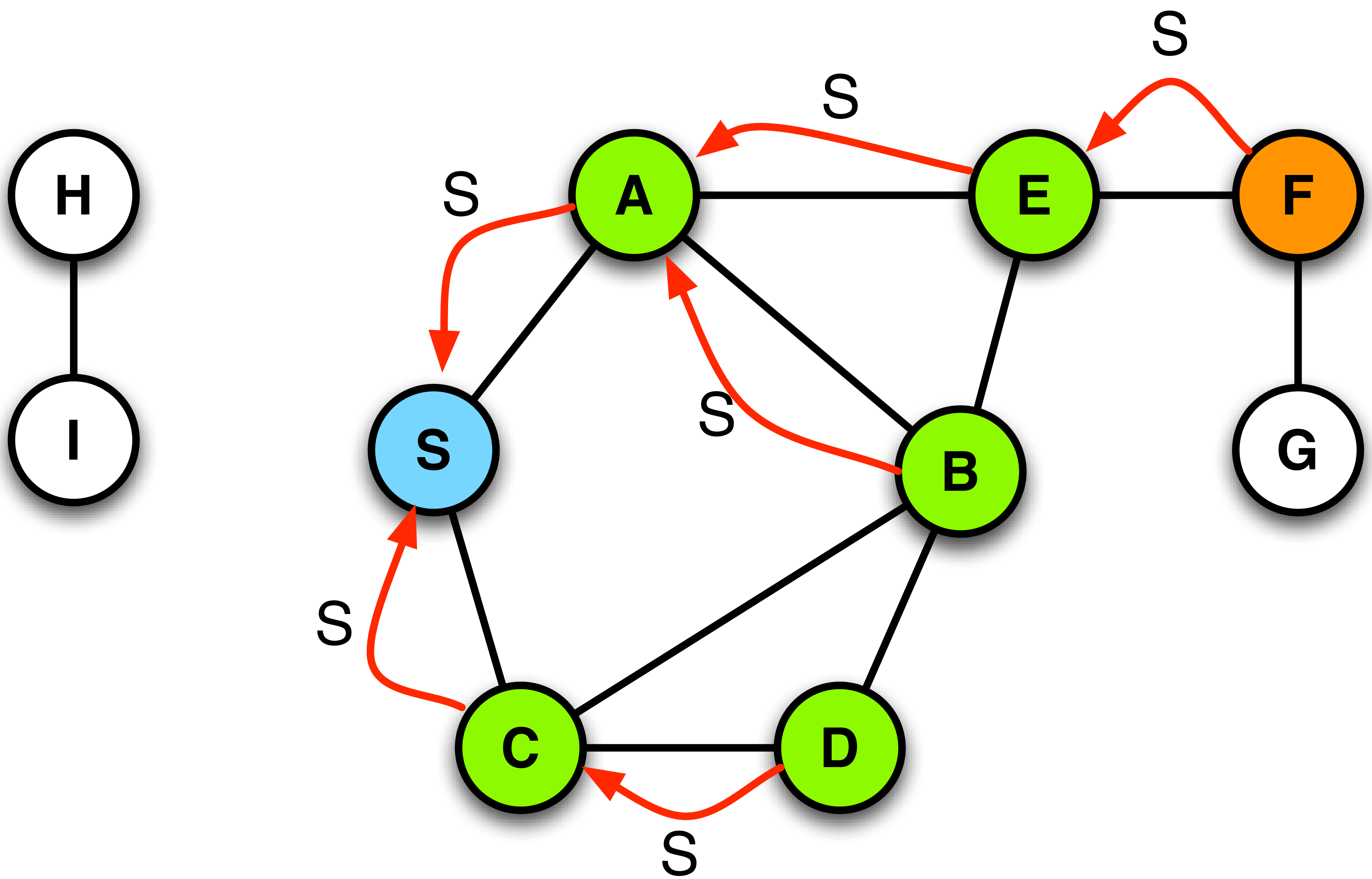

H
I
A
E
F
S
B
G
C
D

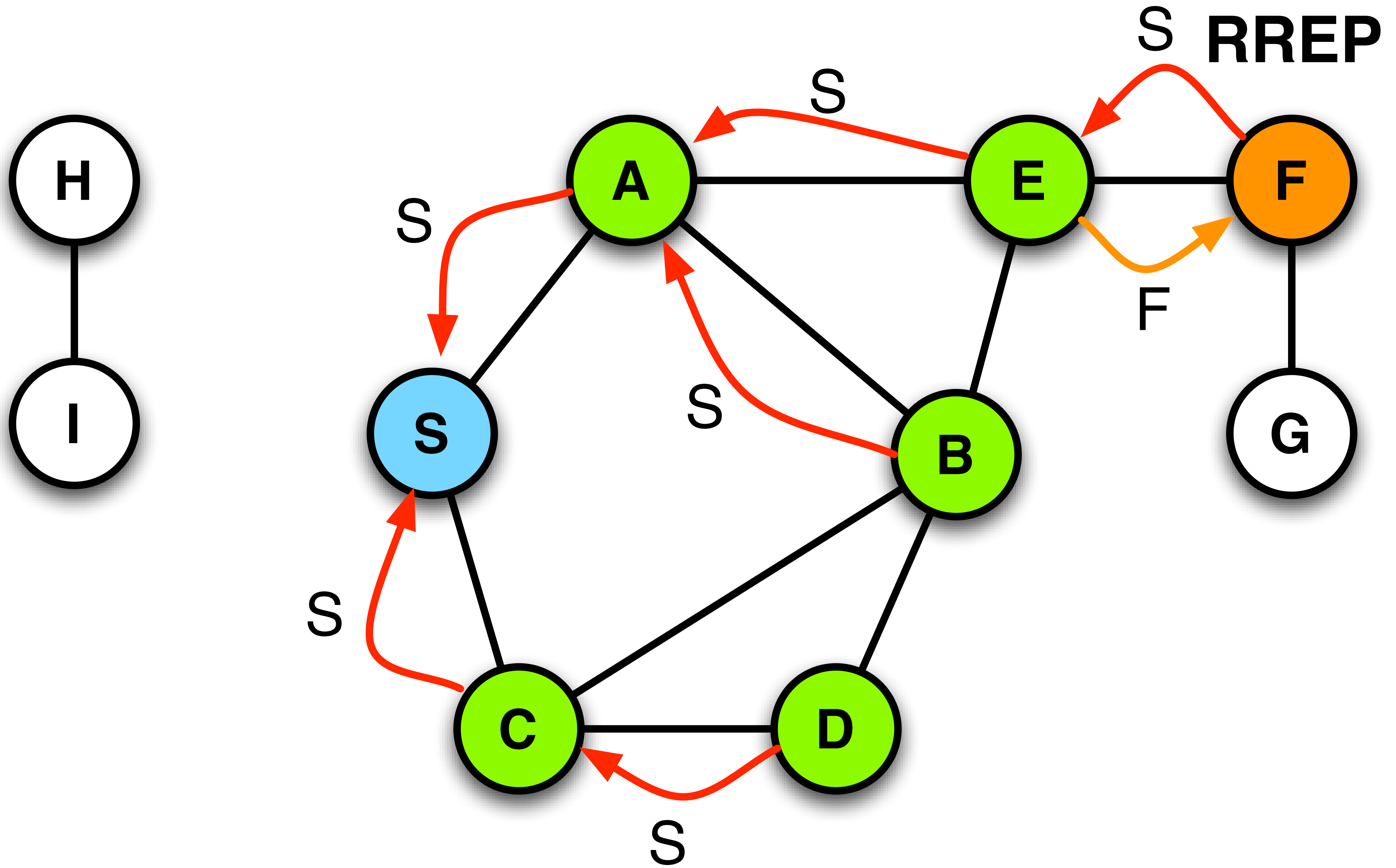

H
A
E
F
Broadcast
I
S
B
G
C
D

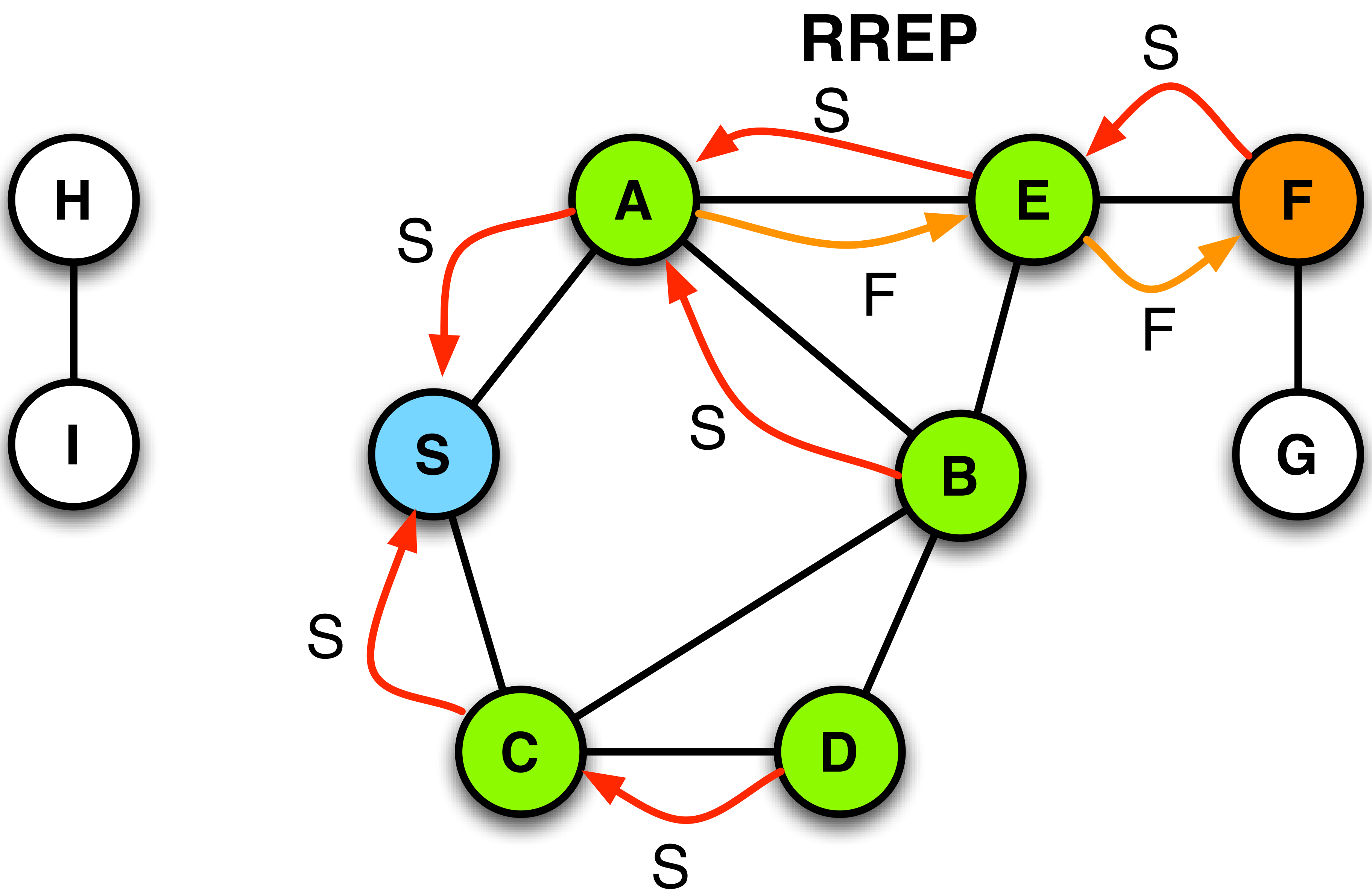

H
I
A
E
F
S
S
S
B
G
S
C
D

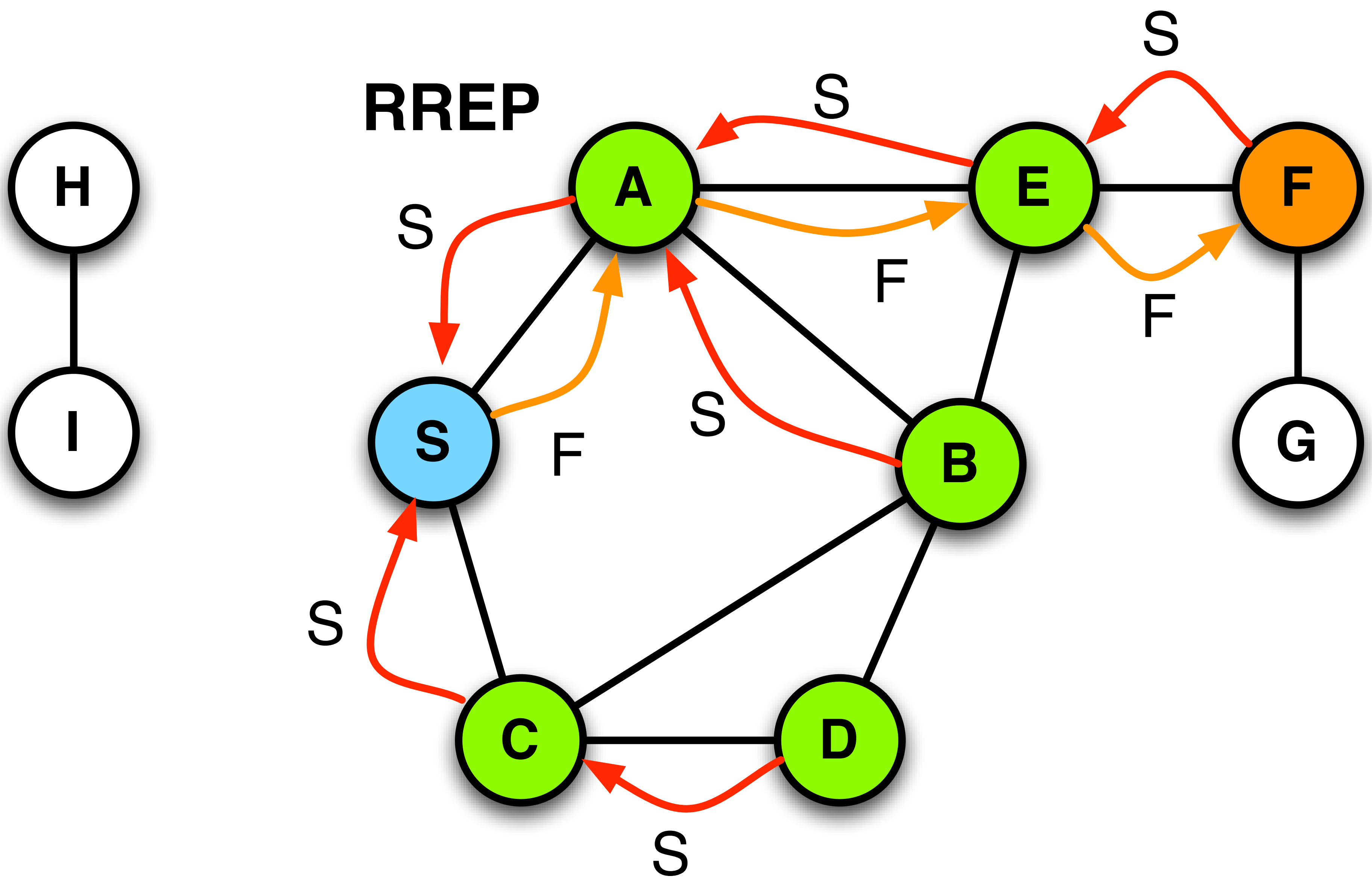


H
I
S
A
E
F
G
B
C
D
S
S
S
S
S
S

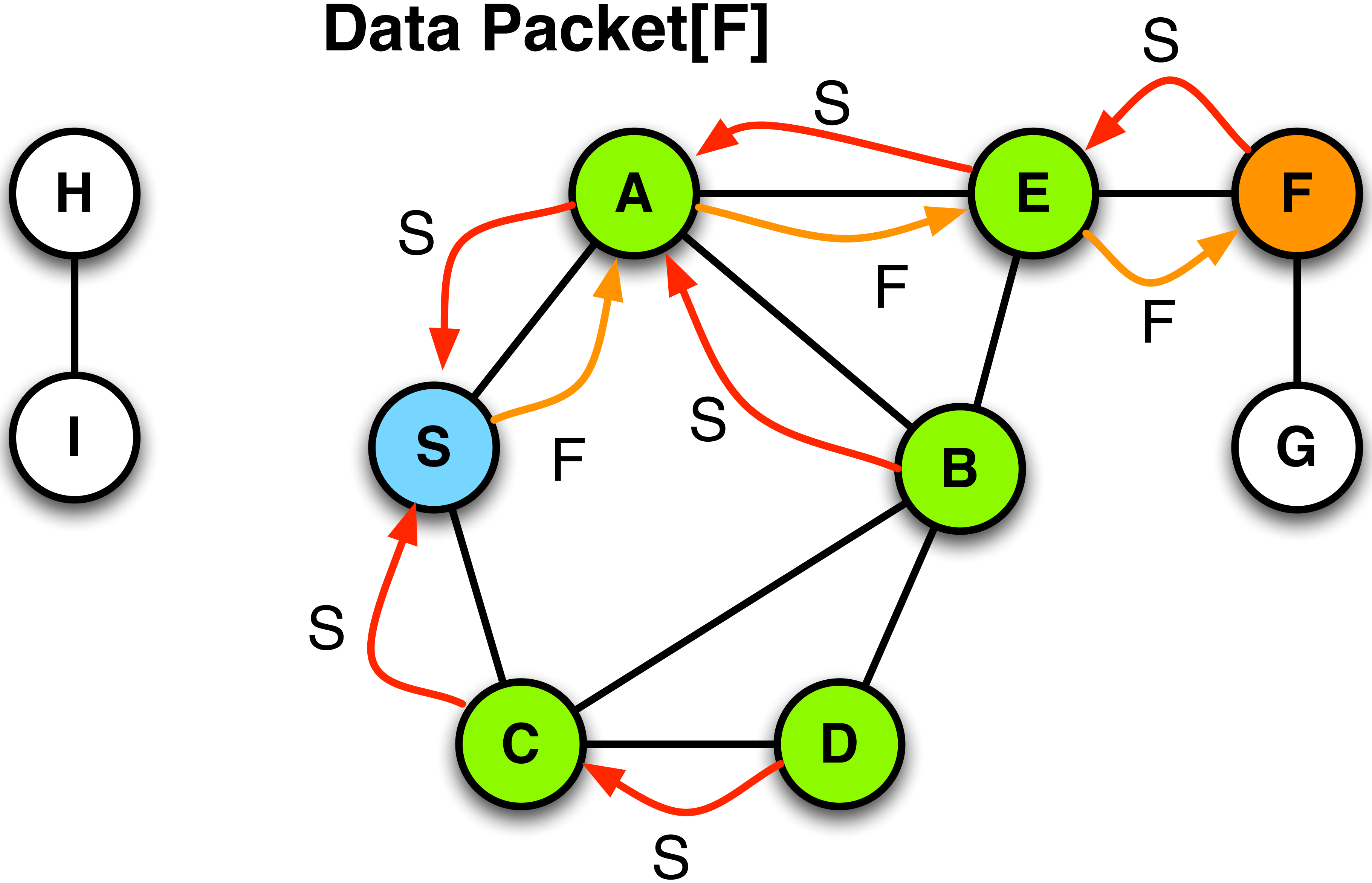

S
S
S
H
A
E
F
I
S
S
B
G
S
C
D
S


RREP
S
S
S
F
S
S
S
H
I
A
E
F
G
S
B
C
D


RREP
S
S
H
A
E
F
S
F
F
I
S
S
B
G
S
C
D
S


RREP
H
I
A
E
F
S
B
G
C
D
S
S
S
F
F
S
F
S
S

Data Packet[F]



Route Reply in AODV

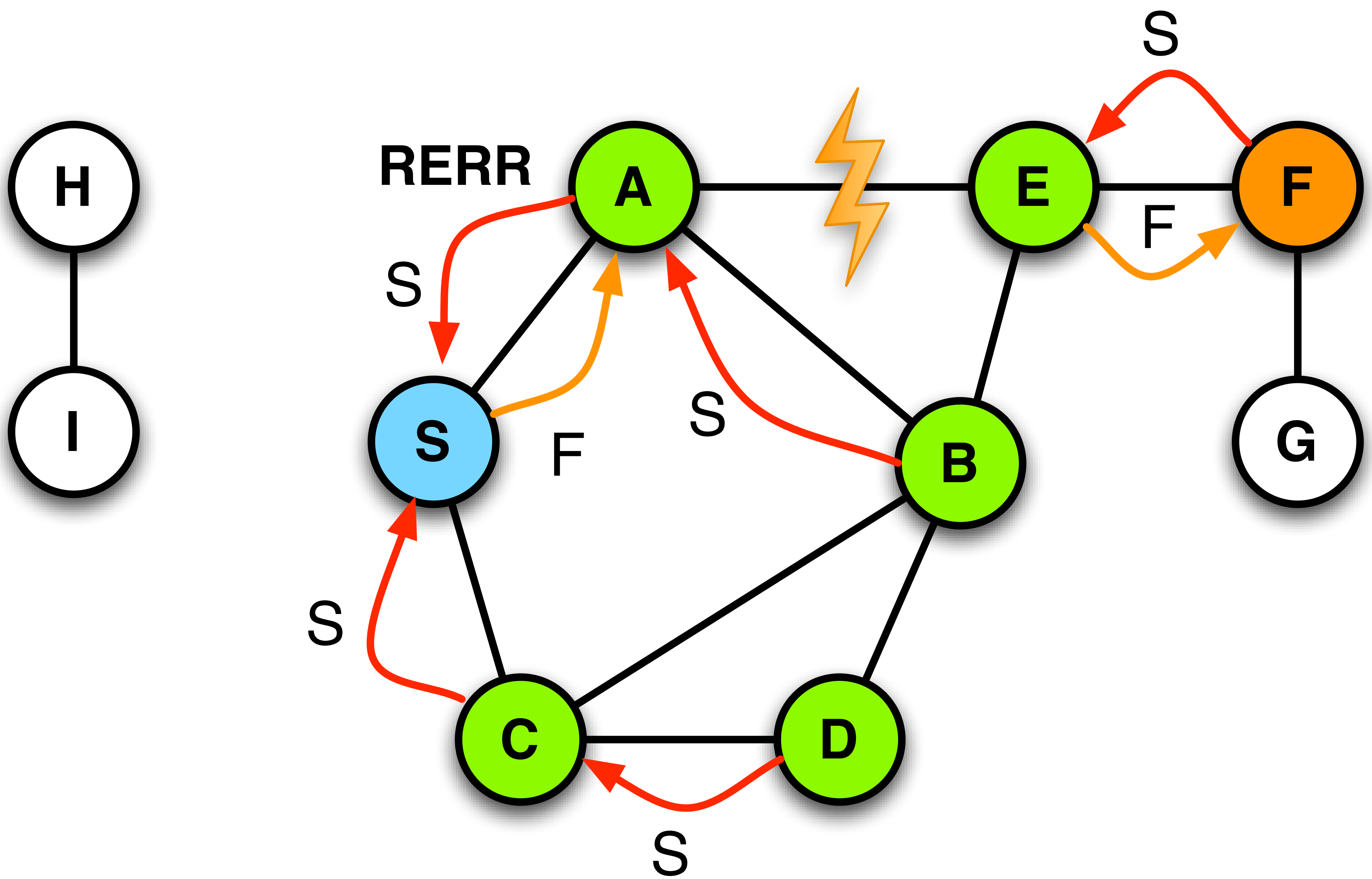
- Intermediate nodes
  - may send route-reply packets, if their cache information is up-to-date
- Destination Sequence Numbers
  - measure the up-to-dateness of the route information
  - AODV uses cached information less frequently than DSR
  - A new route request generates a greater destination sequence number
  - Intermediate nodes with a smaller sequence number may not generate a route reply (RREP) packets

Timeouts

- Reverse pointers are deleted after a certain time
  - RREP timeout allows the transmitter to go back
- Routing table information to be deleted
  - if they have not been used for some time
  - Then a new RREQ is triggered

Link Failure Reporting

- Neighbors of a node X are active,
  - if the routing table cache are not deleted
- If a link of the routing table is interrupted,
  - then all active neighbors are informed
- Link failures are distributed by Route Error (RERR) packets to the sender
  - also update the Destination Sequence Numbers
  - This creates new route request

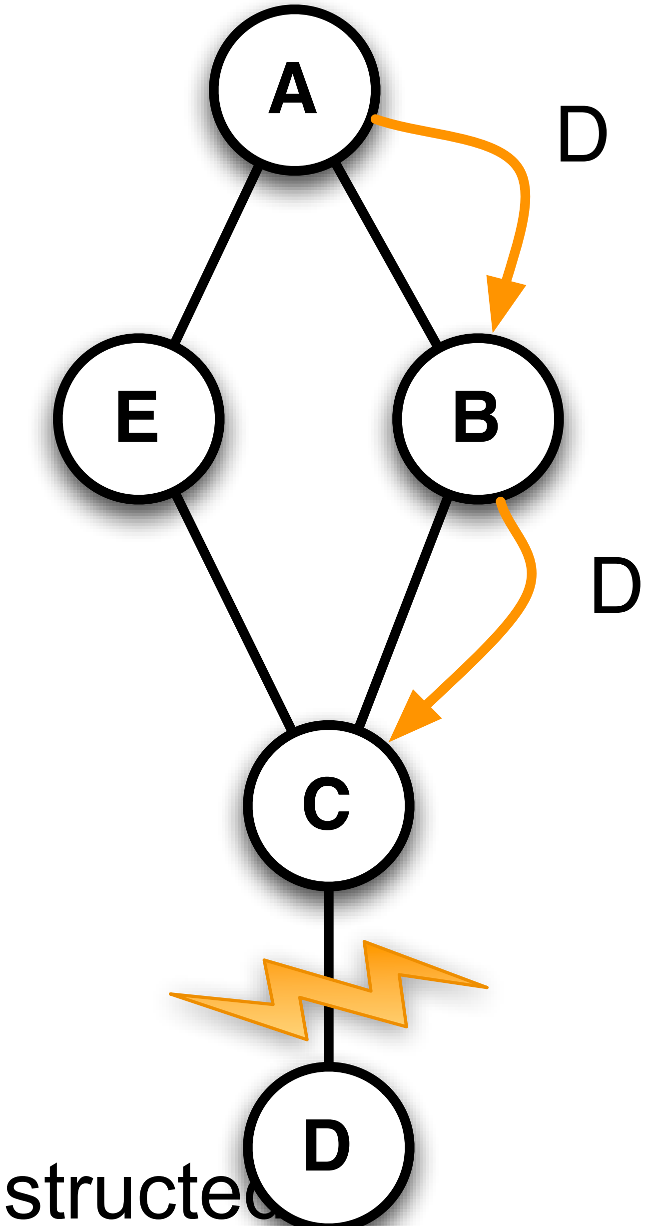

H
I
RERR
A
E
F
S
S
F
S
B
G
S
S
C
D
S
F

Detection of Link Failure

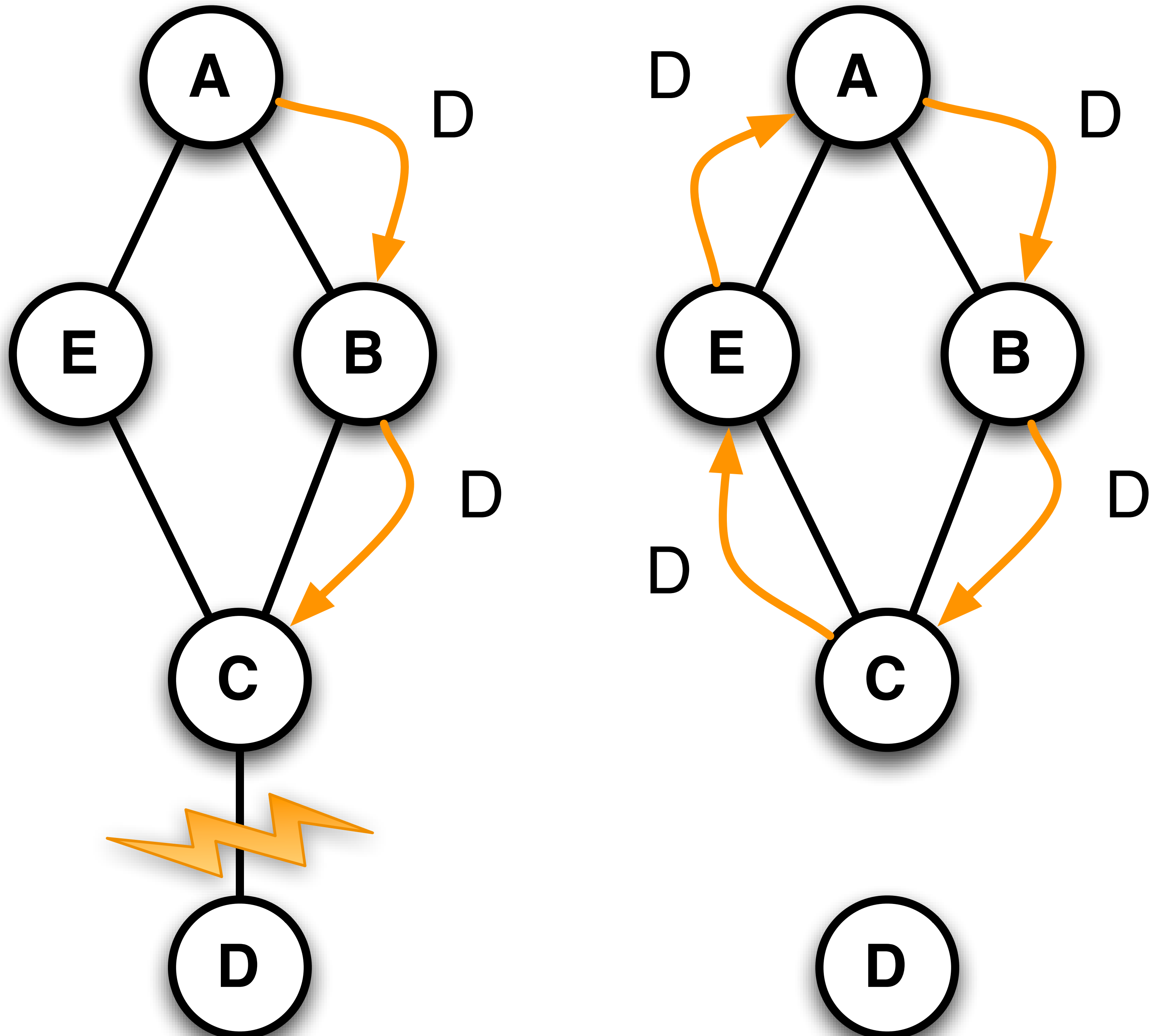
- Hello messages
  - neighboring nodes periodically exchange hello packets from
  - Absence of this message indicates link failure
- Alternative
  - use information from MAC protocol

Sequence Numbers

- When a node receives a message with destination sequence number N
  - then this node sets its number to N
  - if it was smaller before
- In order to prevent loops
  - If A has not noticed the loss of link (C, D)
    - (for example, RERR is lost)
  - If C sends a RREQ
    - on path C-E-A
  - Without sequence numbers, a loop will be constructed
    - since A "knows" a path to D, this results in a loop (for instance, CEABC)



Sequence Numbers



Optimization
Expanding Ring Search

- Route Requests
  - *start with small time-to-live value (TTL)*
  - if no Route Reply (RREP) is received, the value is increased by a constant factor and resent
- This optimization is also applicable for DSR

DYMO - Dynamic MANET On-demand (AODVv2) Routing

- Literature
  - I. Chakeres and C. Perkins, “Dynamic MANET On-demand (DYMO) Routing,” IETF MANET, Internet-Draft, 5 December 2008, draft-ietf-manet-dymo-16.
- Improvement of AODV
  - RREQ, RREP to construct shortest length paths
  - Path accumulation
    - a single route request creates routes to all the nodes along the path to the destination
  - Unreliable links can be assigned a cost higher than one
  - Sequence numbers to guarantee the freshness routing table entries

Routing in MANETs

- Routing
  - Determination of message paths
  - Transport of data
- Protocol types
  - proactive
    - Routing tables with updates
  - reactive
    - repair of message paths only when necessary
  - hybrid
    - combination of proactive and reactive

Routing Protocols for MANETs

- **Proactive**
  - Routes are **demand independent**
  - Standard Link-State und Distance-Vector Protocols
    - Destination Sequenced Distance Vector (**DSDV**)
    - Optimized Link State Routing (**OLSR**)
- **Reactive**
  - Route are determined when needed
    - Dynamic Source Routing (**DSR**)
    - Ad hoc On-demand Distance Vector (**AODV**)
    - Dynamic MANET On-demand Routing Protocol
    - Temporally Ordered Routing Algorithm (**TORA**)
- **Hybrid**
  - combination of reactive und proactive
    - Zone Routing Protocol (**ZRP**)
    - Greedy Perimeter Stateless Routing (**GPSR**)

Optimized Link State Routing

- Literature
  - RFC3626: Clausen, Jacquet, *Optimized Link State Routing Protocol, 2003*
  - First published 1999
- Most proaktive protocols are are based on
  - Link-state routing
  - Distance-Vector routing

Link State Routing

- Connections are periodically published throughout the network
- Nodes propagate information to their neighbors
  - i.e. flooding
- All network information is stored
  - with time stamp
- Each node computes shortest paths
  - possibly also other route optimizations

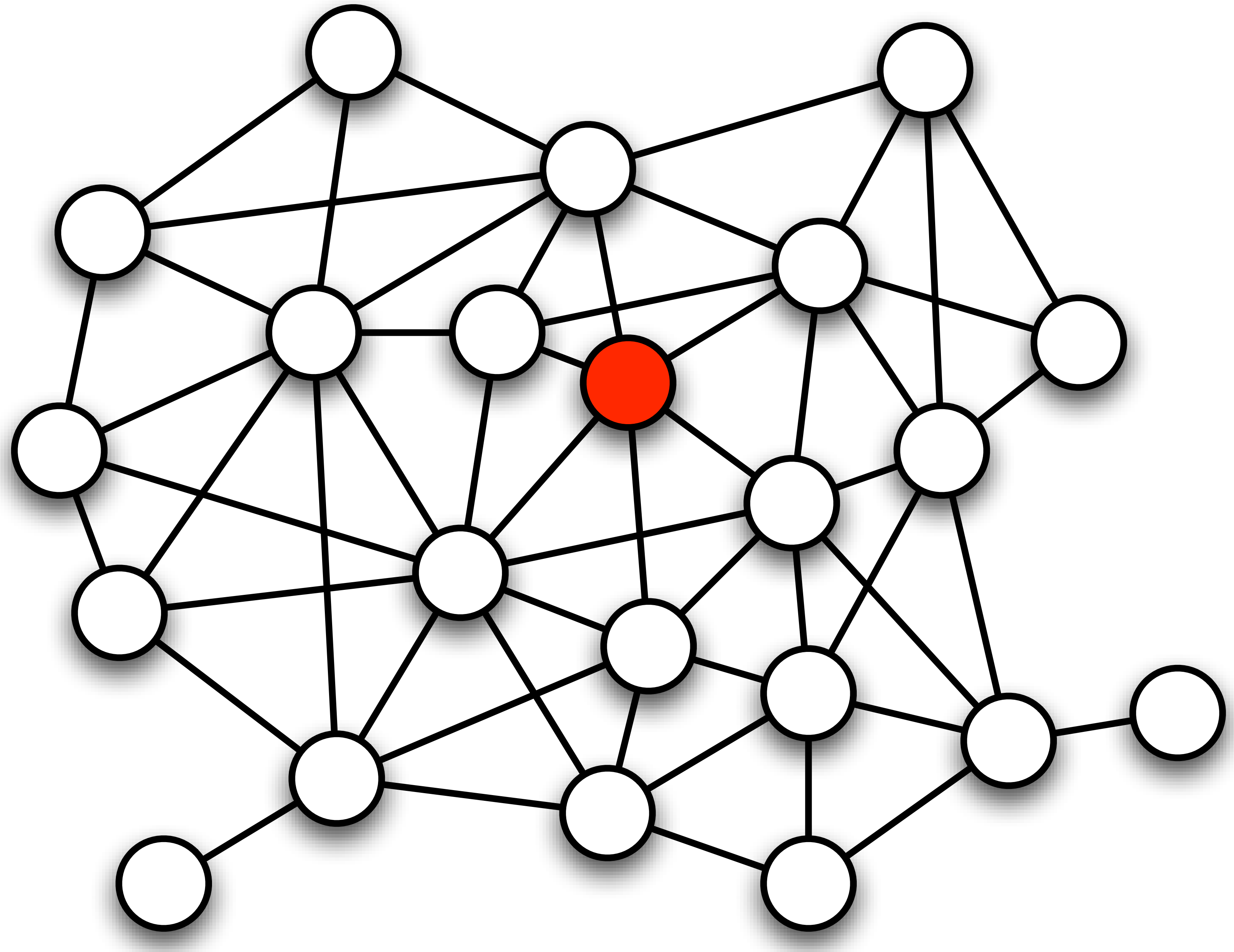
Optimized Link State Routing (OLSR)

- Each nodes broadcasts its neighborhood list
  - Each node can determinate its 2-hop neighborhood
- Reducing the number of messages
  - fewer nodes participate in flooding
- Multipoint relay node (MPRs)
  - are chosen such that each node has at least one multipoint relay node as in its 2-hop neighborhood
  - Only multipoint relay nodes propagate link information
- Node sends their neighborhood lists
  - such that multipoint relay nodes in the 2-hop neighborhood can be chosen

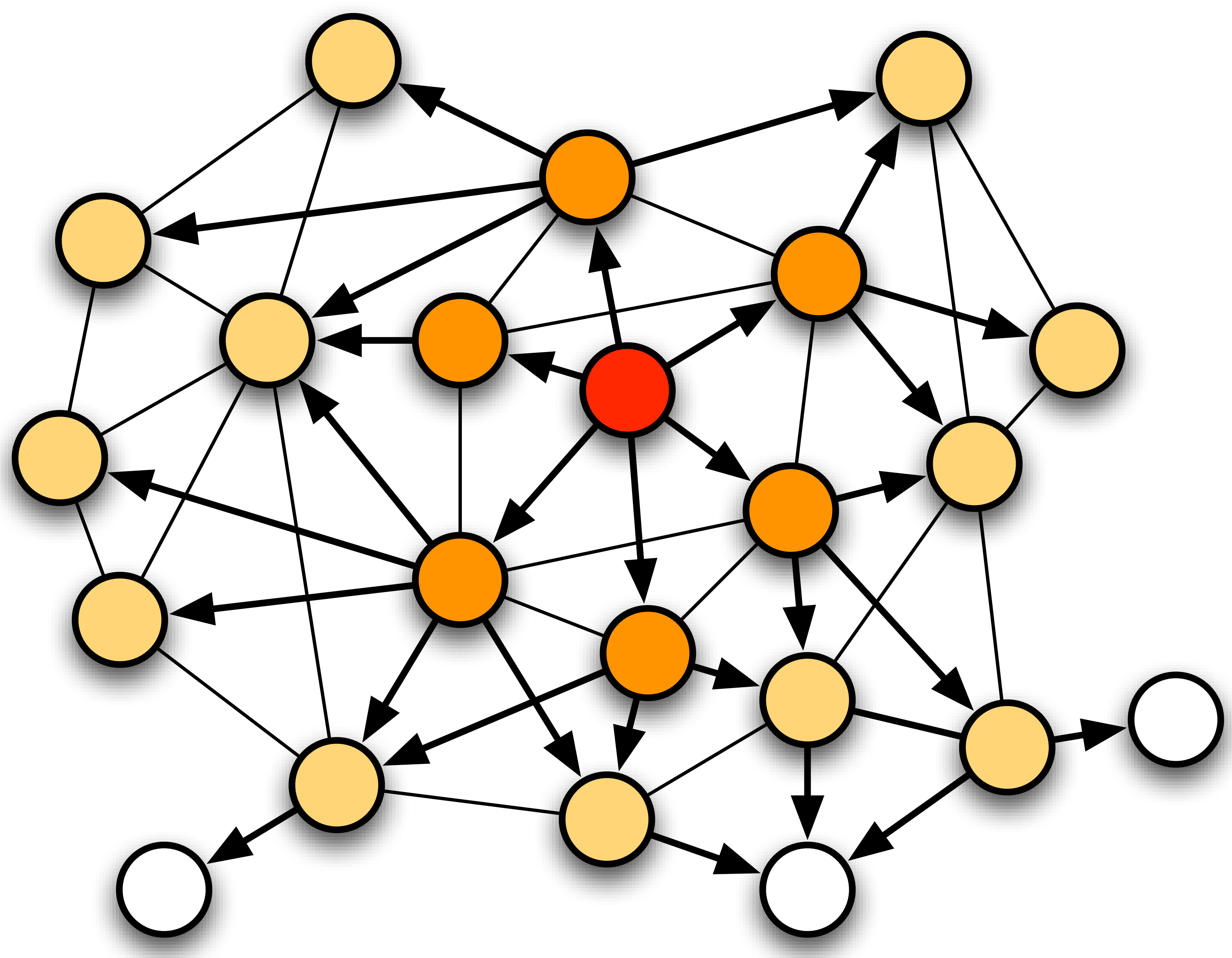
Optimized Link State Routing (OLSR)

- Combines Link-State protocol and topology control
- Topology control
  - Each node chooses a minimal dominating set of the 2 hope neighborhood
    - ***multipoint relays (MPR)***
    - Only these nodes propagate link information
    - More efficient flooding
- Link State component
  - Standard link state algorithm on a reduced network

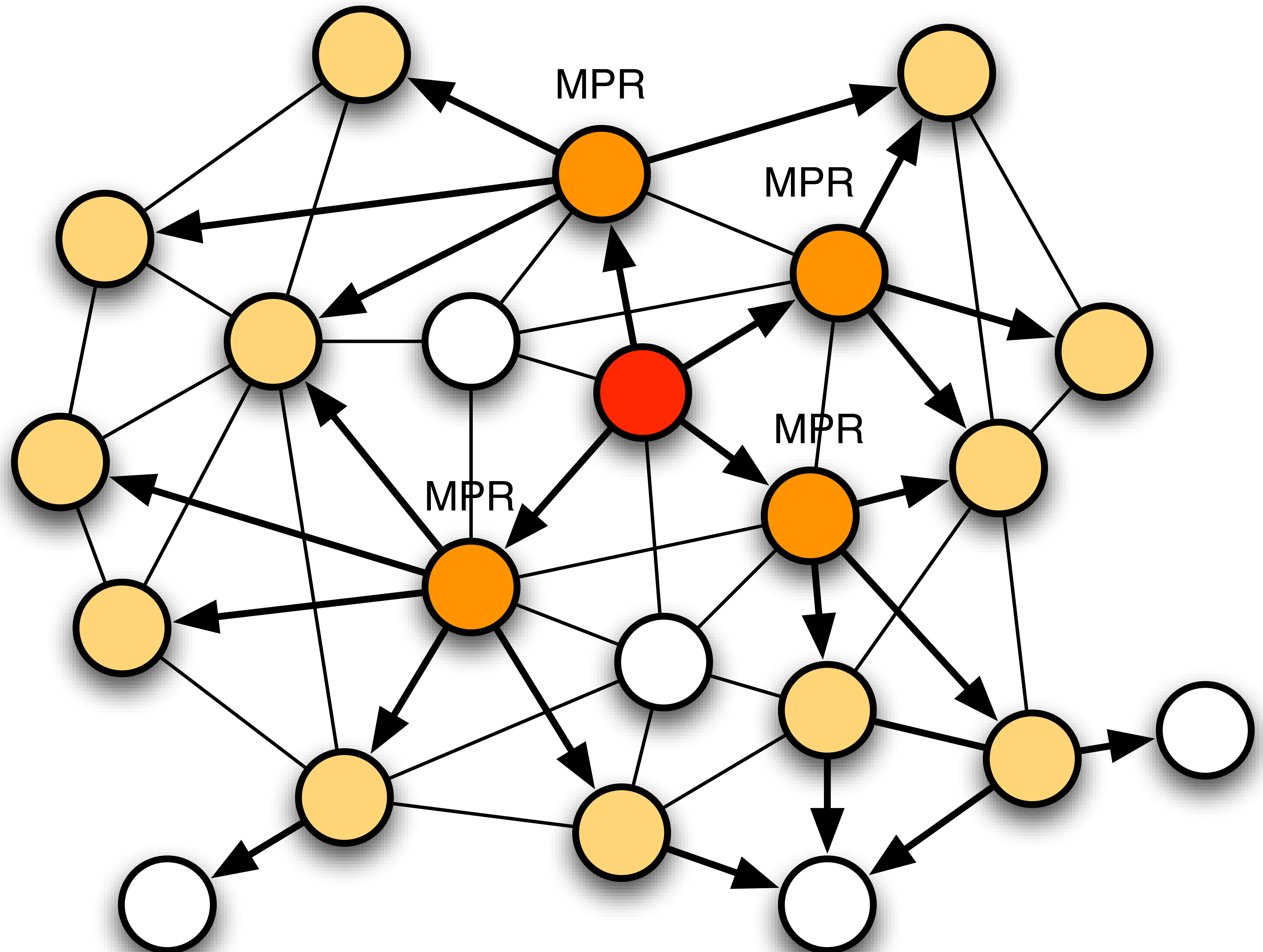
Optimized Link State Routing (OLSR)



Optimized Link State Routing (OLSR)



Optimized Link State Routing (OLSR)



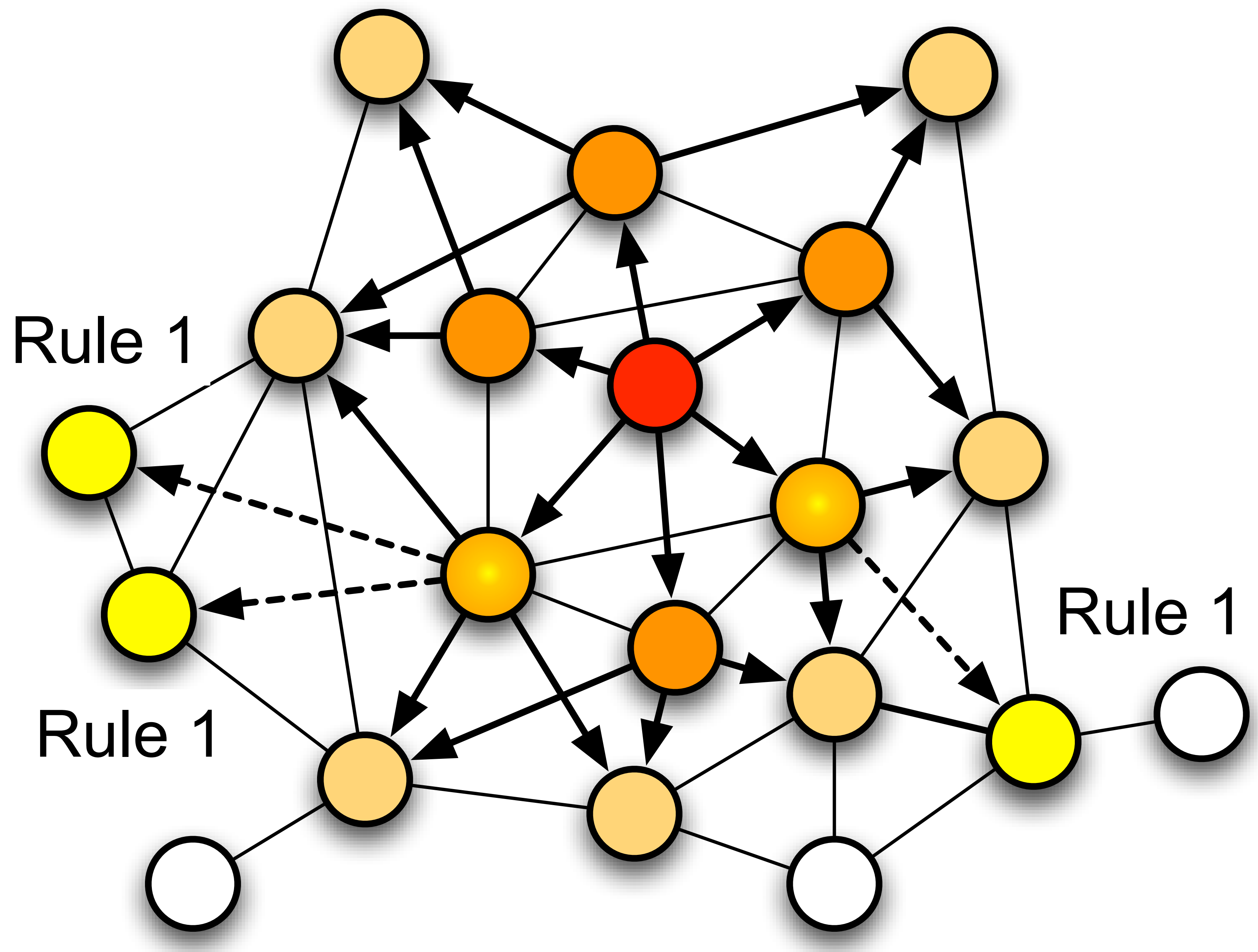
Selection of MPRs

- Multipoint Relaying for Flooding Broadcast Messages in Mobile Wireless Networks, Amir Qayyum, Laurent Viennot, Anis Laouiti, HICCS 2002
- Problem is NP-complete
- Heuristics
  - recommended for OLSR
- Notations
  - N(x): 1 hop neighborhood of x
  - $N^2(x)$: 2 hop neighborhood of x
  - Alle connections are symmetrical

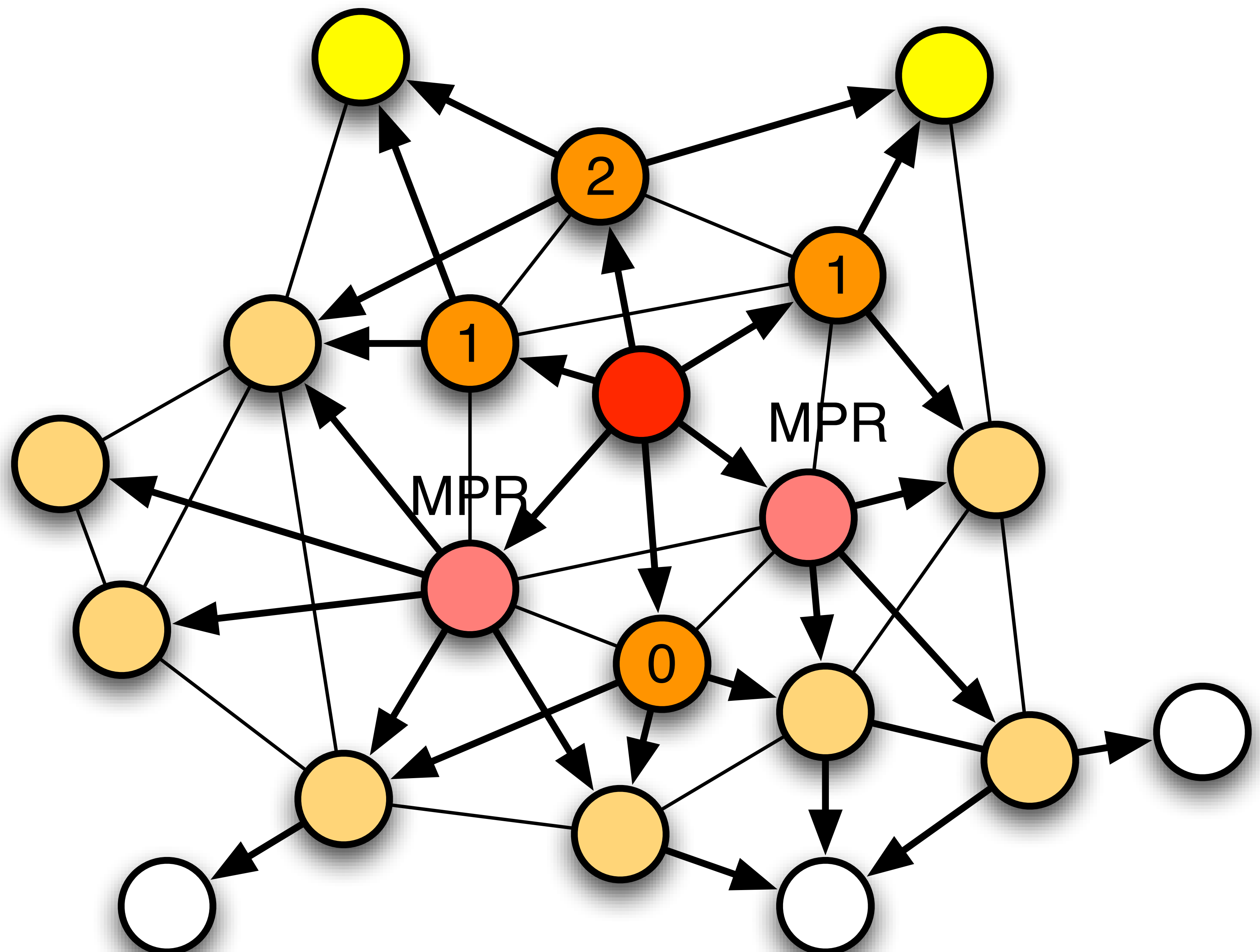
Selection of MPRs

- At the beginning there is no MPR
  - Each node chooses its MPRs
- Rule 1: A node of x is selected as MPR, if
  - it in N(x) and
  - it is the only neighborhood node in the node $N^2(x)$
- Rule 2: If nodes in N^2 (x) are not covered:
  - Compute for each node in N(x) the number of uncovered nodes in $N^2(x)$
  - Select as MPR the node that maximizes the value

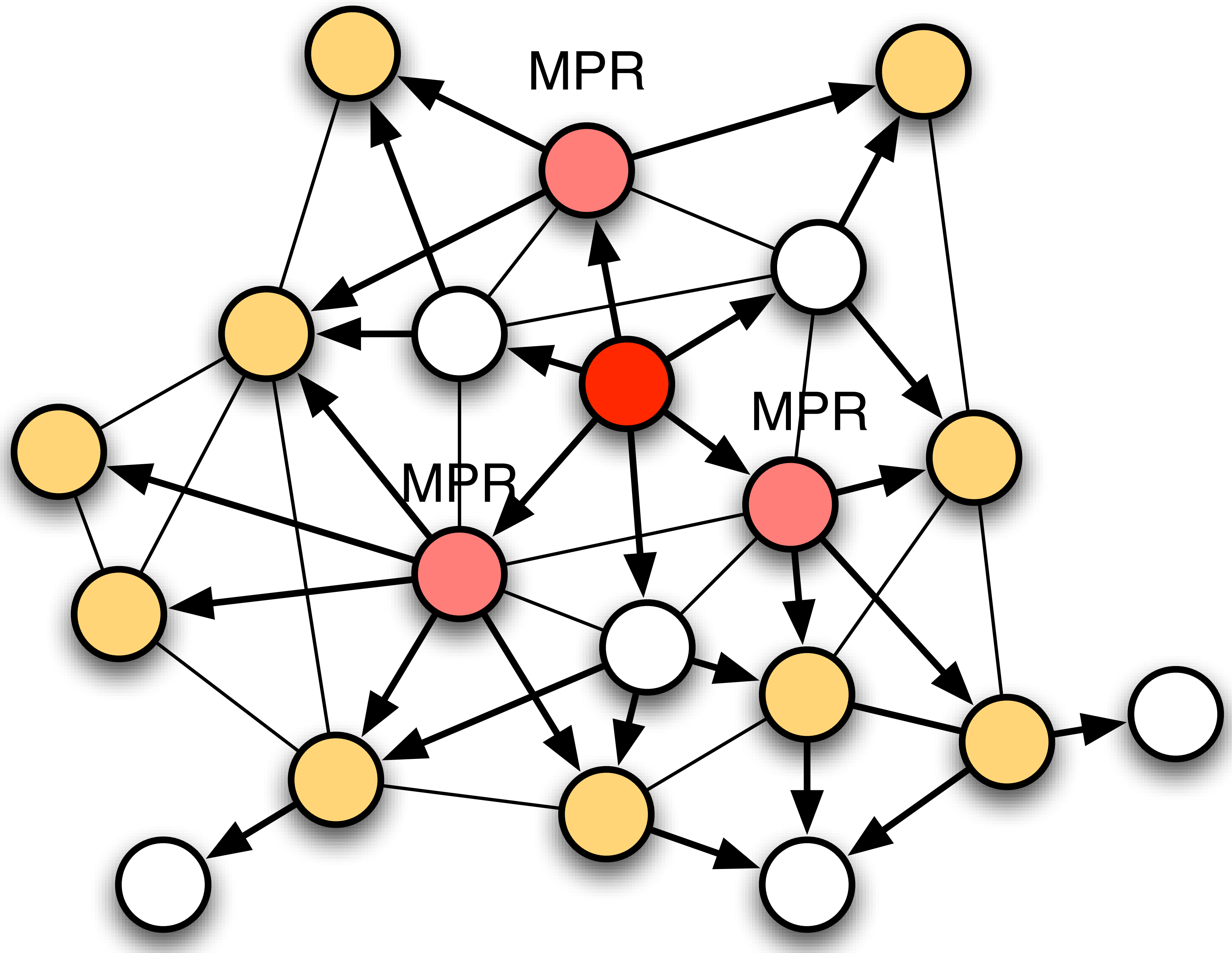
Rule 1



Rule 2



MPRs



CoNe Freiburg

OLSR

- OLSR is flooding link information using MPRs
  - Multipoint-Relays
- Receivers choose their own MPRs for propagating
  - Each node chooses its own MPRs
- Routes use only MPRs as intermediate nodes

Zone Routing Protocol (ZRP)

- Haas 1997
  - *A new routing protocol for the reconfigurable wireless networks*, Proc. of IEEE 6th International Conference on Universal Personal Communications, 562–566
- Zone Routing Protocol combine
  - Proactive protocol
    - for local routing
  - reactive protocol
    - for global routing

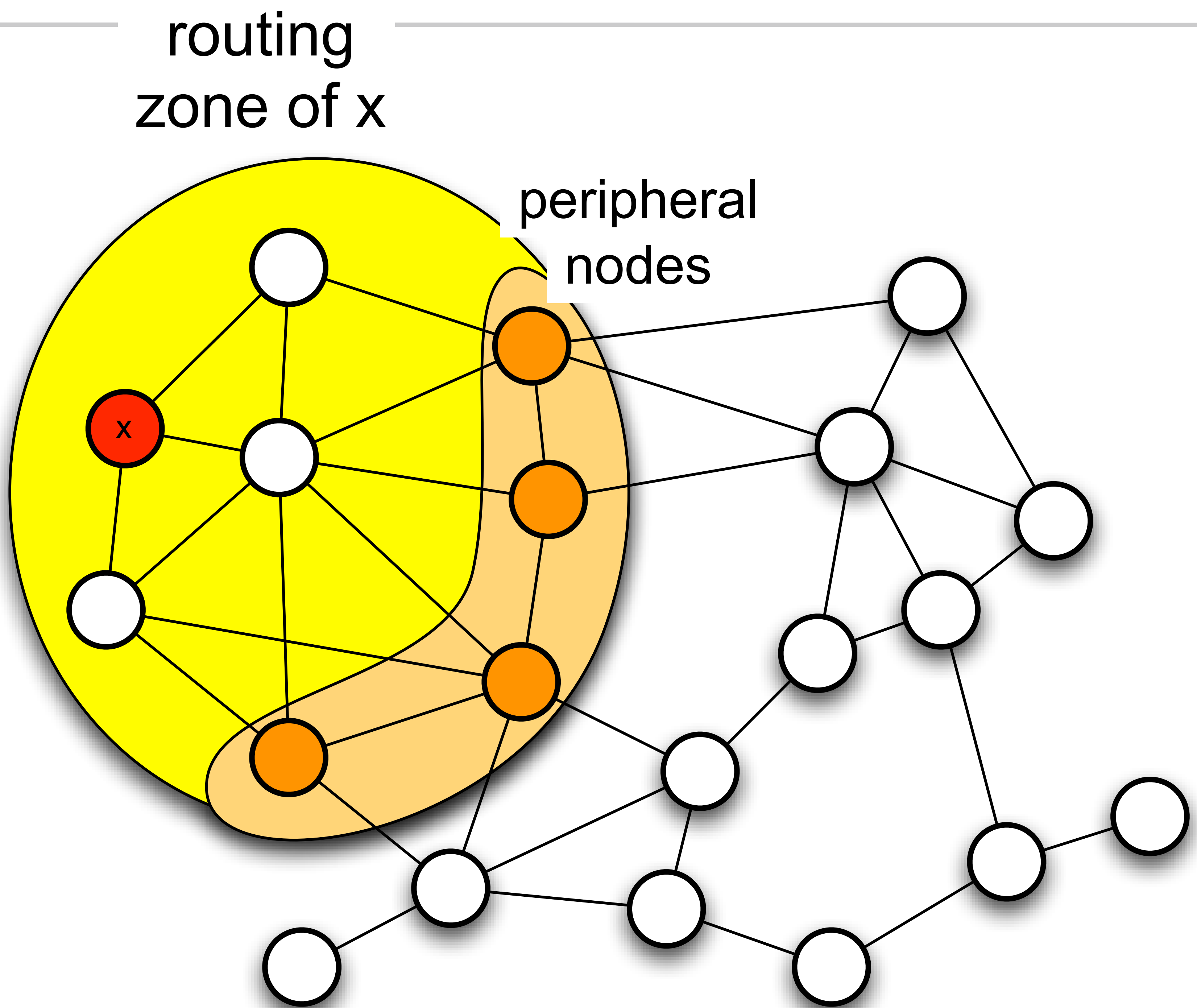
ZRP

- Routing zone of a node x
  - Nodes in a given maximum hop-distance d
- Peripheral nodes
  - all nodes have exactly the hop-distance d
  - within the routing zone x

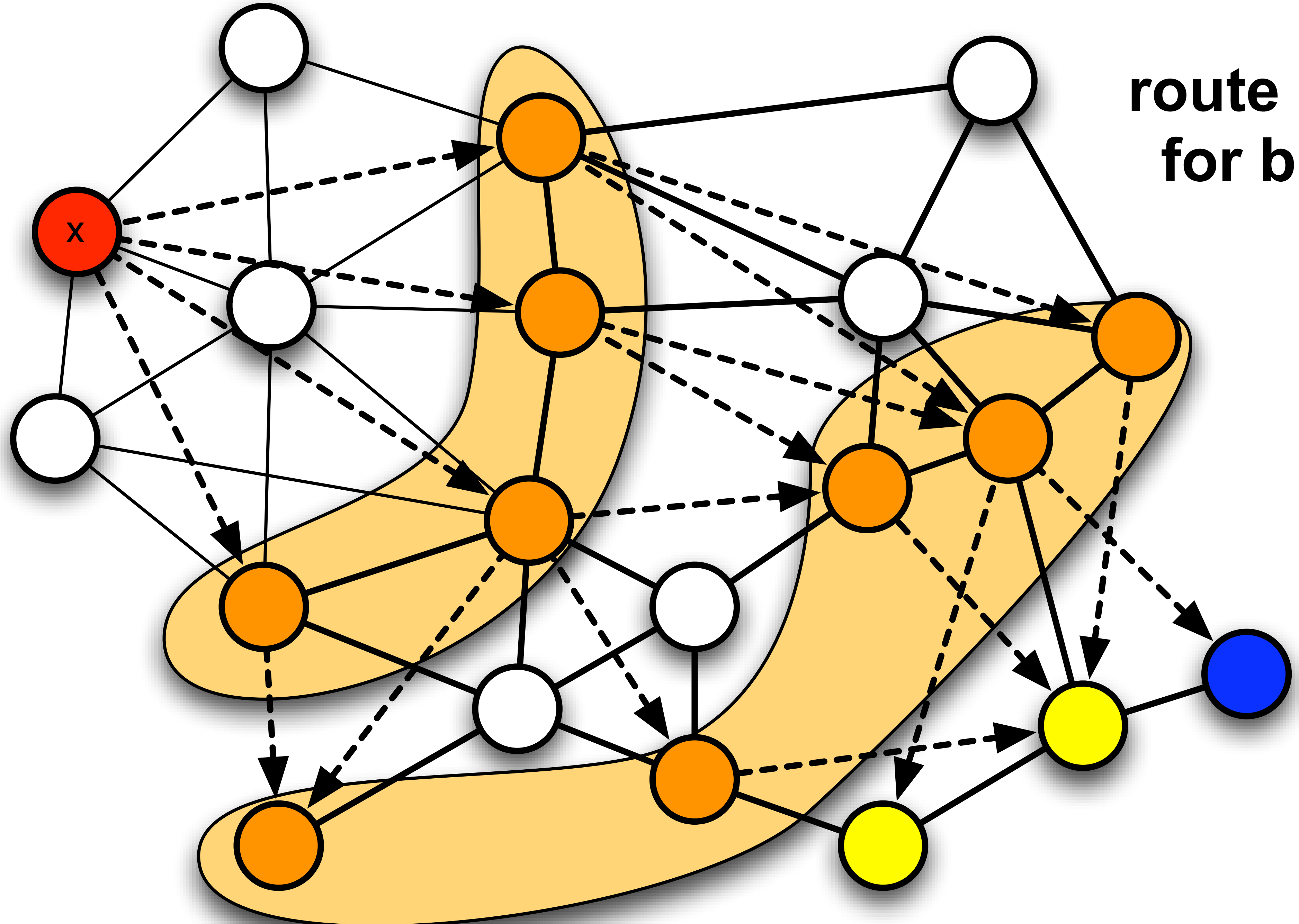
ZRP

- Intra zone routing
  - proactive update the connection information in the routing zone of node
    - e.g. with link state or distance vector protocols
- Inter zone routing
  - Reactive route discovery is used for distant / unknown nodes
  - Procedure similar to DSR
  - Only peripheral nodes reach further information

ZRP: Example with radius d=2

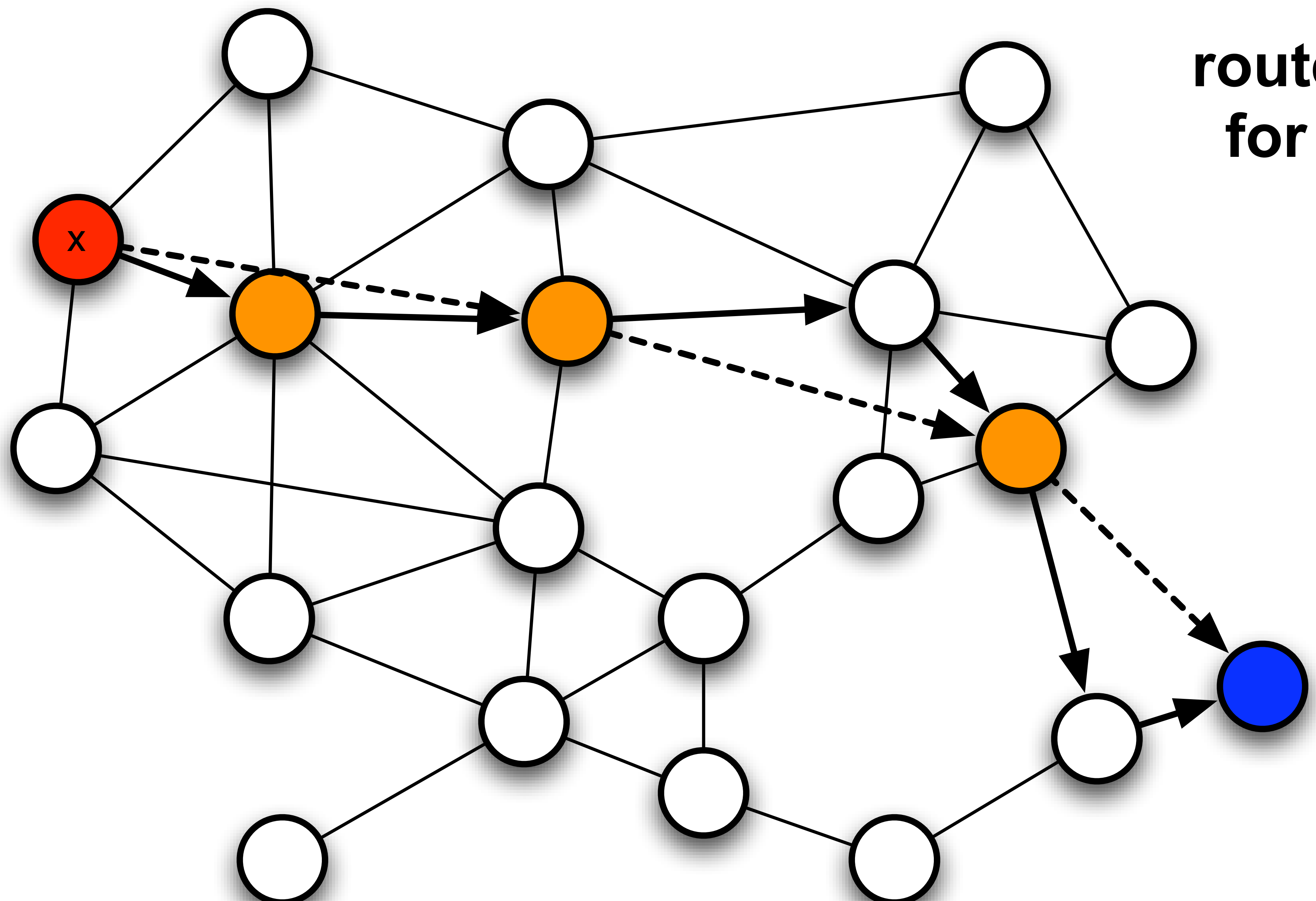


ZRP: Example with radius d=2



route discovery for blue node

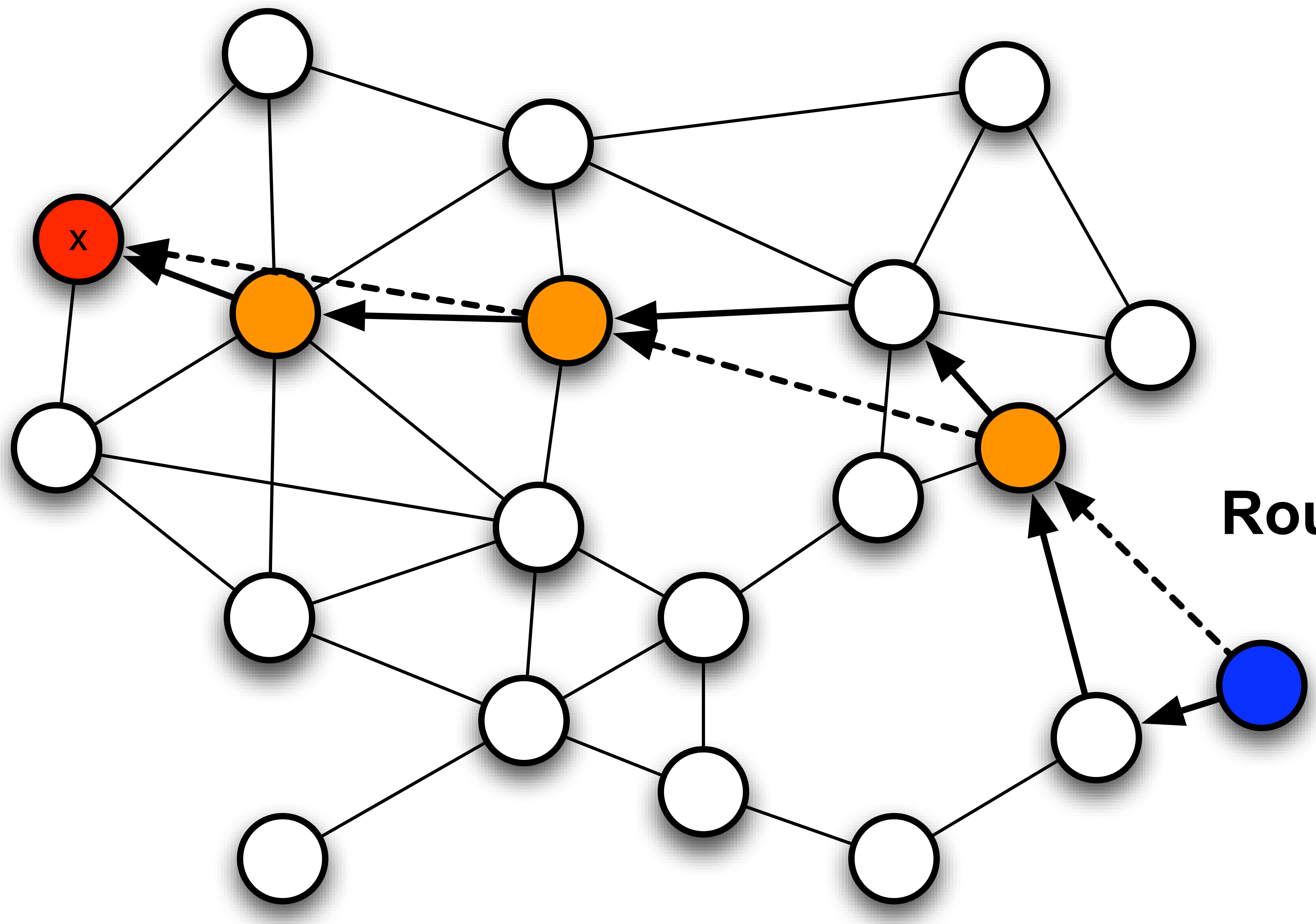
ZRP: Example with radius d=2



route discovery for blue node

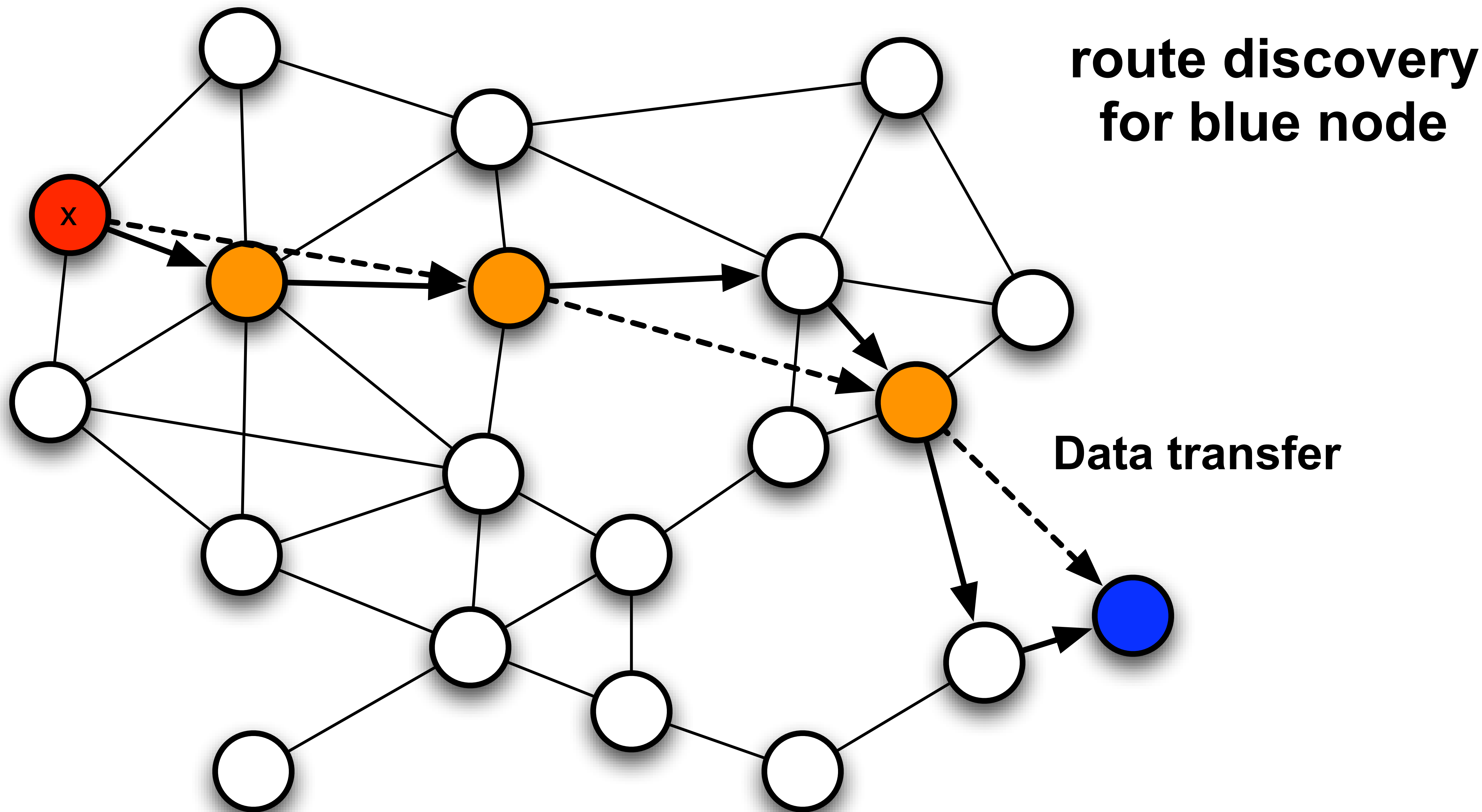
ZRP: Example with radius d=2

route discovery for blue node



Route Reply

ZRP: Example with radius d=2

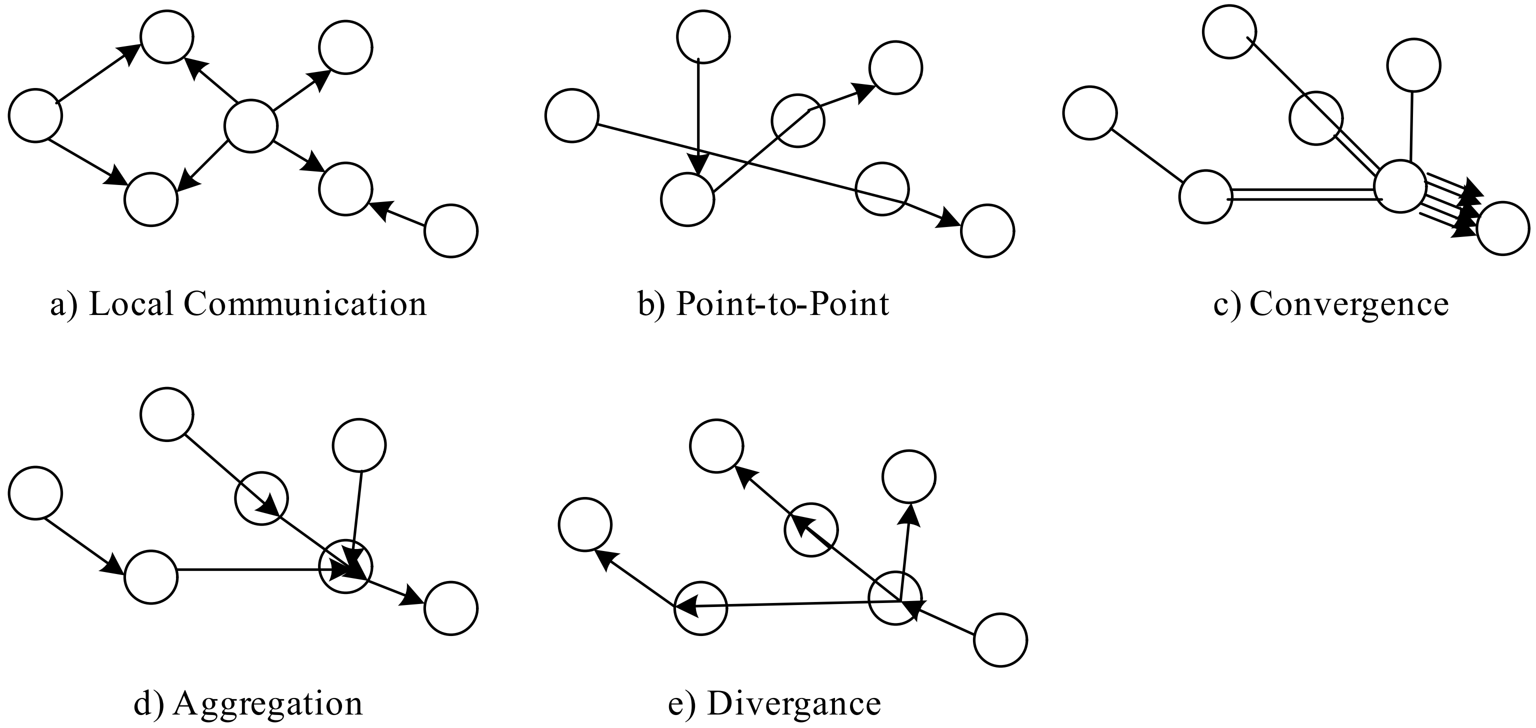


Routing Protocols for WSNs

- Literature
  - From MANET To IETF ROLL Standardization: A Paradigm Shift in WSN Routing Protocols, Watteyne et al, IEEE Communication Survey & Tutorials, Vol. 13, No. 4, 4th Quarter, 2011
  - Routing Protocols in Wireless Sensor Networks: A Survey, Goyal, Tripathy, 2012 Second International Conference on Advanced Computing & Communication Technologies
  - Energy-Efficient Routing Protocols in Wireless Sensor Networks: A Survey, Pantazis et al., IEEE Communication Survey & Tutorials, Vol. 15, No. 2, 2nd Quarter, 2013

Types of Communication

- Single Hop
  - Two participants, sender/receiver, e.g. outdoor temperature sensor
  - Base stations: master/slave, e.g. Bluetooth
  - Many participants, i.e. data mule
- Multihop
  - Local Communication
  - Point-to-Point/Unicast
  - Convergence
  - Aggregation
  - Divergance

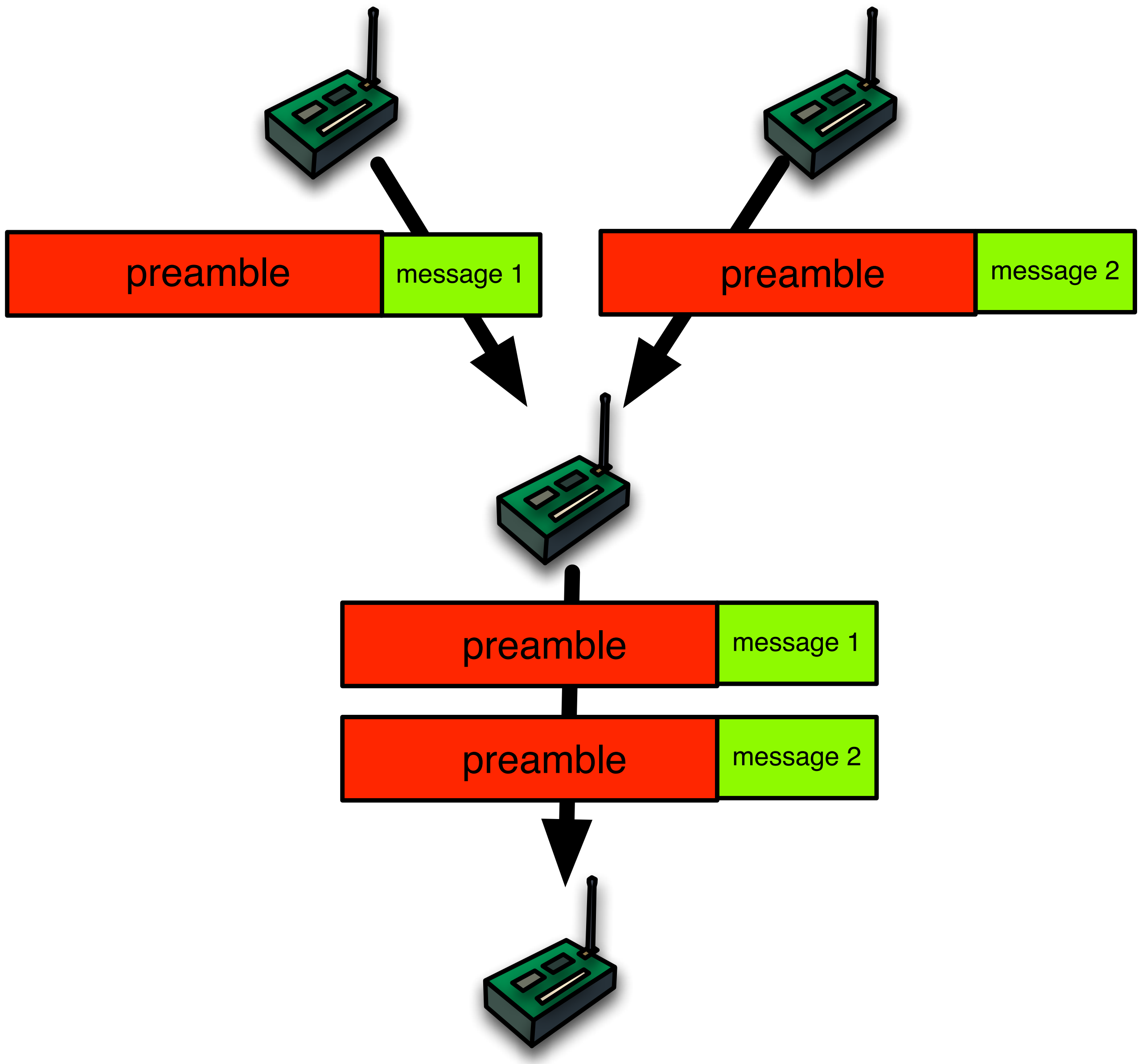


Energy-Efficient Routing Protocols in Wireless Sensor Networks: A Survey, Pantazis et al., IEEE Communication Survey & Tutorials, Vol. 15, No. 2, 2nd Quarter, 2013

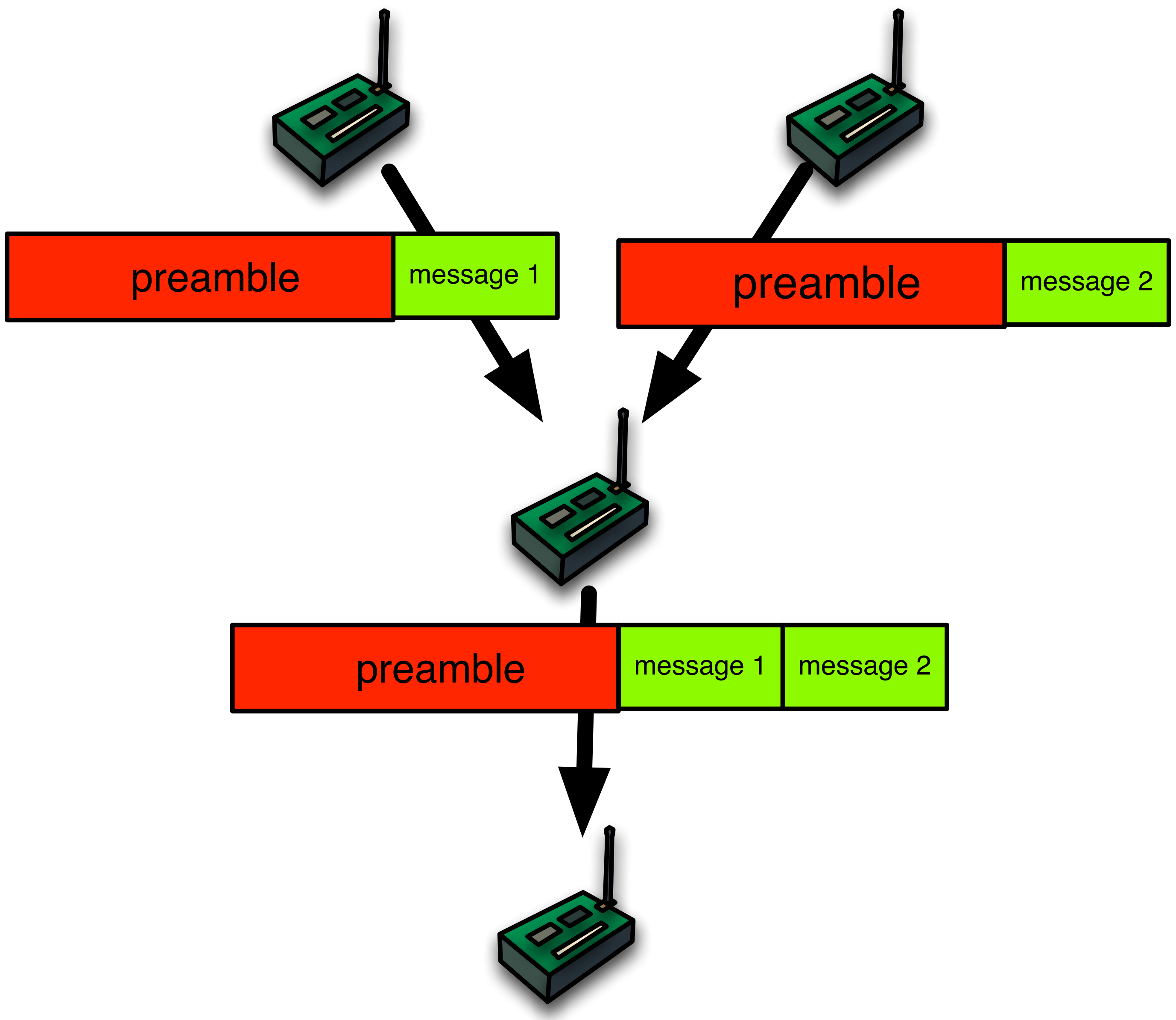
Data Aggregation

- In multi-hop networks combining mesage can improve networking
- Concatenation) of messages
  - overall number of headers is reduced
    - especially for Preamble Sampling
  - smaller costs for collision avoidance
- Recalculation of contents
  - e.g. If the minimum temperature is required, then it satisfies to forward the smallest value
  - For this purpose, collect the input over some time

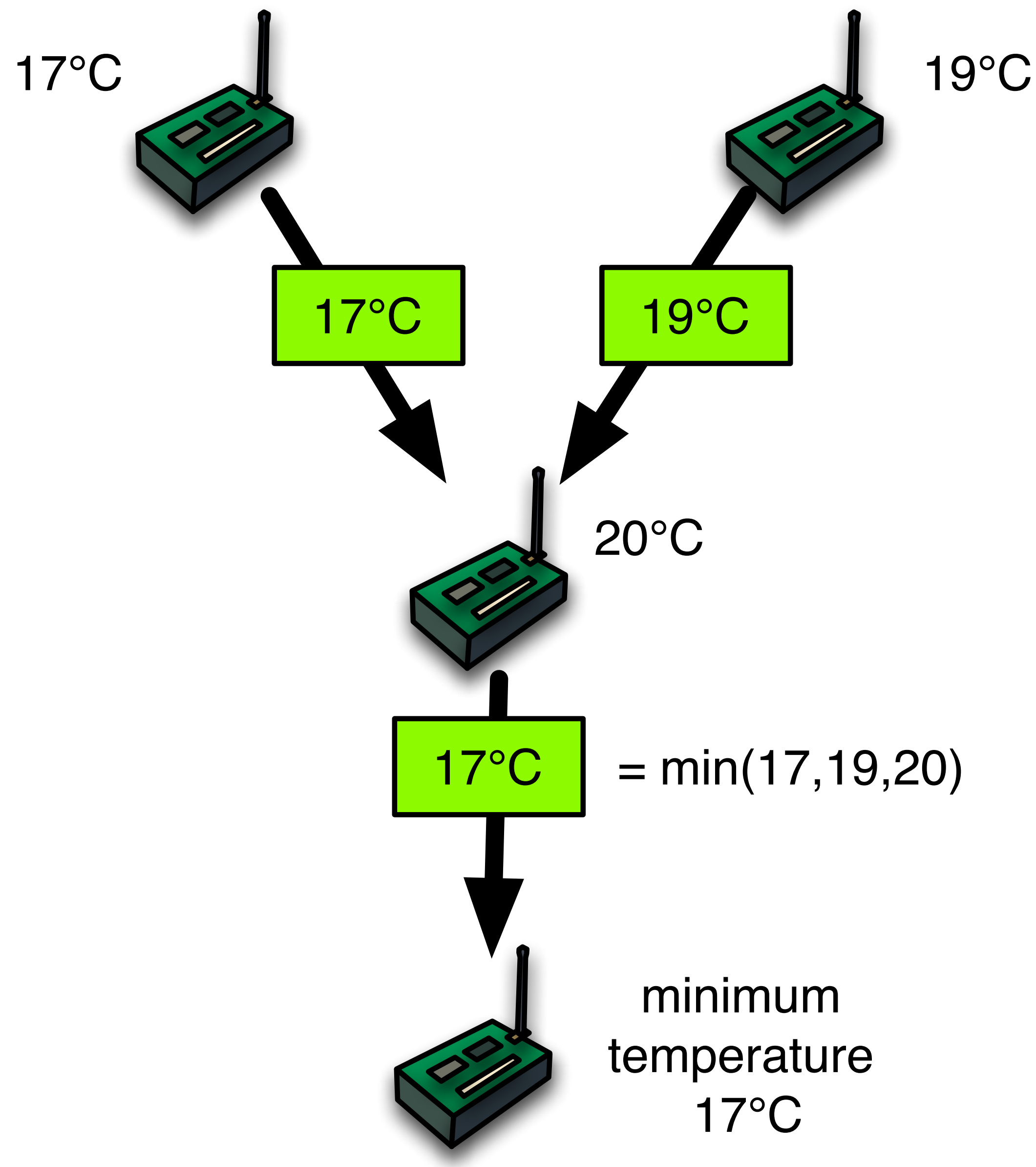
Convergence



Data Aggregation by Concatenation



Real Data Aggregation by Recalculation



Simple Functions for Data Aggregation

- Minimum
  - inner node computes the minimum of input values
- Maximum
  - like Minimum
- Number of sources
  - inner node adds input values
- Sum
  - addition at inner nodes

Aggregable Functions

- Mean
  - compute the number of sensors: n
  - compute the sum of sensor values: S
  - mean = S/n
- Variance
  - Compute average and the average of squares of values
  - $V(X) = E(X^2)-E(X)^2$

Hard Aggregable Functions

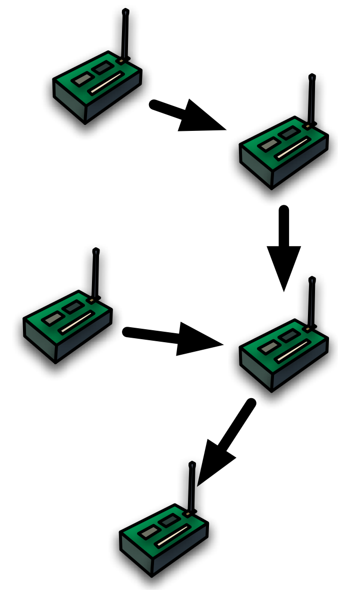
- The following functions cannot be aggregated easily
  - median
  - p-quantile
    - if p is not very small or large
  - number of different values
    - only for large data sets an approximation is possible
- Approximate solution
  - was presented in „Medians and Beyond: New Aggregation Techniques for Sensor Networks, Shrivastava et al. Sensys 04
  - using k words in each message an approximation ratio of log n/k can be achieved

Routing Models for Data Aggregation

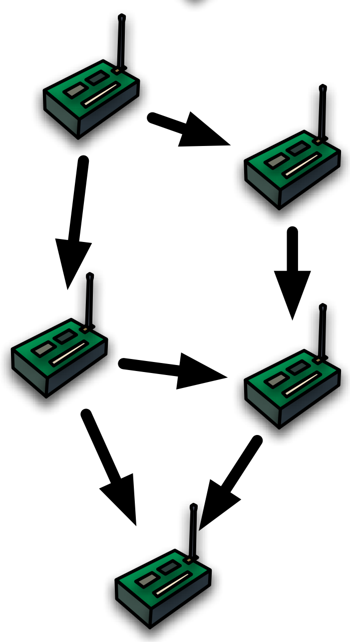
- Address Centric Protocol
  - each sensor sends independently towards the sink
  - not suitable for (real) aggregation
- Data Centric Protocol
  - Forwarding nodes can read and change messages

Communication Graphs for Aggregation

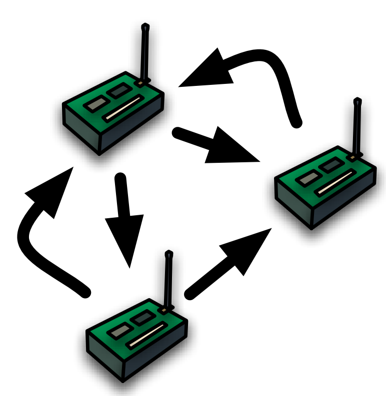
- Tree Structure
  - If there is only a single sink
  - and every source uses only a single path
  - then every communication graph in a WSN is a tree



- DAG (directed acyclic graph)
  - general case
  - caused by changing routing paths to the sink
  - may complicate data aggregation
    - e.g. sum



- General graph
  - Population protocols
  - are not used in WSNs



Probabilistic Counting for Data Aggregation

- Hard problems for Data Aggregation
  - Counting of different elements in a multiset
  - Computation of Median
- Exact computation needs complete knowledge
  - therefore we compute approximations
- Main Technique
  - probabilistic counting
    - „Counting by Coin Tossings“, Philippe Flajolet, ASIAN 2004
  - probabilistic sampling
    - „A note on efficient aggregate queries in sensor networks“, Boaz Patt-Shamir, Theoretical Computer Science 370 (2007) 254–264

Types of WSN Routing

Energy-Efficient Routing Protocols in Wireless Sensor Networks: A Survey, Pantazis et al., IEEE Communication Survey & Tutorials, Vol. 15, No. 2, 2nd Quarter, 2013

- MANET Routing
  - Flooding Based Routing (MANET)
    - Flooding, DSR, AODV, DYMO
  - Cluster-Based Hierarchical Routing
    - Low-Energy Adaptive Clustering Hierarchy (LEACH)
- Geographic Routing
  - Greedy Routing
  - Face Routing
- Self-Organizing Coordinate Systems
  - Inferring Location from Anchor Nodes, Virtual Coordinates
  - Gradient Routing
    - Gradient-Based Routing (GBR)
    - Routing Protocol for Low Power and Lossy Networks (RPL)

Low-energy adaptive clustering hierarchy (LEACH)

- Literature
  - Heinzelman, W., Chandrakasan, A., and Balakrishnan, H., "Energy-Efficient Communication Protocols for Wireless Microsensor Networks", Proceedings of the 33rd Hawaaian International Conference on Systems Science (HICSS), January 2000.
  - Heinzelman, Chandrakasan, Balakrishnan, An Application-Specific Protocol Architecture for Wireless Microsensor Networks, IEEE Transactions on Wireless Communications, Vol. 1, NO. 4, October 2002
- TDMA-based MAC + simple Routing Protocol
- Cluster heads (CH)
  - Randomized, adaptive, self-configuring algorithm
  - use CDMA for communication
- Other nodes
  - communicate only with cluster head using TDMA-MAC
- Application spedific data processing
  - aggregation, compression
- Two-hop-Routing
  - Nodes to CH, CH to base station
  - Minimum energy routing

Adaptive versus Static Clustering

- Cluster members transmit to a cluster head
- Cluster head
  - transmits to the sink
  - Cluster heads are energy intensive
  - are the first to die
- LEACH
  - nodes self-elect to become cluster heads
  - Cluster-heads data from their surrounding nodes and pass it on to the base station
  - is dynamic because the job of cluster-head rotates

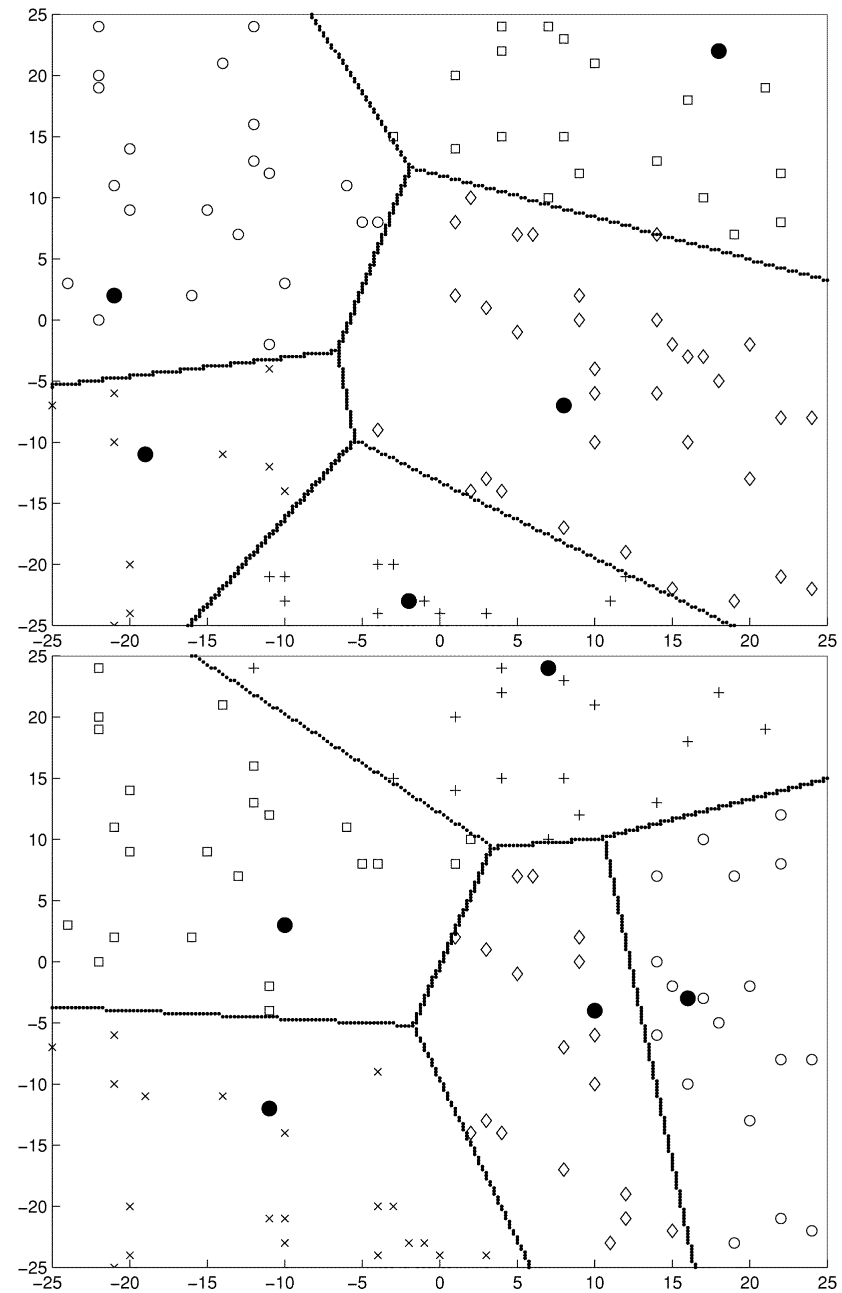


Fig. 3. Dynamic cluster formation during two different rounds of LEACH. All nodes marked with a given symbol belong to the same cluster, and the cluster head nodes are marked with •.

LEACH Protocol

- Steps
  - Cluster Head Selection
    - probabilistic or
    - central (LEACH-C) by base station
  - Cluster Formation
  - Steady State Phase
- Assumptions
  - All nodes can reach the base station (BS)
  - Short transmission ranges can save energy
    - energy path loss ~ d^2

LEACH: Cluster Head Selection Algorithm

- Given
  - k: number of desired cluster heads
  - n: number of nodes
  - p = k/n desired fraction of nodes
    - such that 1/p is a natural number
  - t: round number
  - $t_0 = t - (t \bmod 1/p)$
- Choose randomly $r \in [0,1]$
- In each round compute T(t) : $T(t) = \dfrac{p}{1 - p(t \bmod \lceil \frac{1}{p} \rceil)}$
  - probability that a node i elects itself to become a cluster head
- If (r < T(t)) and
  (node has not been a cluster head in the last 1/p rounds) then
  - Select node as cluster head for round r

LEACH: Cluster Head Selection Algorithm

LEACH: Cluster Formation Algorithm

- Cluster Heads broadcasts an advertisement message using CSMA
- Based on RSSI (received signal strength indicator)
  - each non-cluster node determine its cluster head for this round
- Each non-cluster head transits a join-request message
  - using CSMA
- Cluster head node sets up a TDMA schedule for data transmission within the cluster
  - prevents collision
  - energy conservation for non-cluster-heads

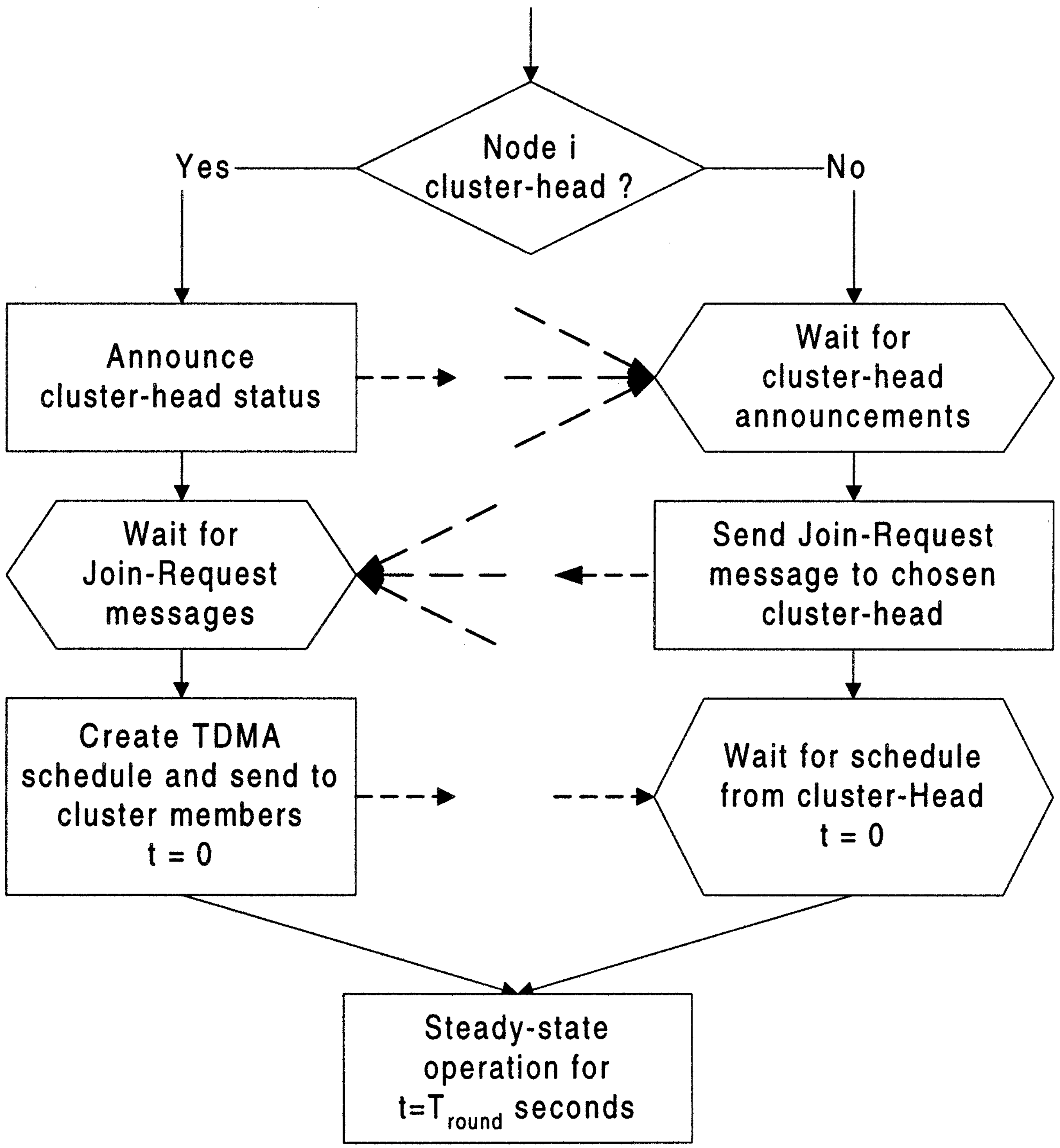
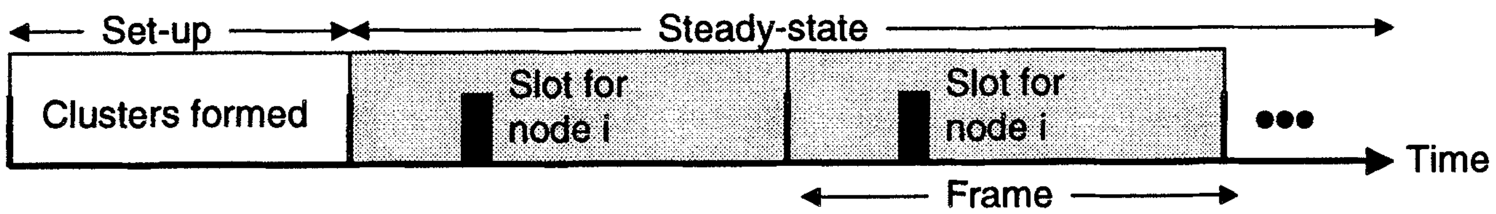


Fig. 2. Flowchart of the distributed cluster formation algorithm for LEACH.

LEACH: Steady State Phase



- Assumptions
  - Setup phase stars at the same time
  - BS sends out synchronized pulses to the nodes
  - Cluster heads are awake all the time
- To reduce inter-cluster interference, each cluster communicates using direct-sequence spread spectrum
- Data is sent from the cluster head to the base station using CDMA

LEACH: Optimal number of clusters

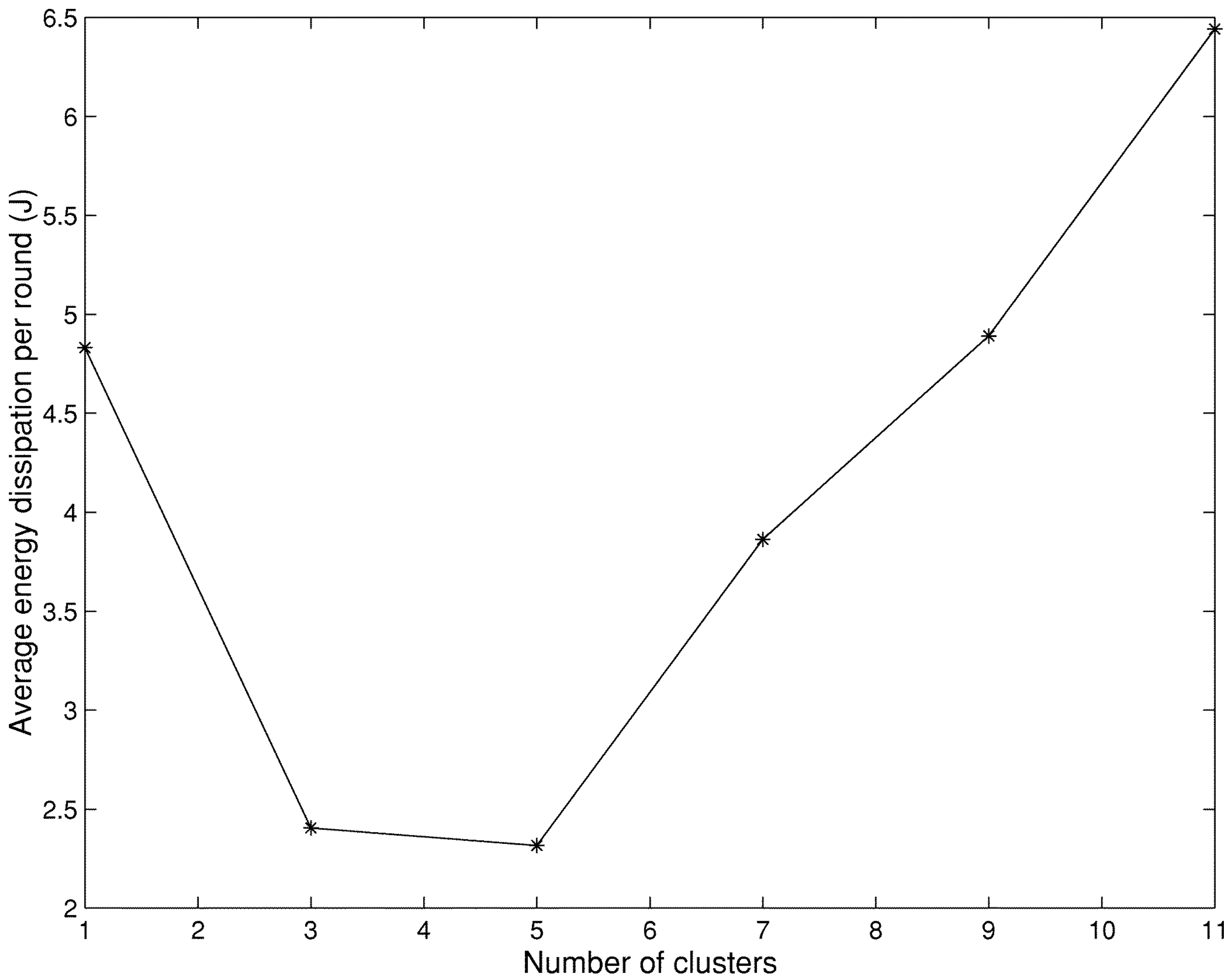


Fig. 6. Average energy dissipated per round in LEACH as the number of clusters is varied between 1 and 11. This graph shows that LEACH is most energy efficient when there are between 3 and 5 clusters in the 100-node network, as predicted by the analysis.

CoNe Freiburg

LEACH-C

- Base station cluster formation
- Use a central control algorithm to form clusters
  - During setup phase each node sends its location and energy level to the base station
  - base station assigns cluster heads and cluster
  - base station broadcasts this information
  - steady-state phase is same as LEACH

ALBERT-LUDWIGS-UNIVERSITÄT FREIBURG

Algorithms for Radio Networks

Routing

University of Freiburg
Technical Faculty
Computer Networks and Telematics
Christian Schindelhauer

CoNe Freiburg

IIF INSTITUT FÜR INFORMATIK FREIBURG