



Internet of Things

Thomas C. Schmidt

t.schmidt@haw-hamburg.de

HAW Hamburg, Dept. Informatik



Agenda

- 🕒 The Internet of Things
 - ➡ Motivation and Use Cases
- 🕒 IoT on Wireless Link Layers
- 🕒 IP in the Internet of Things
- 🕒 Mobile Ad Hoc Routing in the Internet of Things



What is the Internet of Things?

A system in which objects in the physical world can be connected to the Internet by sensors and actuators (coined 1999 by Kevin Ashton)

Key aspects:

- E2E communication via Internet standards
- Machine-to-machine communication
- Embedded devices, often constrained and on battery
- Typically without user interface
- Very large multiplicities, w/o manual maintenance



IoT: Connecting the Physical World to the Internet



Industrial
Automation



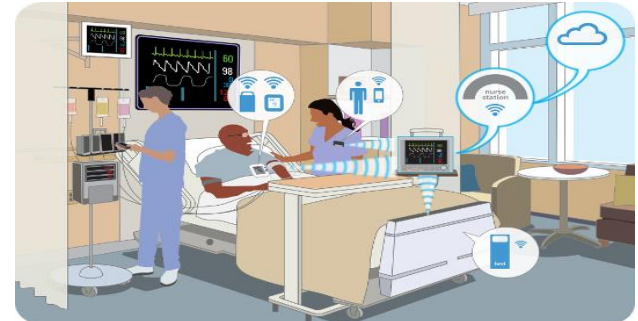
Micro- & Nano
Satellites



Connected Vehicles



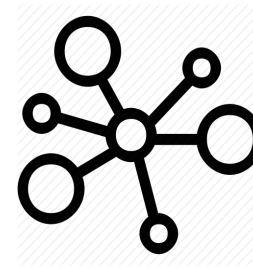
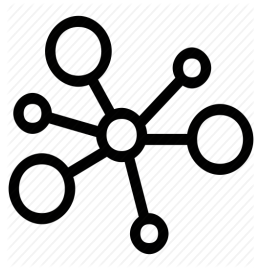
Smart Homes



eHealth



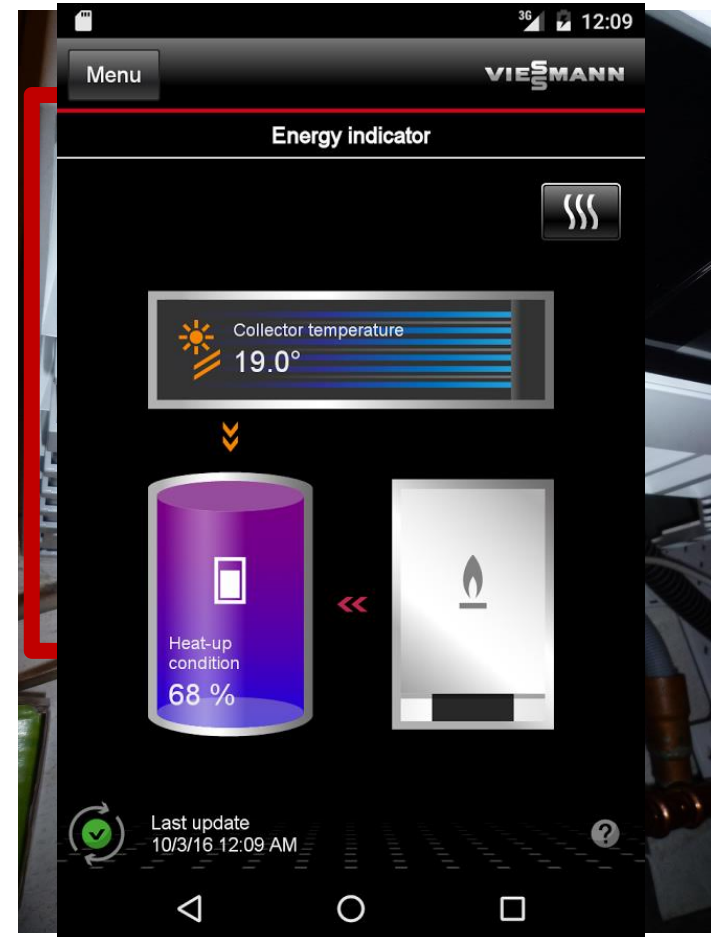
Use Case: Security in Harsh Industrial Environments



Smart DOM Hamburg



„Smart“ Heating



Evolution Towards an IoT

Distributed local intelligence

Embedded
Controllers

Wireless sensor network

Wireless
Networking

Internet of Things ?

IPv4 Uplink
to the Cloud

+

+



This is not yet an Internet of Things!



No Internet without Open Speech and Open Standards



Application

Transport

Network

Link

XHTML XDI CBOR RDF
 JSON Telnet
 CoAP HTTP XMPP

TCP UDP
 TLS/SSL

OSPF RPL DHCP BGP
 OLSR IPv6 SLAAC IPv4

IEEE802.15.4 LoRa BLE
 Ethernet

Evolution towards an *Internet oT*

Distributed local intelligence

Embedded Controllers

Wireless sensor network

Wireless Networking

Hype-Internet of Things

IPv4 Uplink to the Cloud

+

+

+

Interoperable Information

+

Distributed Security

+

Things loosely joined by IPv6

The Real Internet of Things (C. Bormann)



The many faces of IoT

High-end IoT



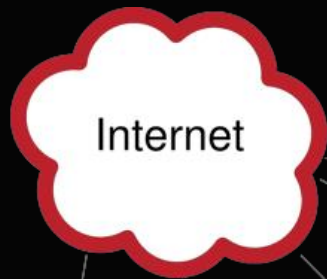
Processor: GHz, 32/64 Bit
Memory: M/Gbytes
Energy: Watt
Network access: 5G, WLAN

Low-end (or constrained) IoT



Processor: MHz, 8/16/32 Bit
Memory: kbytes
Energy: MWatt
Network access: 802.15.4, BLE

The Internet (as we know it)



Memory ~ 500 MB



Memory ~ 1 GB



Various hardware, but more importantly:

- Open access specs
 - interoperability
- Open source:
 - OS + protocol implementations
 - Share dev load, accelerate innovation



Memory > 4GB



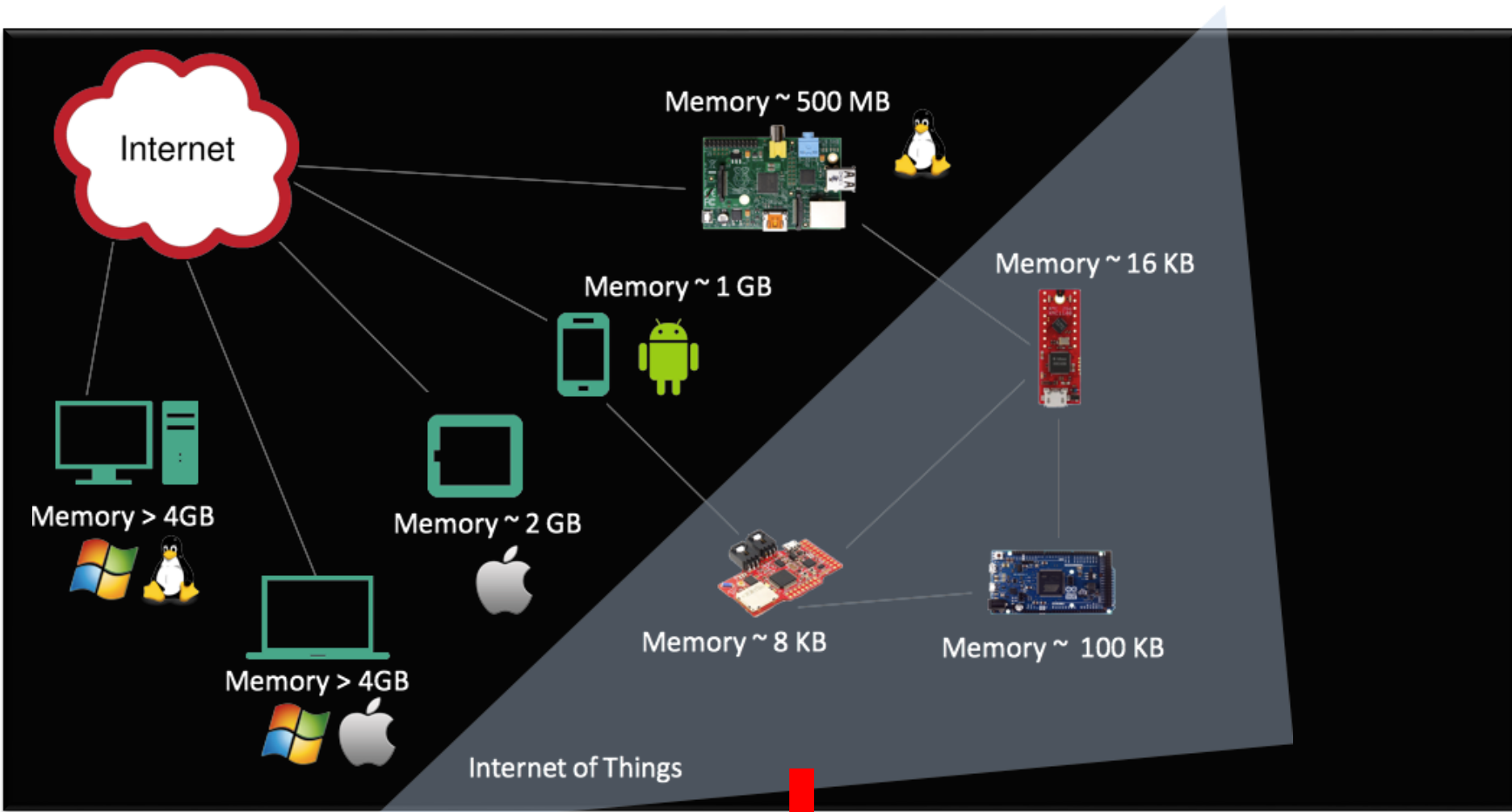
Memory ~ 2 GB



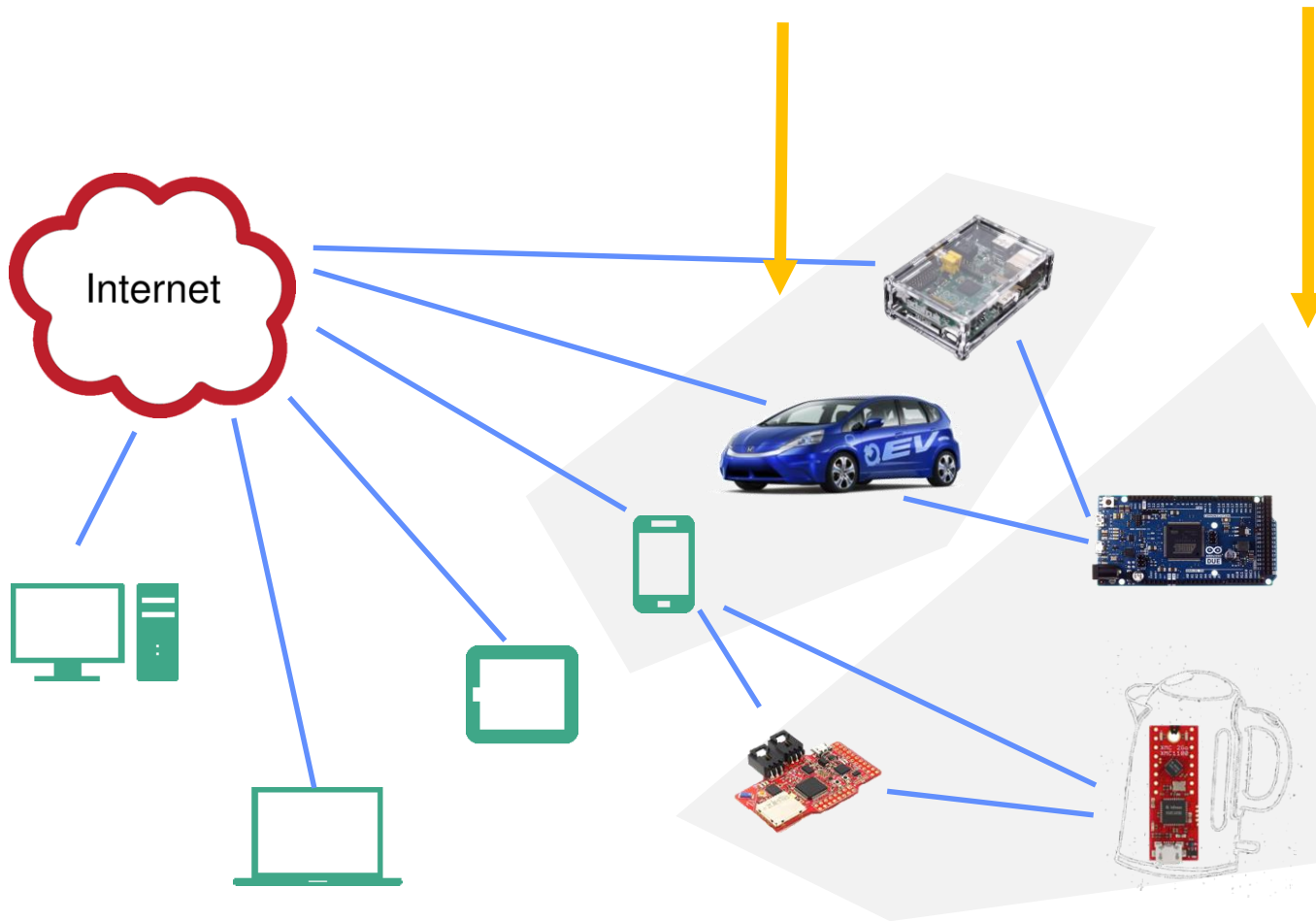
Memory > 4GB



The Internet of Things (IoT)



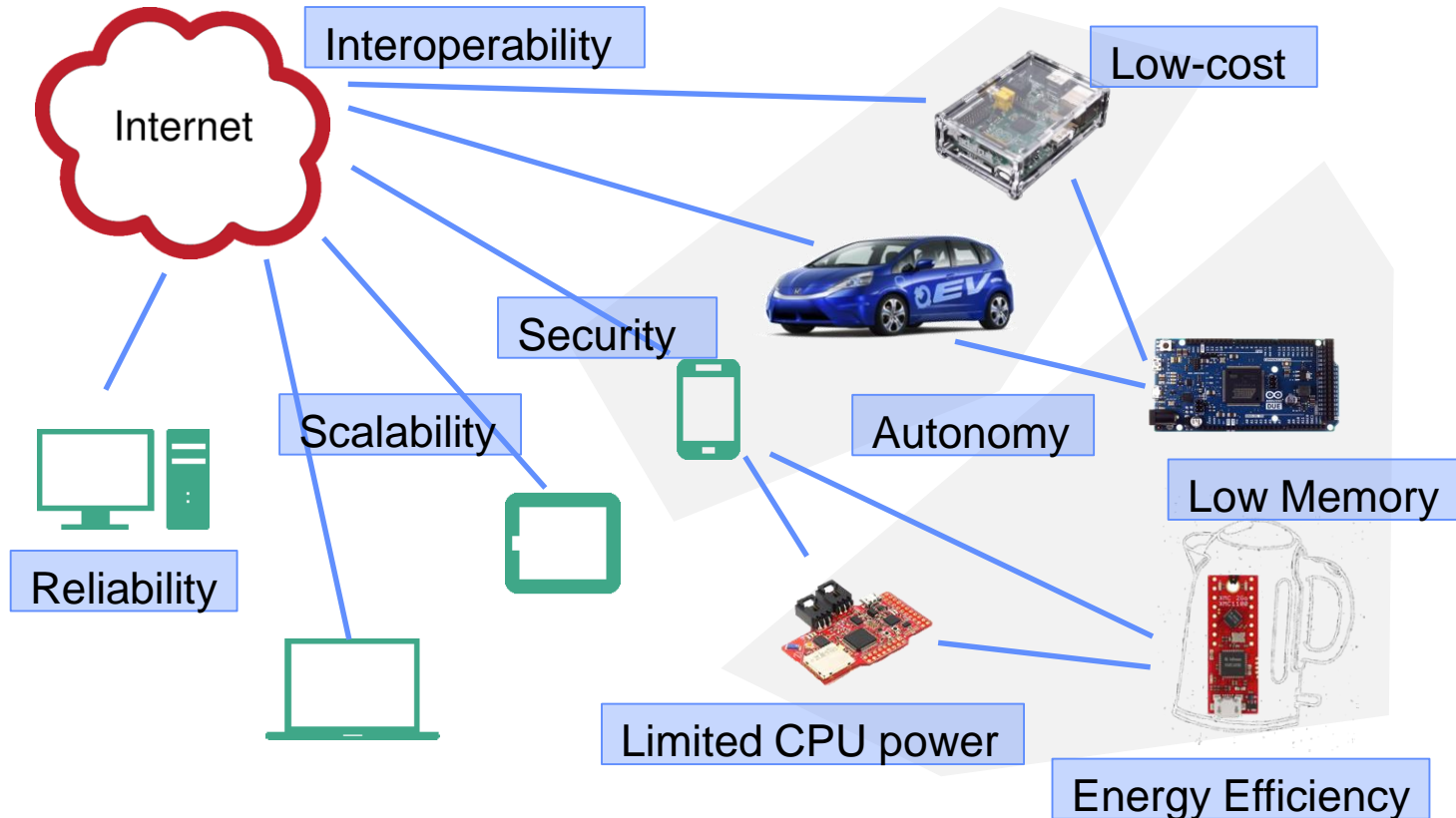
IoT Devices: High-end vs Low-end



C.Bormann et al.
"RFC 7228:
Terminology for
Constrained-Node
Networks,"
IETF, May 2014.



IoT Requirements

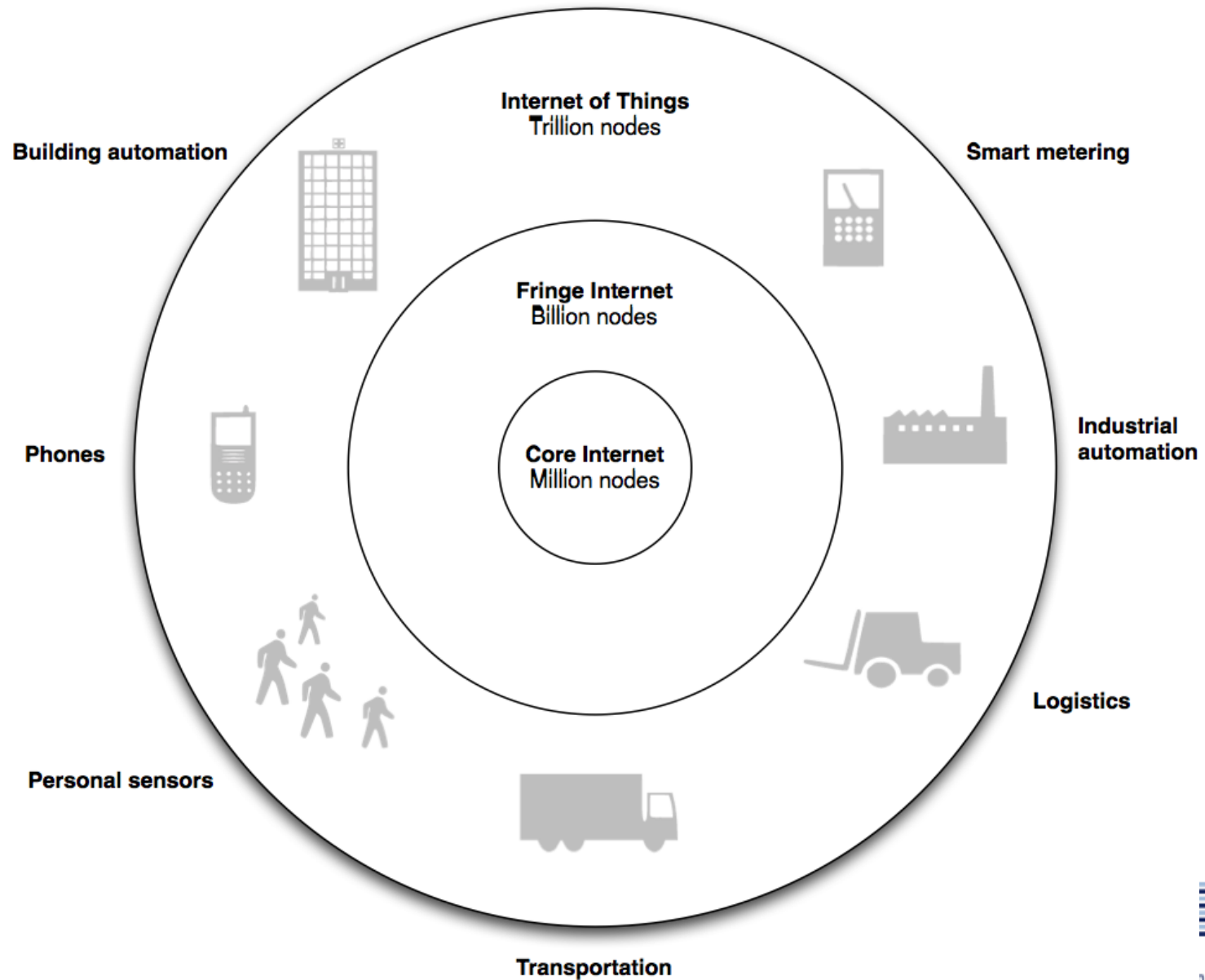


IoT Key Challenges

Five key areas according to ISOC:

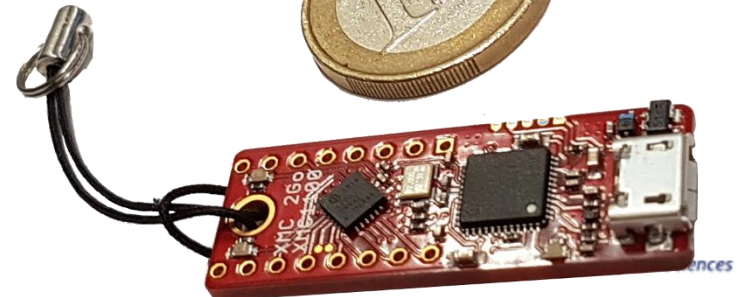
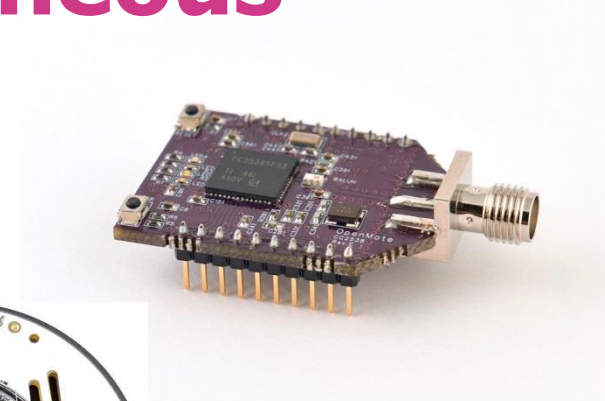
1. Security
2. Privacy
3. Interoperability and standards
4. Legal, regulatory, and rights
5. Emerging economies and development





The IoT is Very Heterogeneous

- o Various boards
- o A zoo of components
- o Broad range of radios
- o Different Link-layers
- o Competing network layers
- o Diverging interests and technologies
- o A lot of experimentation ...

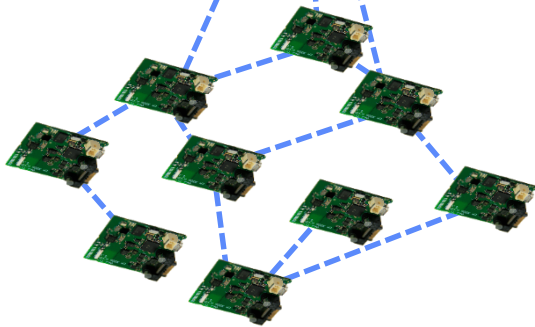


IoT Applications

- o Facility, Building and Home Automation
- o SmartCities & SmartGrids
- o Personal Sports & Entertainment
- o Healthcare and Wellbeing
- o Asset Management
- o Advanced Metering Infrastructures
- o Environmental Monitoring
- o Security and Safety
- o Industrial Automation



IoT Use Cases



Nature Monitoring

Intermittent connectivity



Industry 4.0



Micro Satellites



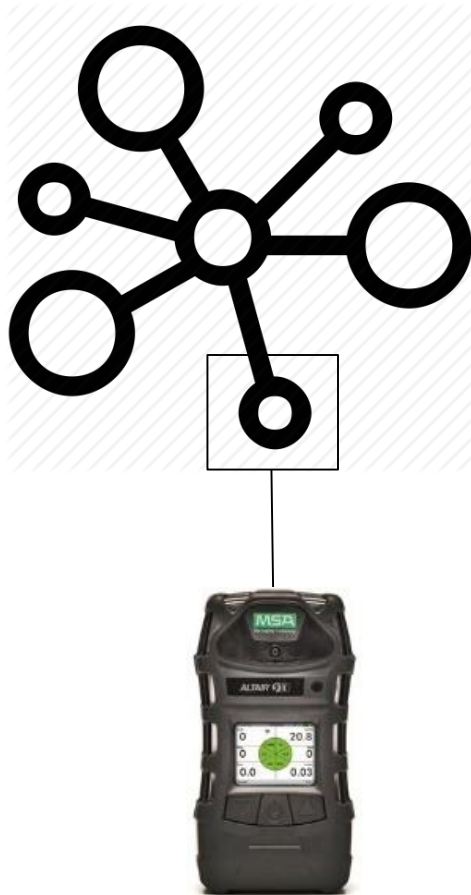
Use Case Safety Monitoring

Workers in industrial process plants

- Perform maintenance in safety-critical environments
- Dangerous events may occur at any time
 - exposure to toxic/combustible gases
 - oxygen depletion in confined spaces
 - gas leaks/sudden outbursts of fire
- Continuous recording of sensor data required



Technical Setting



- o Body sensors
 - IoT controller
- o Protocols
 - Alarm
 - Mission log
 - Configuration
 - Management
- o Communication via border gateway to cloud
 - **Mobility**
 - **Intermittent connectivity**

Agenda

- 🕒 The Internet of Things
- 🕒 IoT on Wireless Link Layers
 - ➡ Excursion to the World of Wireless
 - ➡ Low Power Lossy Links
- 🕒 IP in the Internet of Things
- 🕒 Mobile Ad Hoc Routing in the Internet of Things

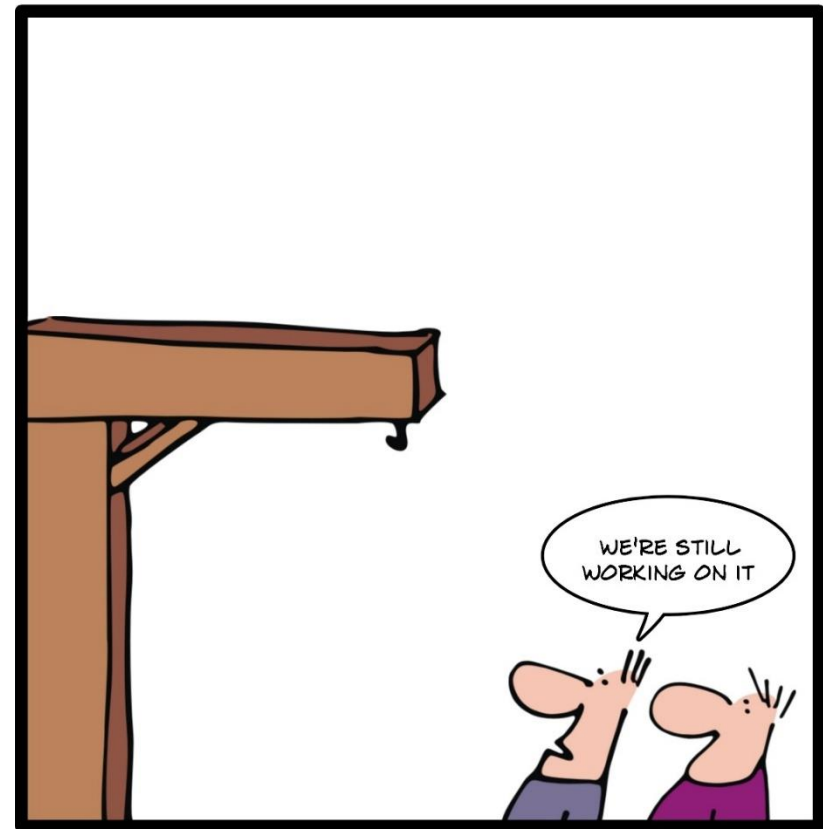


Mobile Wireless Networks

Two scenarios:

1. Mobile users with roaming infrastructure
→ Mobile IP(v6)
2. Spontaneous networks of (autonomous) edge devices
→ the IoT scenario

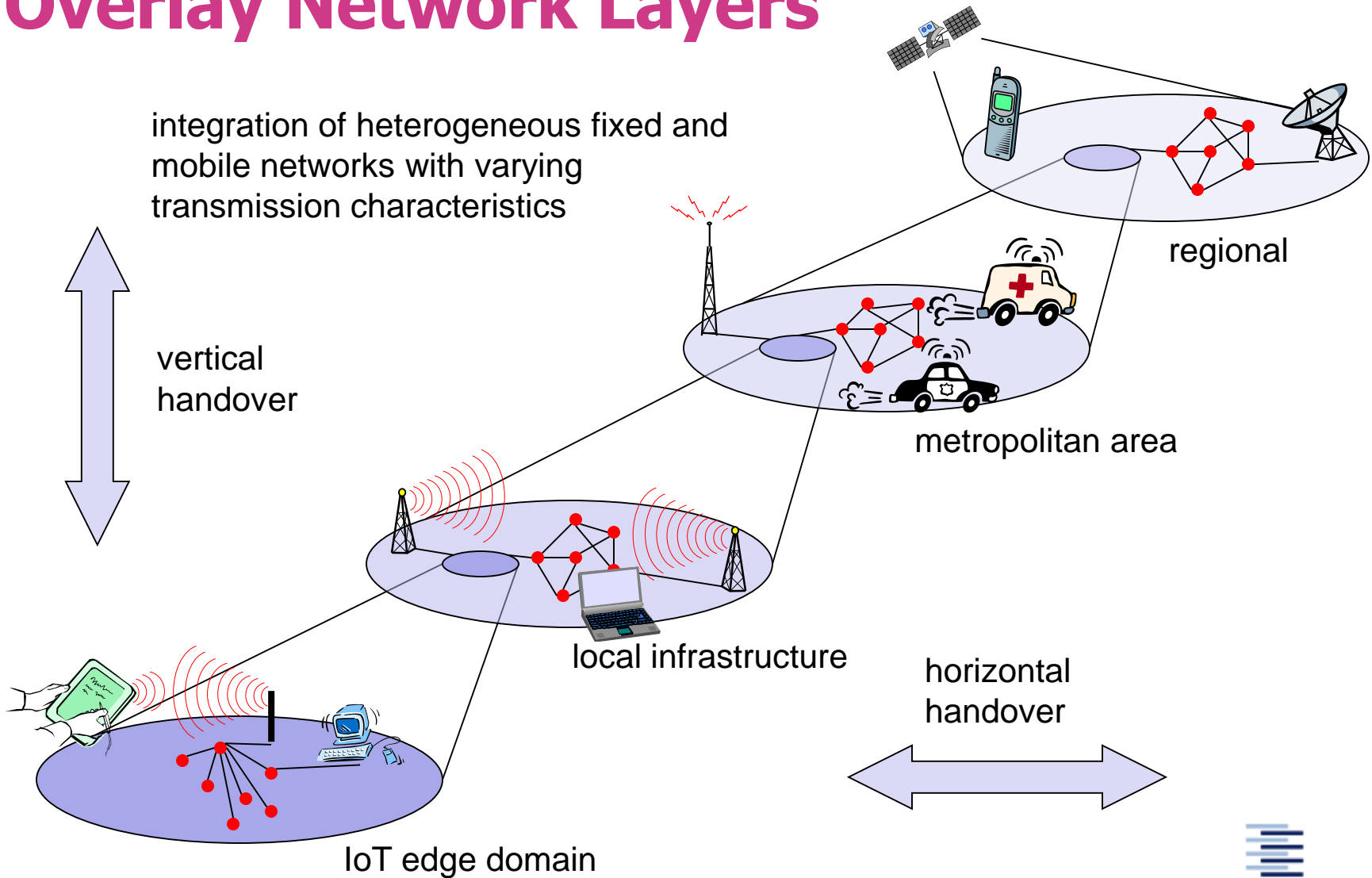
THE HISTORY OF WIRELESS



LONDON 1783:
THE FIRST PROTOTYPE OF THE WIRELESS GALLOWES

Hochschule für Angewandte Wissenschaften Hamburg
Hamburg University of Applied Sciences

The Global View: Overlay Network Layers



Mobile Ad Hoc Networks

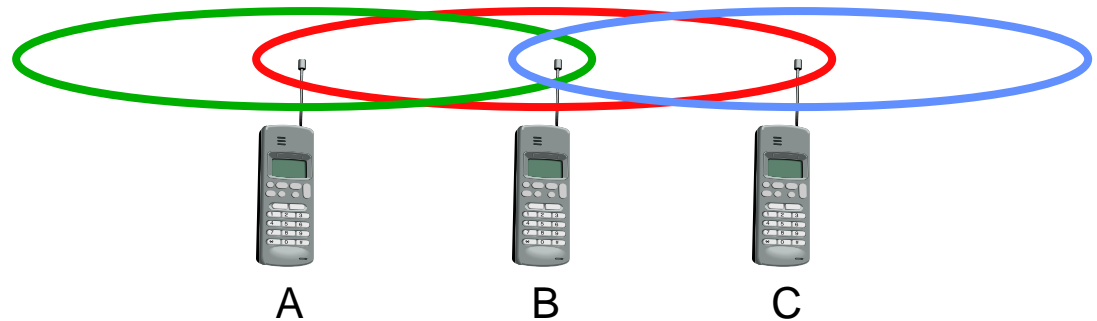
- o Formed by wireless hosts which may be mobile
- o Without (necessarily) using a pre-existing infrastructure
- o Routes between nodes may potentially contain multiple hops
- o Motivations:
 - Ease of deployment, low costs
 - Speed of deployment
 - Decreased dependence on infrastructure



Hidden and exposed terminals

o Hidden terminals

- A sends to B, C cannot receive A
- C wants to send to B, C senses a "free" medium (CS fails)
- collision at B, A cannot receive the collision (CD fails)
- A is "hidden" for C

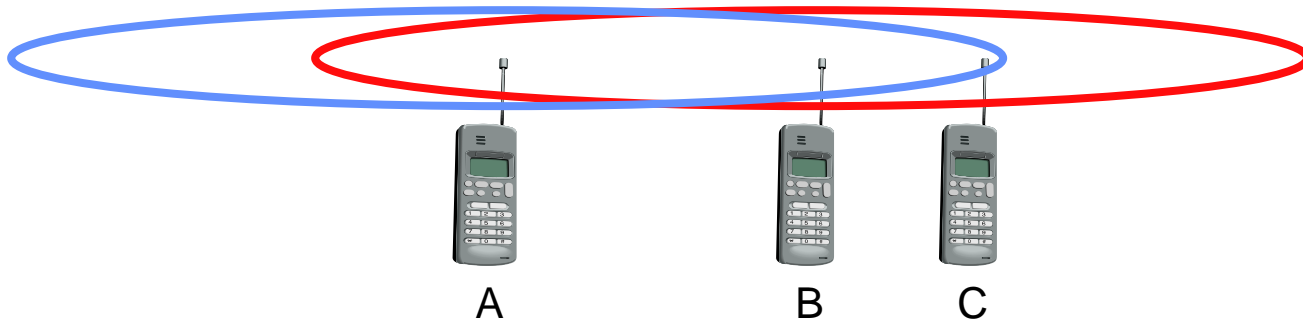


o Exposed terminals

- B sends to A, C wants to send to another terminal (not A or B)
- C has to wait, CS signals a medium in use
- but A is outside the radio range of C, therefore waiting is not necessary
- C is "exposed" to B

Near and far terminals

- o Terminals A and B send, C receives
 - signal strength decreases proportional to the square of the distance
 - the signal of terminal B therefore drowns out A's signal
 - C cannot receive A

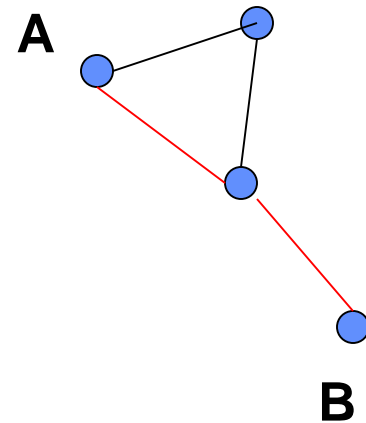
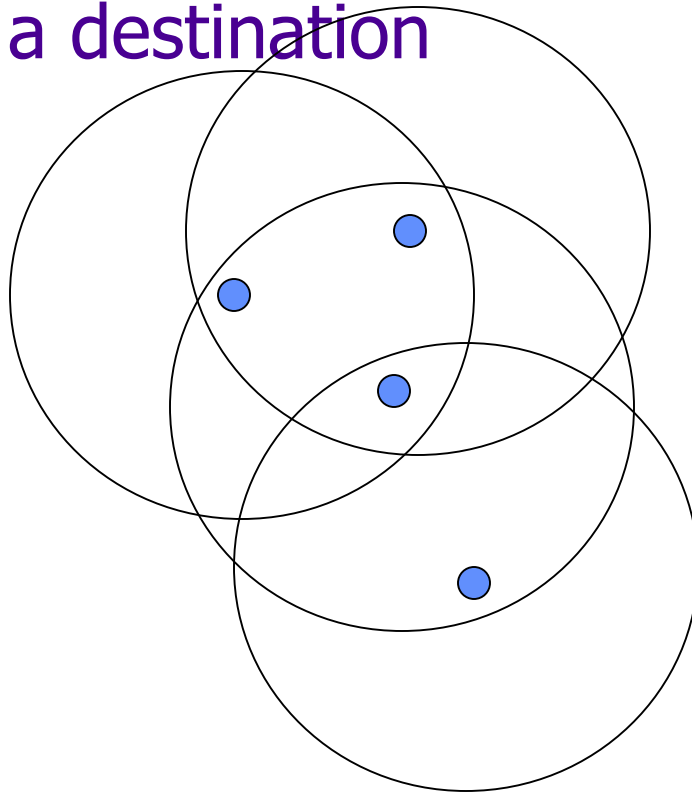


- o If C for example was an arbiter for sending rights, terminal B would drown out terminal A already on the physical layer
- o Also severe problem for CDMA-networks - precise power control needed!



Mobile Ad Hoc Topologies

o May need to traverse multiple wireless links to reach a destination



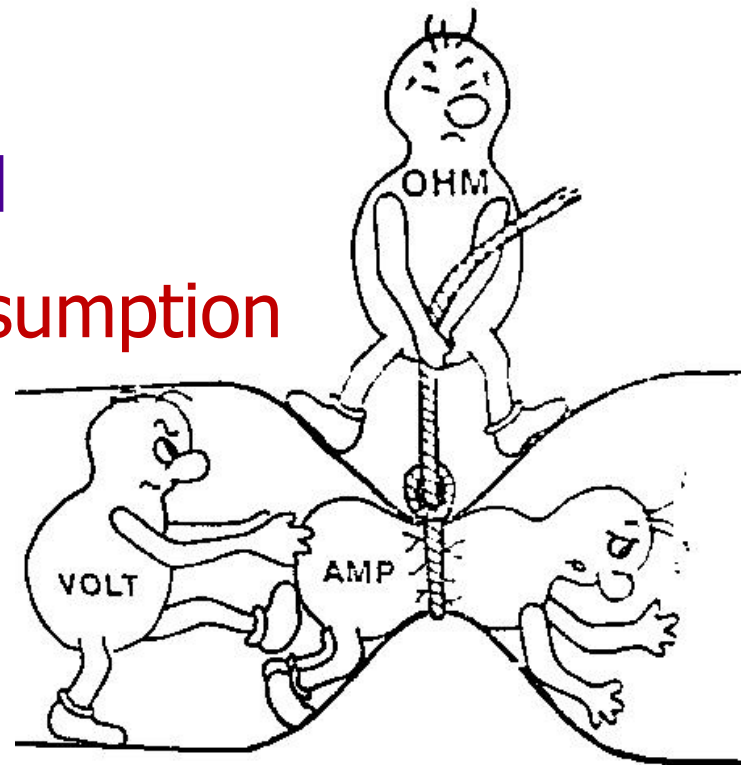
Two Solution Spaces

- o IP on the single link
 - Single-hop solution
 - Adaptation to constraints
- o IP for multi-hop traversal
 - Routing protocol
 - Changing topologies due to link degradation and mobility

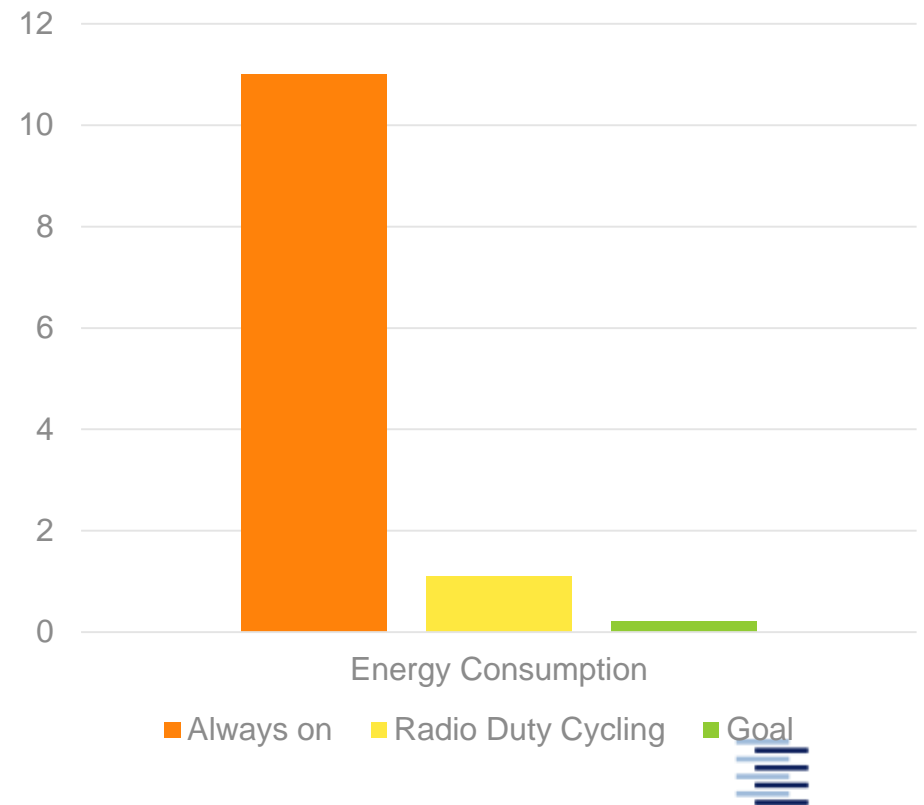


Low Power Lossy Wireless

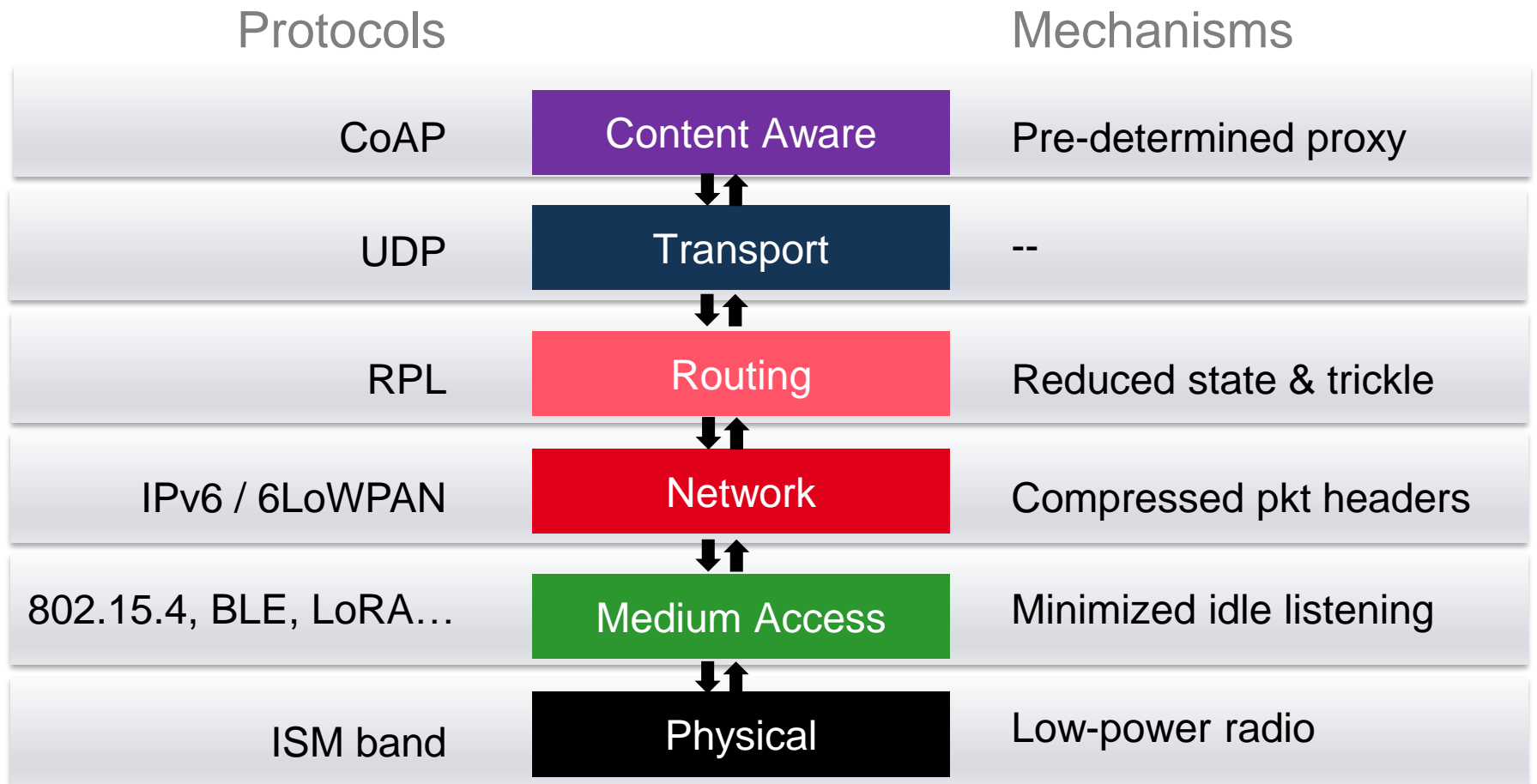
- o Default networking for the constrained IoT
- o Typically battery operated
- o Key problem: **energy consumption**
- o Low power leads to loss
- o Transmission capabilities are weak



How to Reduce the Radio Energy Consumption?



Energy Savings along the IoT Protocol Stack



Link Layer Aspects

- o Inherently unreliable due to wireless medium
- o Small packet size: ~ 100 Bytes
- o Low bandwidth: ~ 100 kbit/s
- o Topologies include star and mesh
- o Networks are ad hoc & devices have limited accessibility
- o Typical radios
 - Short range: IEEE 802.15.4, Bluetooth Low Energy (BLE)
 - Long range: NB-IoT, LoRA, Sigfox (proprietary)



IEEE 802.15.4

o Common low-power radio

- Lower layer of Zigbee and (some) Xbee
- IP convergence layer: 6LowPAN

o Characteristics of 802.15.4:

- Frequencies: 868 MHz, 915 MHz, 2.4 GHz
- 16-bit short or IEEE 64-bit extended MAC addresses
- Entire 802.15.4 frame size is 127 bytes, 25 bytes frame overhead
- Bandwidth ranges from 20 to 250 kbit/s
- Outreach ranges from 1 to 100 m
- 802.15.4 subnets may utilize multiple radio hops

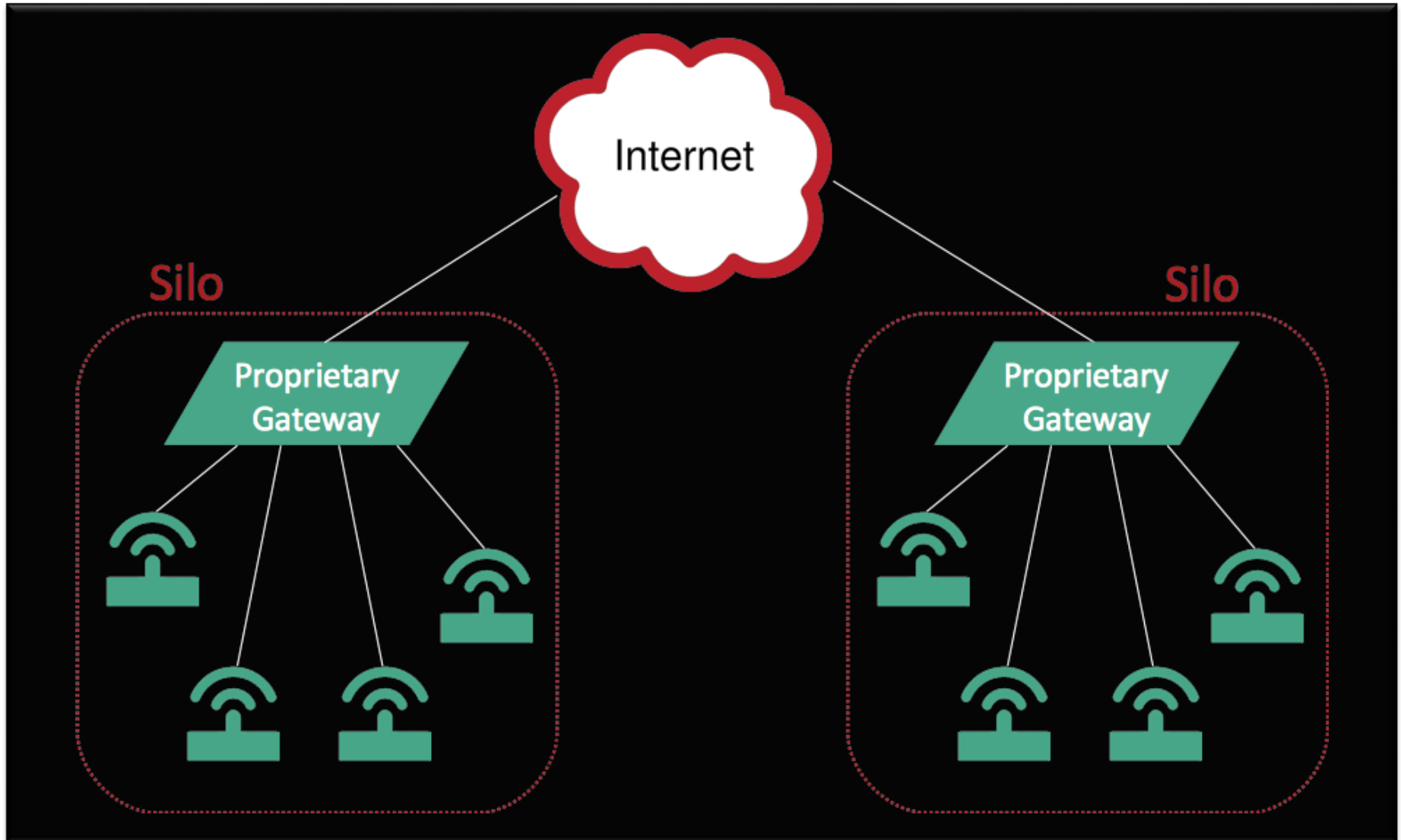


Agenda

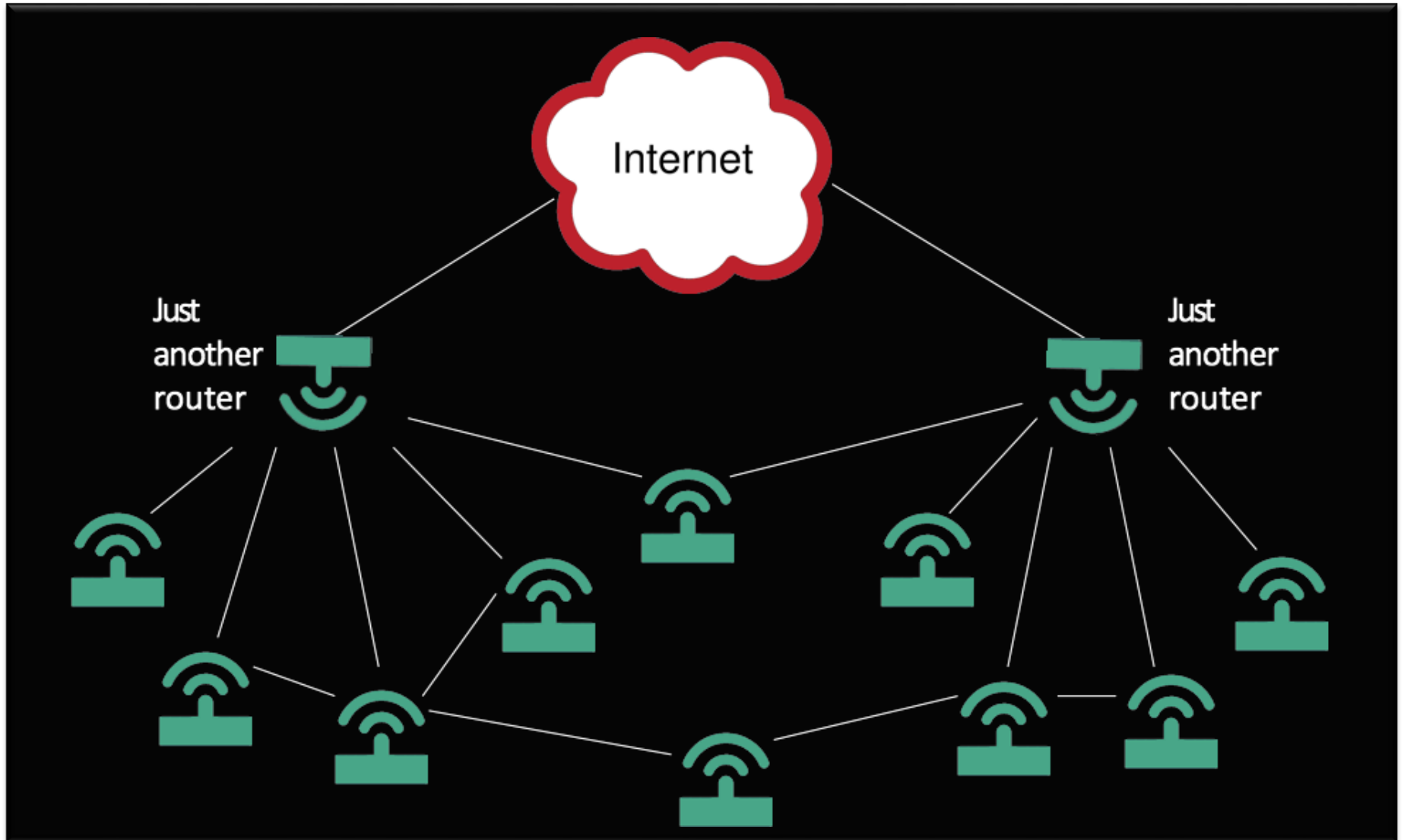
- 🕒 The Internet of Things
- 🕒 IoT on Wireless Link Layers
- 🕒 IP in the Internet of Things
 - ➡ Architectural Challenges
 - ➡ 6LoWPAN Adaptation Layer
 - ➡ Application-Layer Protocols
- 🕒 Mobile Ad Hoc Routing in the Internet of Things



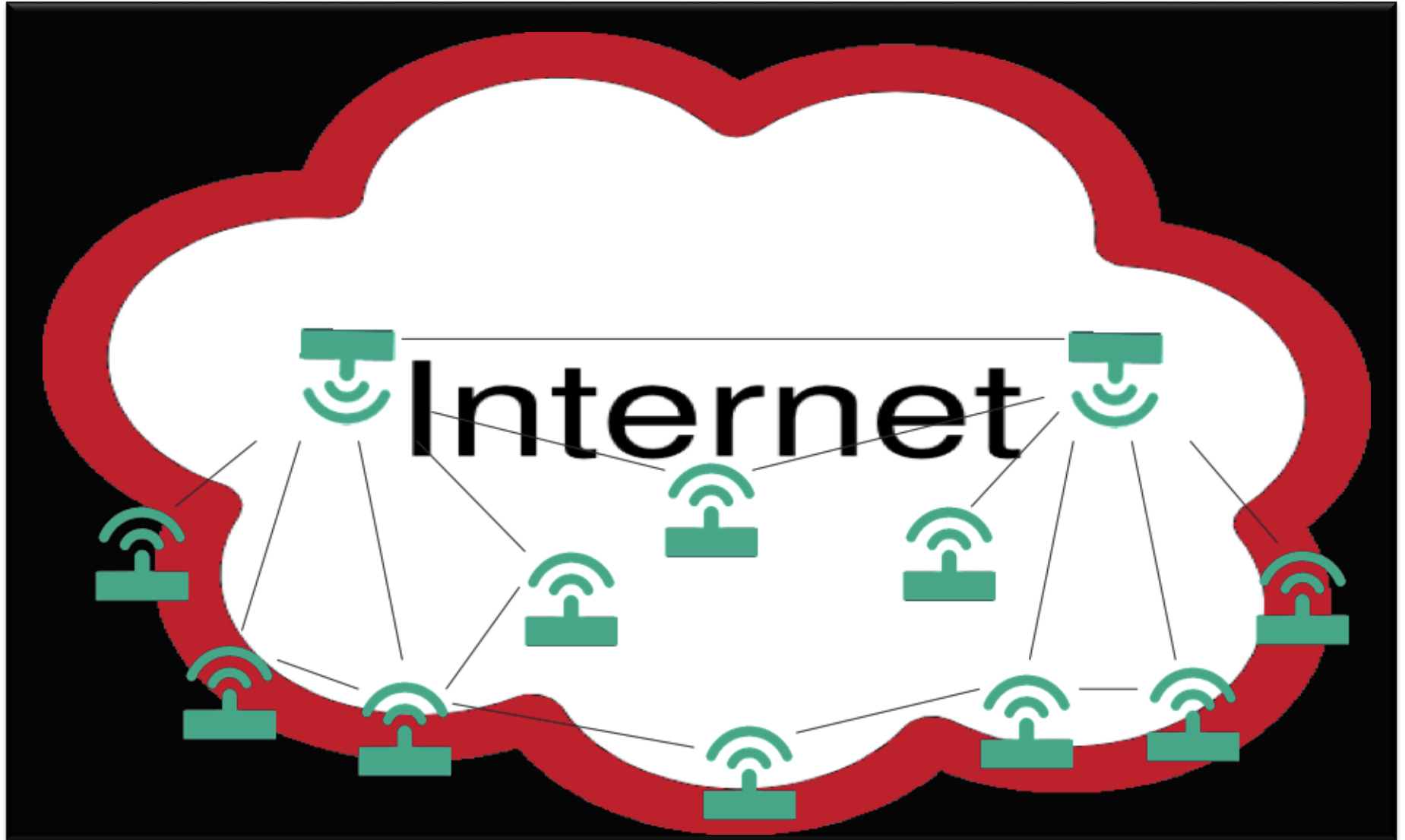
The IoT today looks mostly like this



The IoT we want looks more like that



The IoT we want is... the Internet!



The Difference

o Network level interoperability

- End-to-end connectivity per default
 - Device-to-device connectivity
- => No more walls!

o System level interoperability

- Efficient hardware-independent software
 - No device lock-down
- => No more waste!



IP in the Internet of Things

- o 100+ Billion microcontrollers exist worldwide (in contrast to several hundred million Internet devices)
 - Rapid growths and demands for *scalable* connectivity
 - Integrate into the global Internet with E2E data flows
 - Interoperable, long-lived, reliable standards required: **IP++**
- o Link-layers are different
 - All wireless, dedicated technologies
- o Constraint Communication: Low Power Lossy Networks (LLN)
 - Measures of Bytes ... instead of Megabytes
- o Constraint Devices: Microcontrollers
 - Measures of kHz and kByte
 - Often on batteries




What is 6LoWPAN

- o IPv6 over Low-Power (\supset Personal) wireless Area Networks
- o A transparent way to integrate embedded devices into the global Internet
 - Global addressing
 - E2E transport between embedded and core devices
- o IPv6 adaptation to LLNs
 - Stateless and stateful header compression
 - Optimized neighbor discovery
 - Standard Socket API

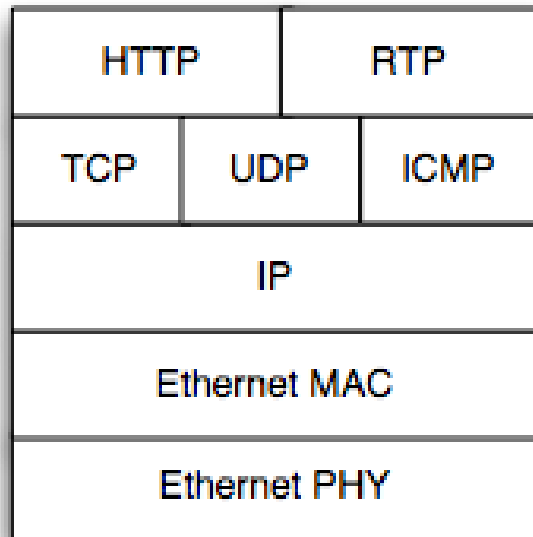


Challenges of LoWPAN

Impact Analysis	Addressing	Routing	Security	Network management
Low power (1-2 years lifetime on batteries)	Storage limitations, low overhead	Periodic sleep aware routing, low overhead	Simplicity (CPU usage), low overhead	Periodic sleep aware management, low overhead
Low cost (<\$10/unit)	Stateless address generation	Small or no routing tables	Ease of Use, simple bootstrapping	Space constraints
Low bandwidth (<300kbps)	Compressed addresses	Low routing overhead	Low packet overhead	Low network overhead
High density (<2-4? units/sq ft)	Large address space – IPv6	Scalable and routable to *a node*	Robust	Easy to use and scalable
IP network interaction	Address routable from IP world	Seamless IP routing	Work end to end from IP network	Compatible with SNMP, etc 

Protocol Stack

TCP/IP Protocol Stack



Application

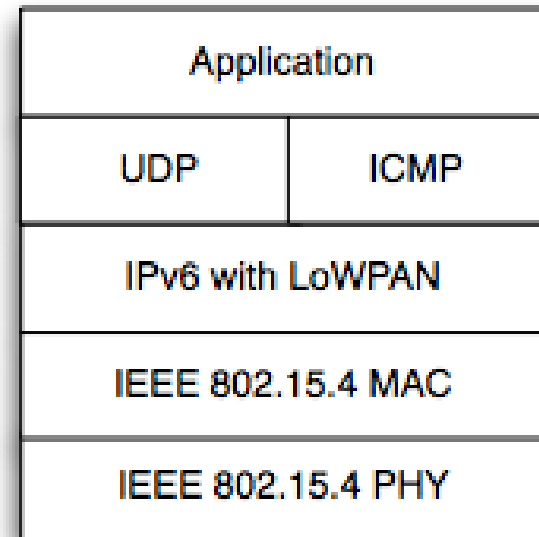
Transport

Network

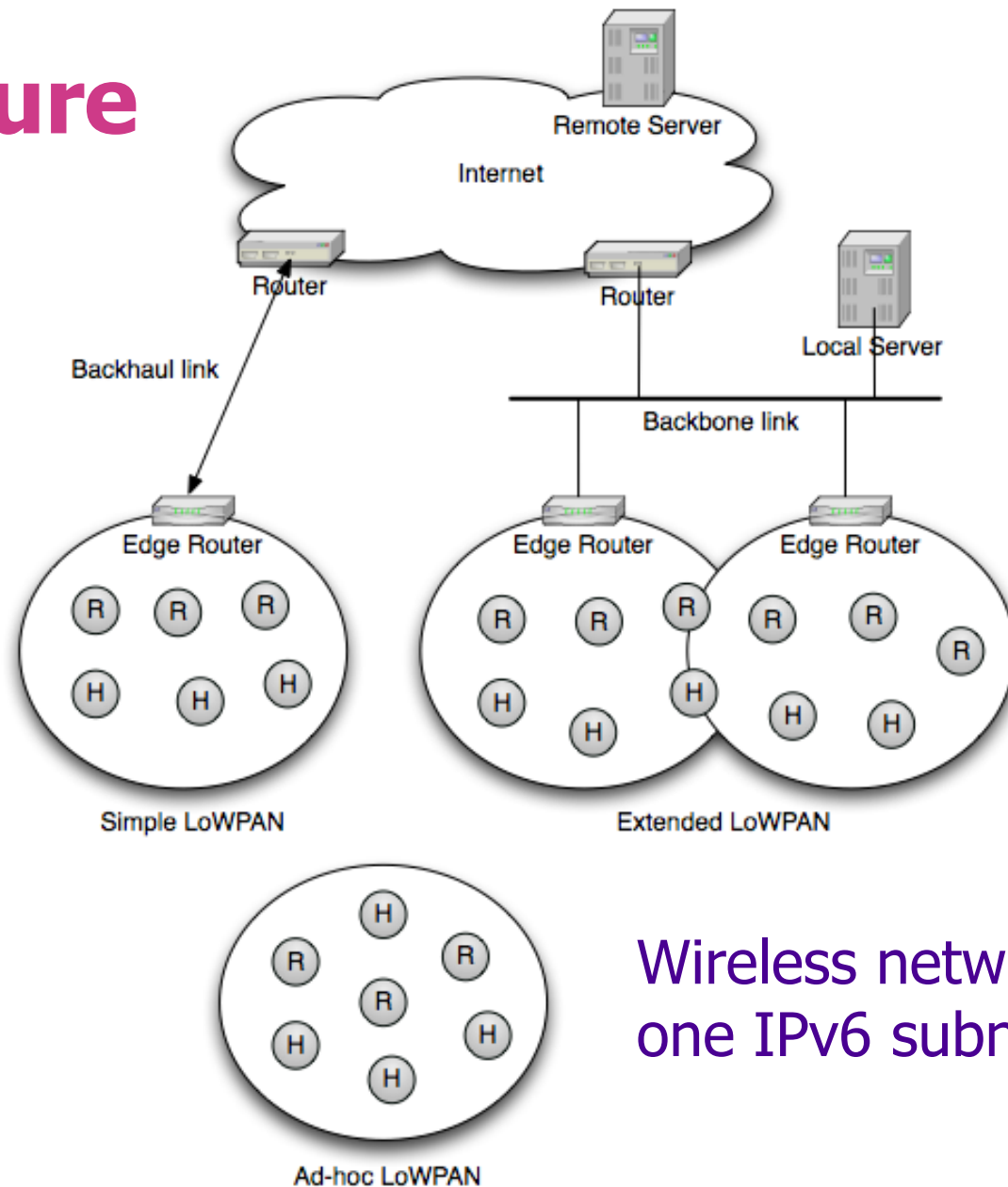
Data Link

Physical

6LoWPAN Protocol Stack



Architecture



Wireless network is one IPv6 subnet



Architecture

- o LoWPANs are stub networks
- o Simple LoWPAN
 - Single Edge Router
- o Extended LoWPAN
 - Multiple Edge Routers with common backbone link
- o Ad-hoc LoWPAN
 - No route outside the LoWPAN
- o Internet integration issues
 - Maximum transmission unit
 - Application protocols
 - IPv4 interconnectivity
 - Firewalls and NATs
 - Security

IPv6	
Ethernet MAC	LoWPAN Adaptation
	IEEE 802.15.4 MAC
Ethernet PHY	IEEE 802.15.4 PHY

IPv6-LoWPAN Router Stack



Key Problems

- o Efficient use of available bits in a packet
 - Frame: 127 bytes – 25 bytes L2 header
 - IPv6 header: 40 bytes, UDP header: 8 bytes ...
- o IPv6 MTU size ≥ 1280
 - IP packets need transparent fragmentation on frames
 - Lost fragments cause retransmission of entire packet
- o Wireless ad hoc networks can be multihop
 - No direct router link \leftrightarrow Router Advertisement
 - Multicast is only local \leftrightarrow Neighbor Discovery



Base Solution: RFC 4944

Makes 802.15.4 look like an IPv6 link:

o Efficient encapsulation

- Stateless IP/UDP header compression of intra-packet redundancy
- Unicast + Multicast address mapping

o Adaptation layer for fragmentation (1280 MTU on ~100 bytes packets)

- Fragmentation: Datagram tag + offset
- No dedicated fragment recovery

o Mesh forwarding

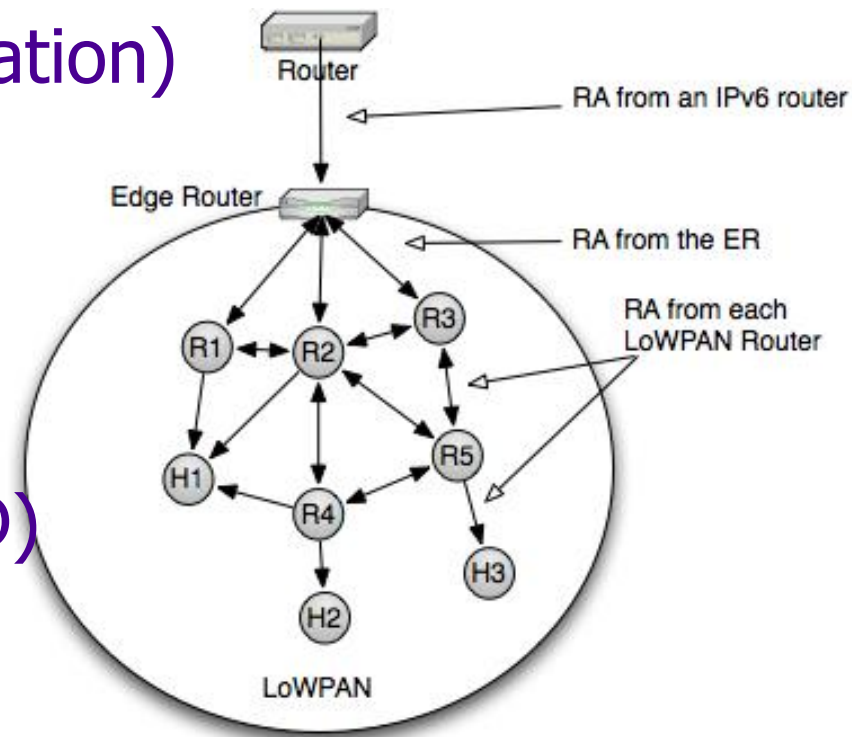
- Link generated by „mesh-under“ (L2) routing
- Identify originator and final destination



Adaptive Neighbor Discovery

RFC 6775

- o Includes „route-over“ (L3 routing)
- o Multihop forwarding of Router Advertisements (GW and prefix dissemination)
- o Address Registration and Confirmation at Router
- o Router keeps track of wireless nodes (incl. DAD)



Typical 6LoWPAN-ND Exchange

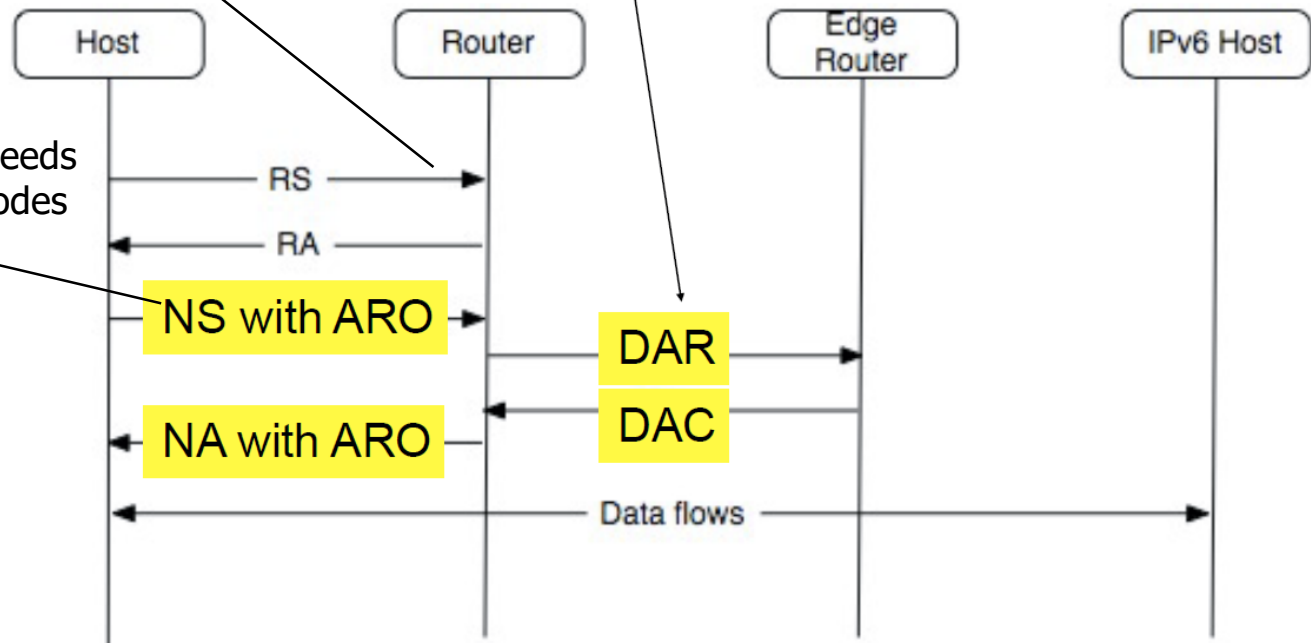
Solicited router advertisement only

- removes periodic Router Advertisements
- includes 6LoWPAN context option

Optional multi-hop DAD

Address registration

- removes multicast needs
- supports sleeping nodes



- o Authoritative Border Router Option (ABRO) to distribute prefix and context across a route-over network

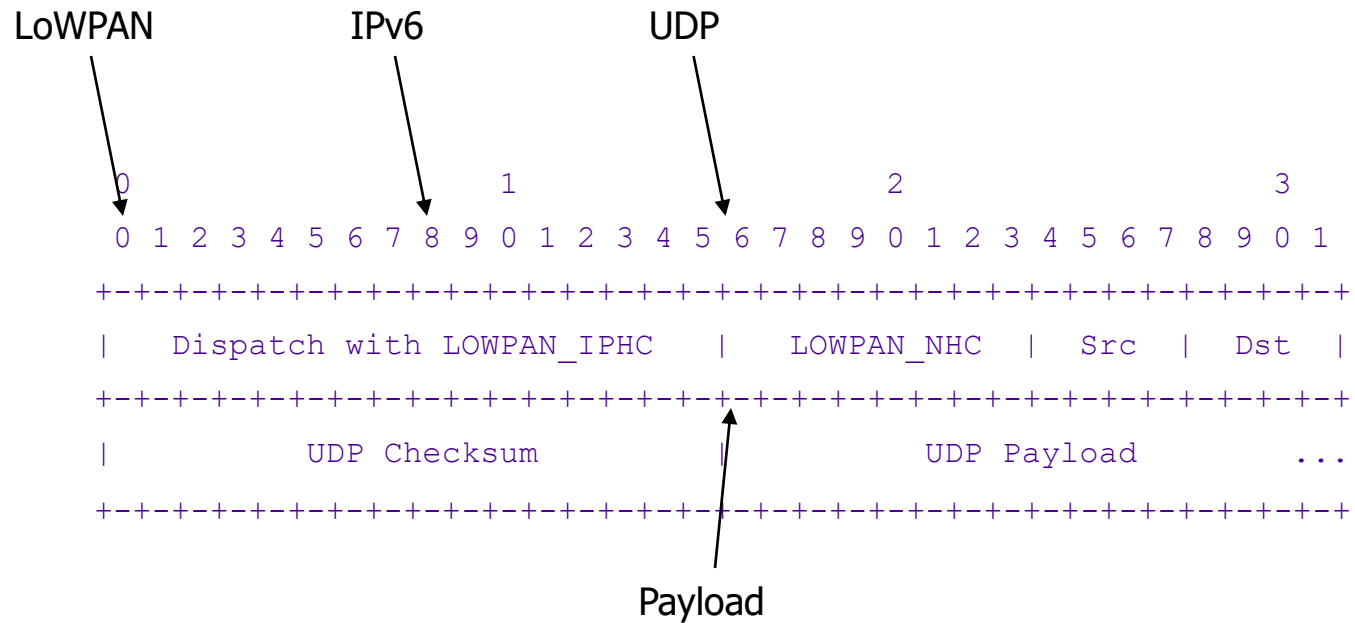


Improved Header Compression RFC 6282

- o Router Advertisements distribute a well-known area context
 - Common prefix – LoWPAN is a flat network
 - 6LoWPAN-HC – header compression methods
- o No addresses – Interface Identifiers derived from MAC addresses
 - Optional unicast and multicast address fields (compressed)
- o Remaining IPv6 header fields compressed or elided
 - Length derived from frame, ToS and Flow Label elided
- o Stateless UDP header compression including short ports and selected checksum removal
 - Length derived from frame length



LoWPAN UDP/IPv6 Headers

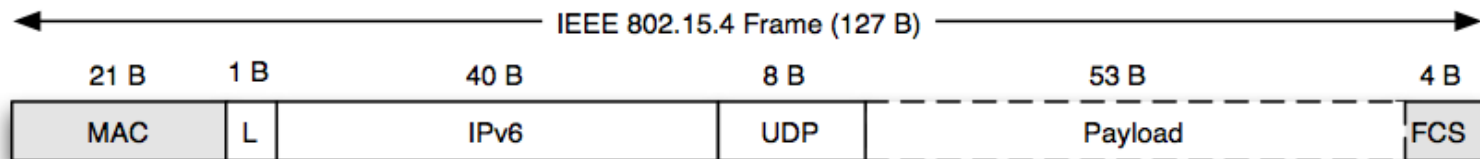


6 Bytes!

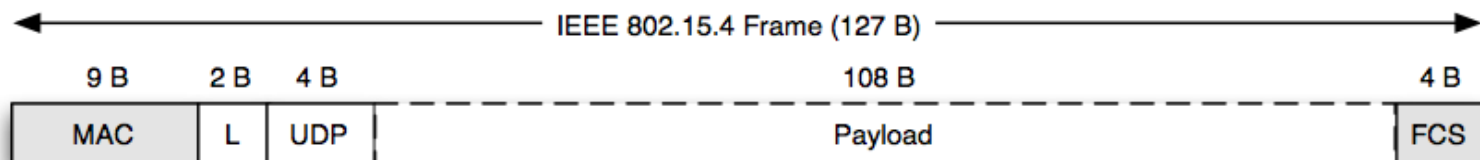


6LoWPAN Headers

- o Orthogonal header format for efficiency
- o Stateless header compression



Full UDP/IPv6 (64-bit addressing)



Minimal UDP/6LoWPAN (16-bit addressing)



COAP:

Constrained Application Protocol

- o Constrained machine-to-machine Web protocol
- o Representational State Transfer (REST) architecture
- o Simple proxy and caching capabilities
- o Asynchronous transaction support
- o Low header overhead and parsing complexity
- o URI and content-type support
- o UDP binding (may use IPsec or DTLS)
- o Reliable unicast and best-effort multicast support
- o Built-in resource discovery



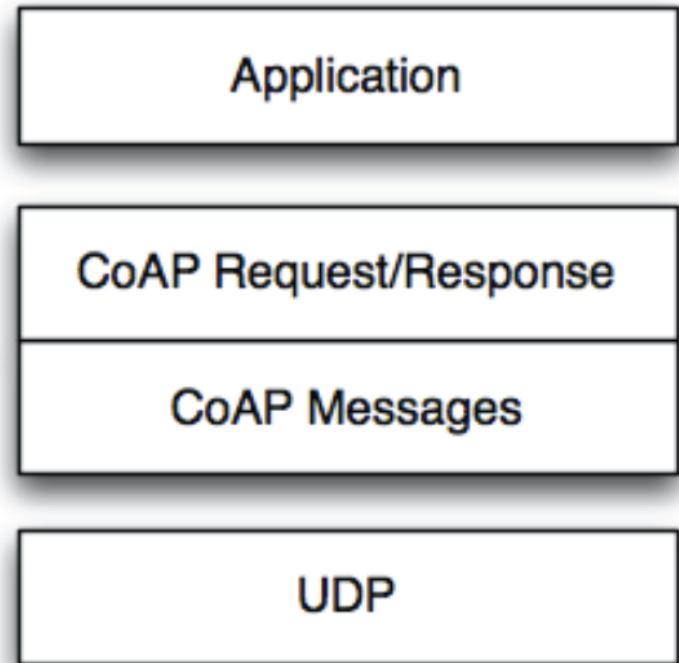
COAP Message Semantic

Four messages:

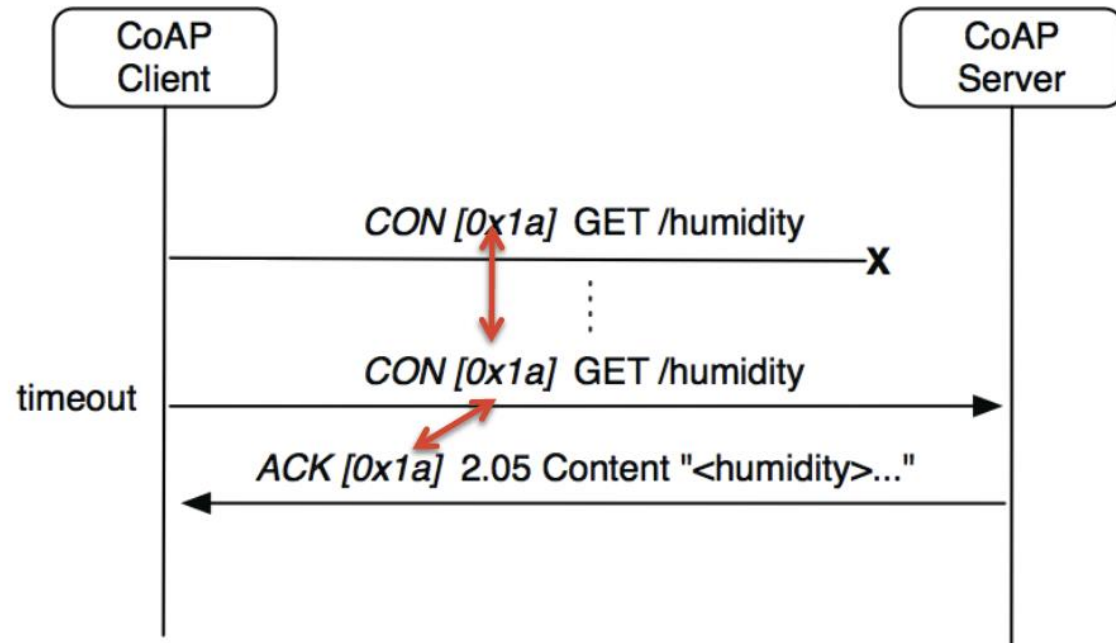
- Confirmable (**CON**)
- Non-Confirmable (**NON**)
- Acknowledgement (**ACK**)
- Un-processing (**RST**)

REST Request/Response
piggybacked on CoAP Messages

Methods: **Get, Put, Post, Delete**

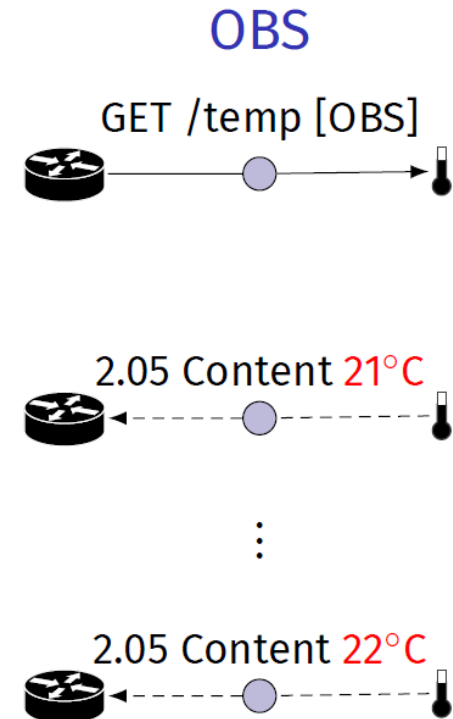
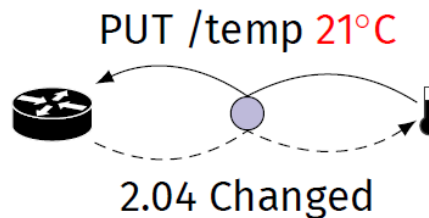
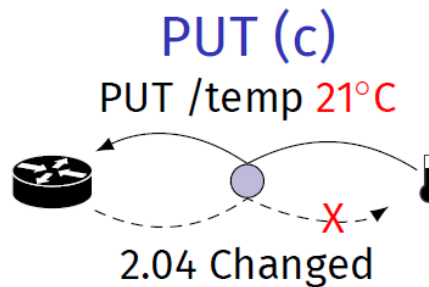
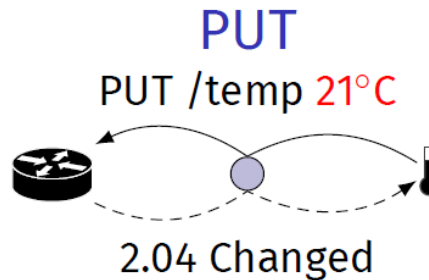
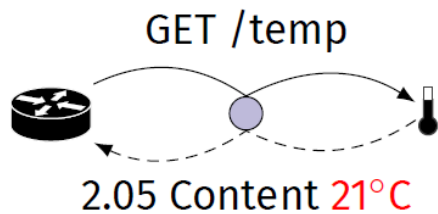
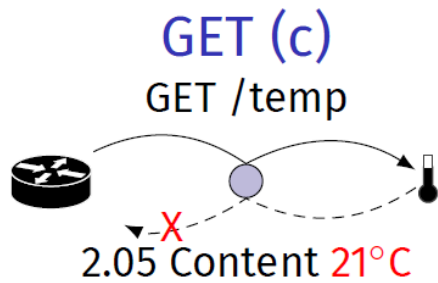
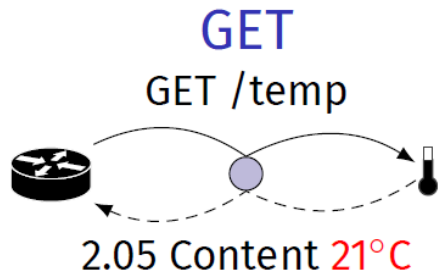


Message Transactions, Packet Loss



- o Each message carries an ID (transactional processing) and an optional token (for asynchronous matching)
- o Stop and Wait approach
- o Repeat a request in case ACK (or RST) is not coming back

COAP Operational Modes



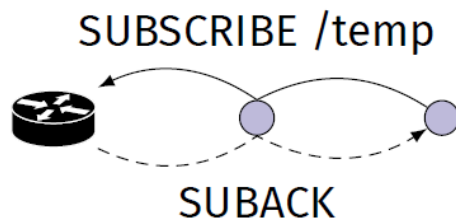
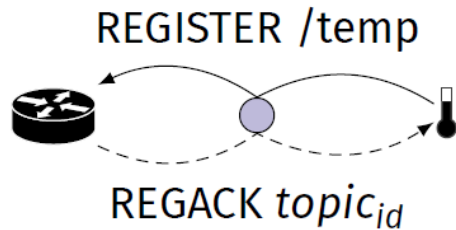
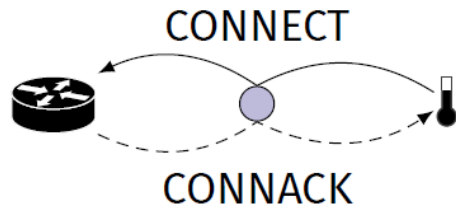
MQTT:

Message Queuing Telemetry Transport

- o Publish-subscribe protocol (IBM 1999)
- o Lightweight & simple on top of TCP/IP
- o MQTT-SN – UDP-based variant for the IoT
- o Publishers and subscribers exchange data via a Broker
- o Different quality levels:
 - Q0 – unreliable
 - Q1 – reliable

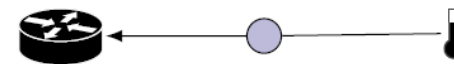


MQTT-SN Operational Modes



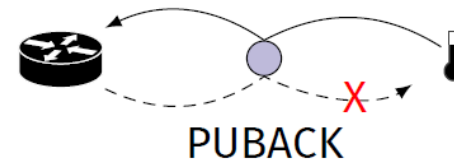
Q0

PUBLISH $topic_{id}$ 21°C

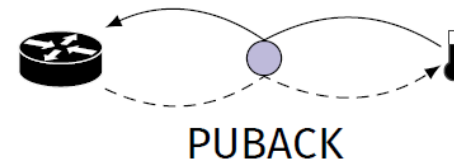


Q1

PUBLISH $topic_{id}$ 21°C



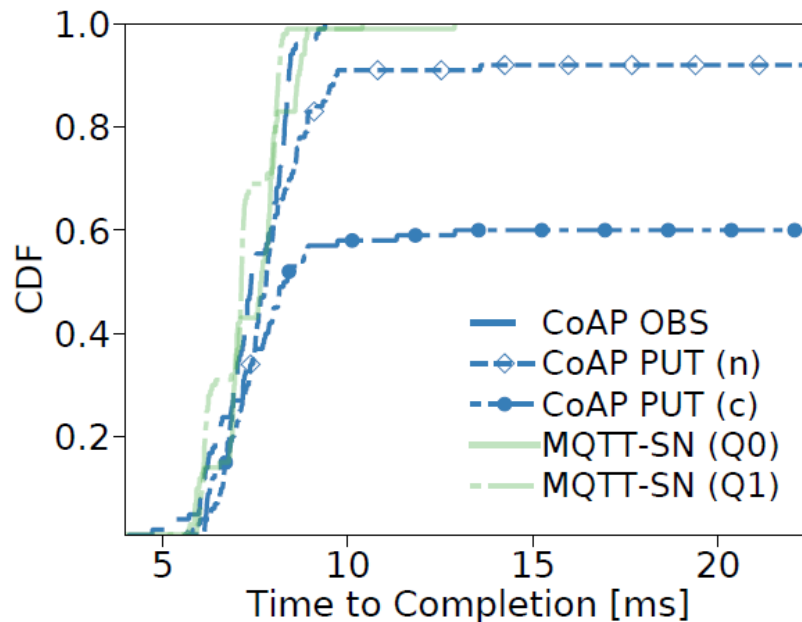
PUBLISH $topic_{id}$ 21°C



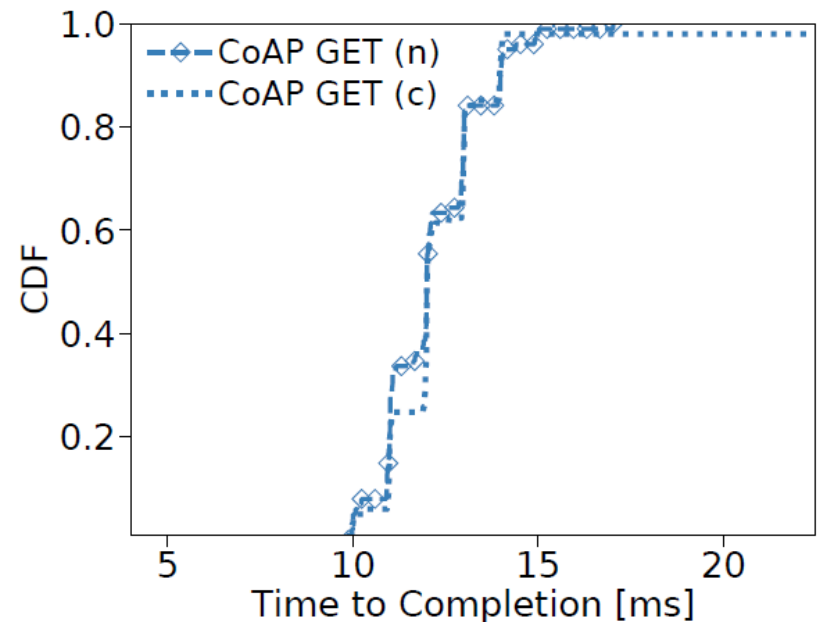
Performance Comparison

Experiments in a Single Hop Testbed

Time to content arrival for **scheduled** publishing every 50 ms



Push protocols



Pull protocols

Cenk Gündogan, Peter Kietzmann, M. Lenders, H. Petersen, T. Schmidt, M. Wählisch,
NDN, CoAP, and MQTT: A Comparative Measurement Study in the IoT,
In: Proc. of 5th ACM Conference on Information-Centric Networking (ICN), Sept. 2018.

Further Aspects & Activities

- o 6LoWPAN on Blue Tooth Low Energy & Lora
- o Application Layer Encoding: CBOR
 - RFC 7049 Concise Binary Object Representation
 - Minimal code size, small message sizes
 - Based on the JSON data model

o Widely implemented:



Contiki



Agenda

- 🕒 The Internet of Things
- 🕒 IoT on Wireless Link Layers
- 🕒 IP in the Internet of Things
- 🕒 Mobile Ad Hoc Routing in the Internet of Things
 - ➡ Properties of MANETs
 - ➡ Routing in MANETs



Many Variations of MANETs

o Fully Symmetric Environment

- all nodes have identical **capabilities** and **responsibilities**

o Asymmetric Capabilities

- transmission ranges and radios may differ (→ asymmetric links)
- battery life at different nodes may differ
- processing capacity may be different at different nodes
- speed of movement

o Asymmetric Responsibilities

- only some nodes may route packets
- some nodes may act as **leaders** of nearby nodes (e.g., cluster head)

o Varying Traffic Characteristics

Performance Properties of MANETs

o One-Hop Capacity:

Consider MANET of n equal nodes, each acting as router, with constant node density. Then the One-Hop Capacity grows linearly $\rightarrow O(n)$

o Total Capacity surprisingly low:

- Consider MANET of n equal nodes, each acting as router in an *optimal* set-up, then the Node Capacity to reach an arbitrary destination reads $\rightarrow O(1/\sqrt{n})$
- Node Capacity further decreases under wireless transmission $\rightarrow O(1/\sqrt{(n \ln(n))})$



Unicast Routing in MANETs - Why is it different ?

- o Host mobility
 - link failure/repair due to mobility may have different characteristics than those due to other causes
- o Rate of link failure/repair may be high when nodes move fast
- o New performance criteria may be used
 - route stability despite mobility
 - energy consumption
- o Many routing protocols proposed – no universal solution



Routing Protocols

o Proactive protocols

- Determine routes independent of traffic pattern
- Traditional link-state and distance-vector routing protocols are proactive

o Reactive protocols


- Maintain routes only if needed
- Saves bandwidth and energy at sparse scenarios

o Hybrid protocols

- Proactive route discovery for the relevant, e.g. Gateways
- Reactive route discovery for the remainders



Trade-Off

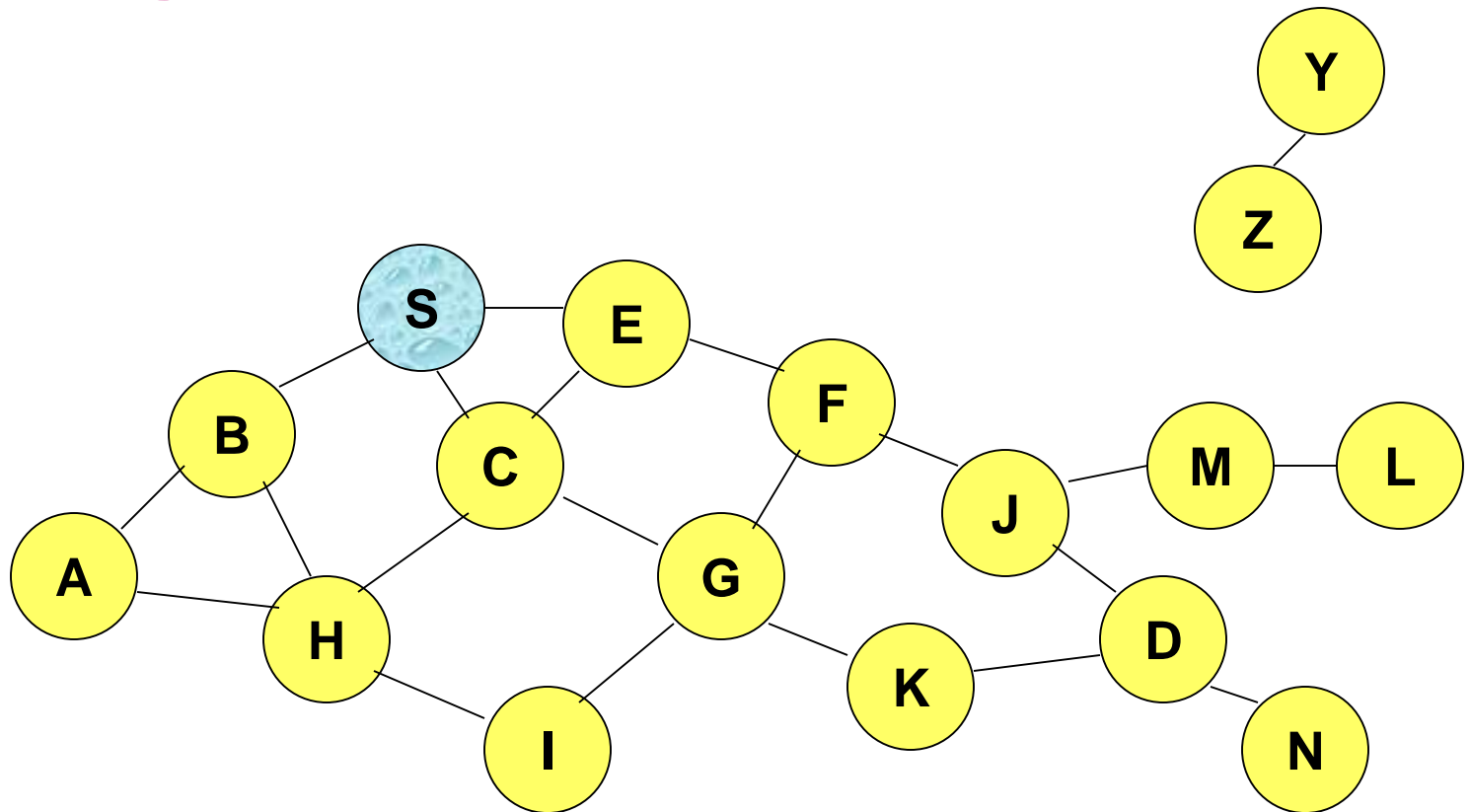
- o Latency of route discovery
 - Proactive protocols may have lower latency since routes are maintained at all times
 - Reactive protocols may have higher latency because a route from X to Y will be found only when X attempts to send to Y
- o Overhead of route discovery/maintenance
 - Reactive protocols may have lower overhead since routes are determined only if needed
 - Proactive protocols can (but not necessarily) result in higher overhead due to continuous route updating
- o Which approach achieves a better trade-off depends on 
the traffic and mobility patterns

Flooding for Data Delivery

- o Sender S broadcasts data packet P to all its neighbors
- o Each node receiving P forwards P to its neighbors
- o Sequence numbers used to avoid the possibility of forwarding the same packet more than once
- o Packet P reaches destination D provided that D is reachable from sender S
- o Node D does not forward the packet



Flooding for Data Delivery



Represents a node that has received packet P
Represents that connected nodes are within each other's transmission range

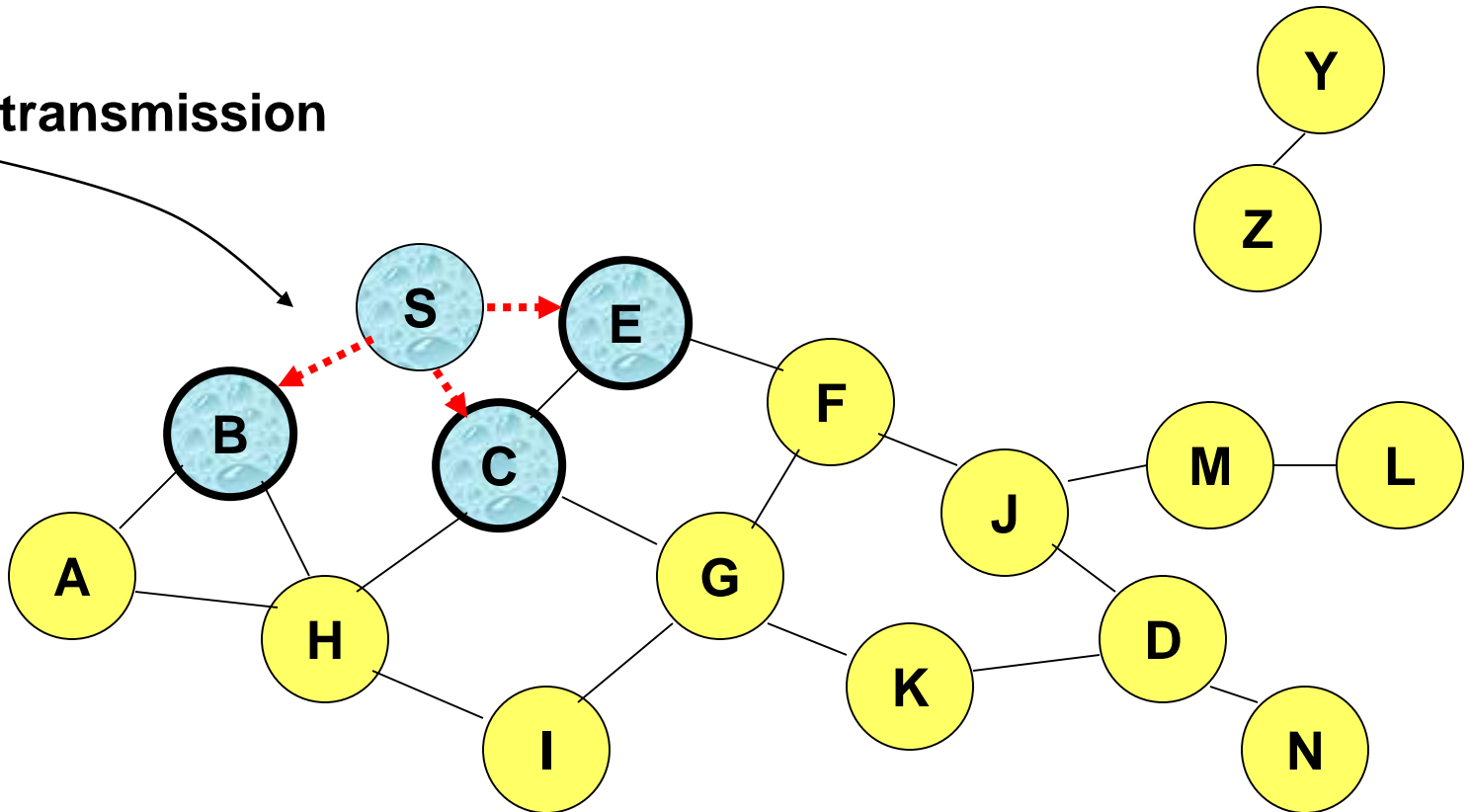


Hafen Hamburg

Hamburg University of Applied Sciences

Flooding for Data Delivery

Broadcast transmission



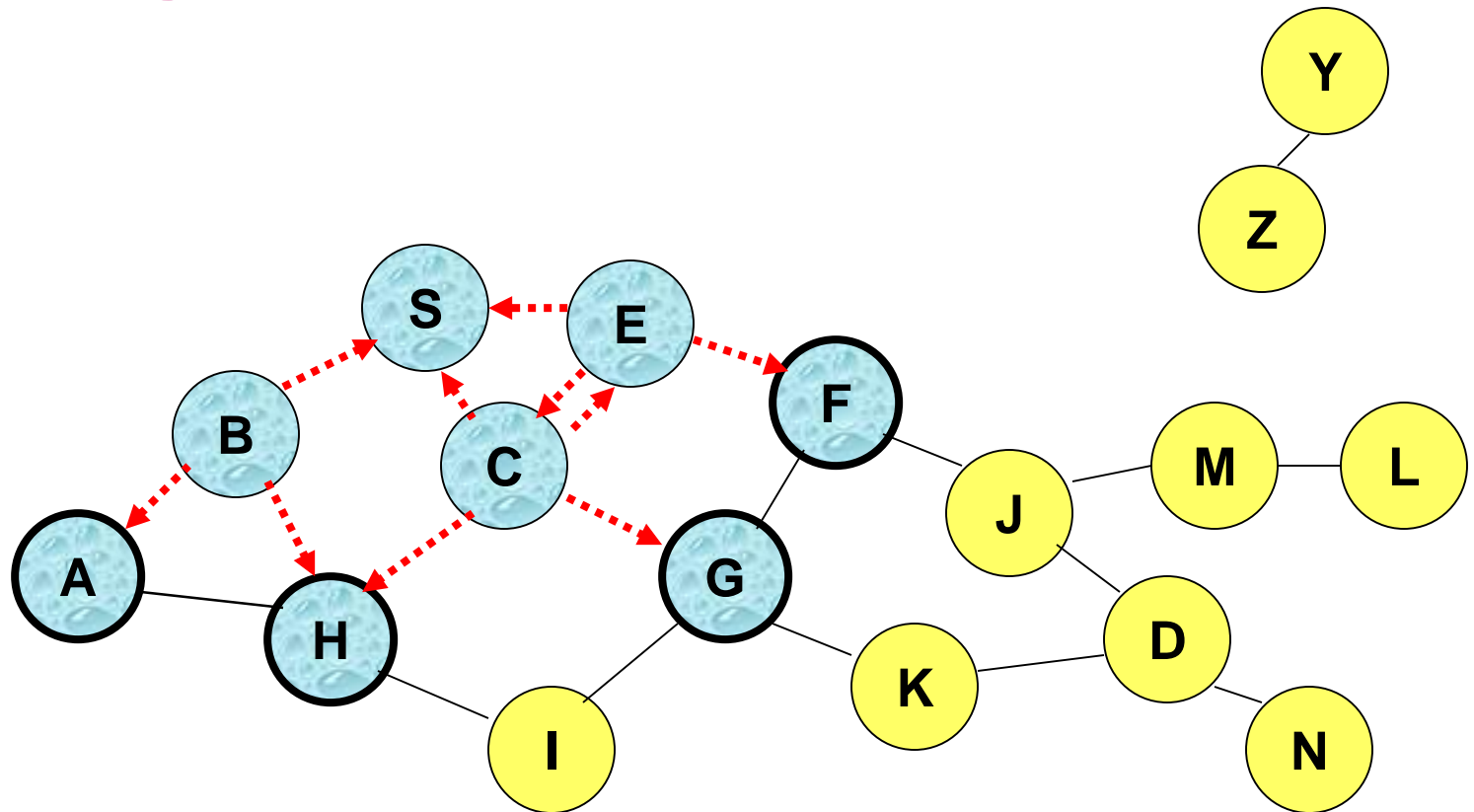
Represents a node that receives packet P for the first time



Represents transmission of packet P



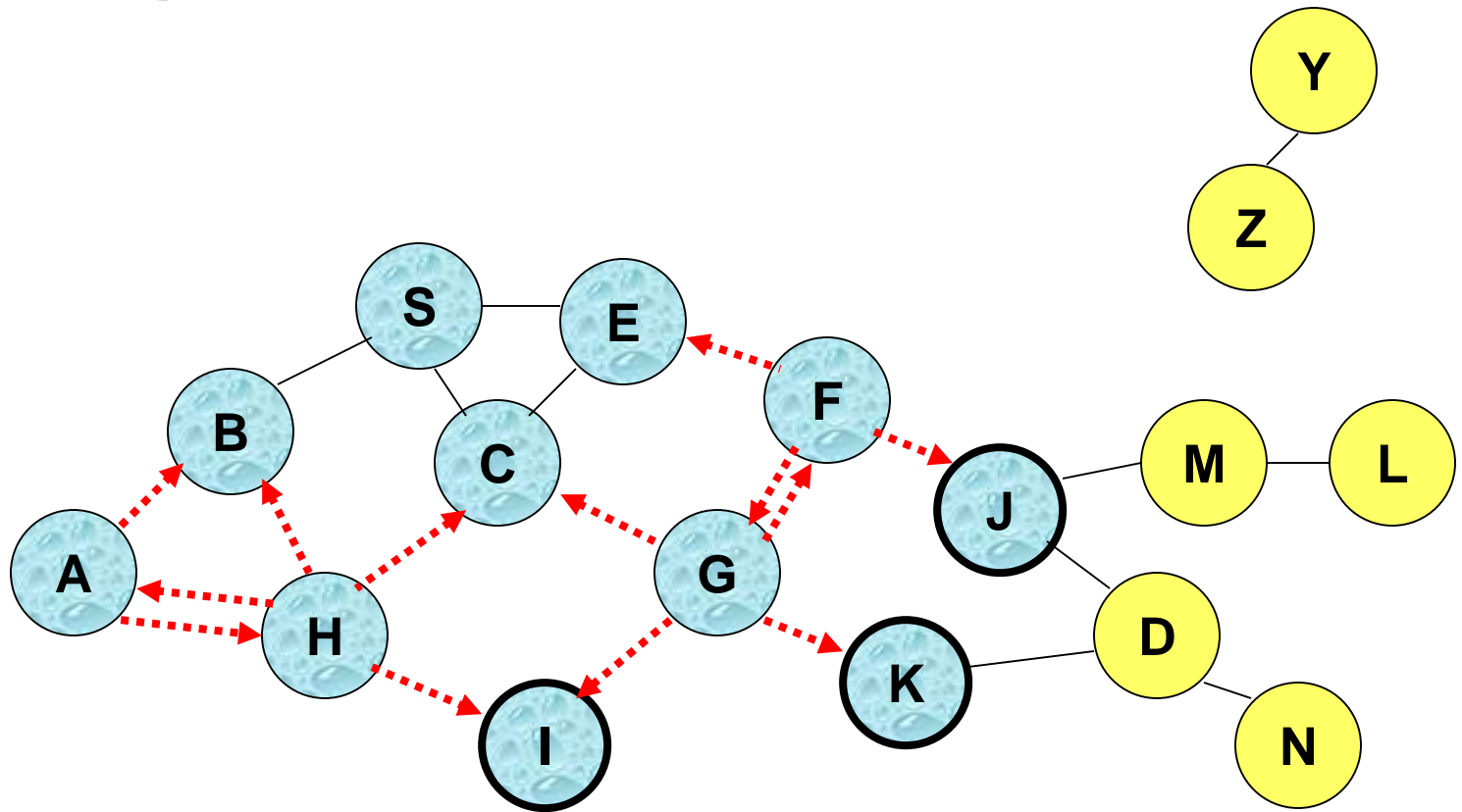
Flooding for Data Delivery



- **Node H receives packet P from two neighbors:**
potential for collision

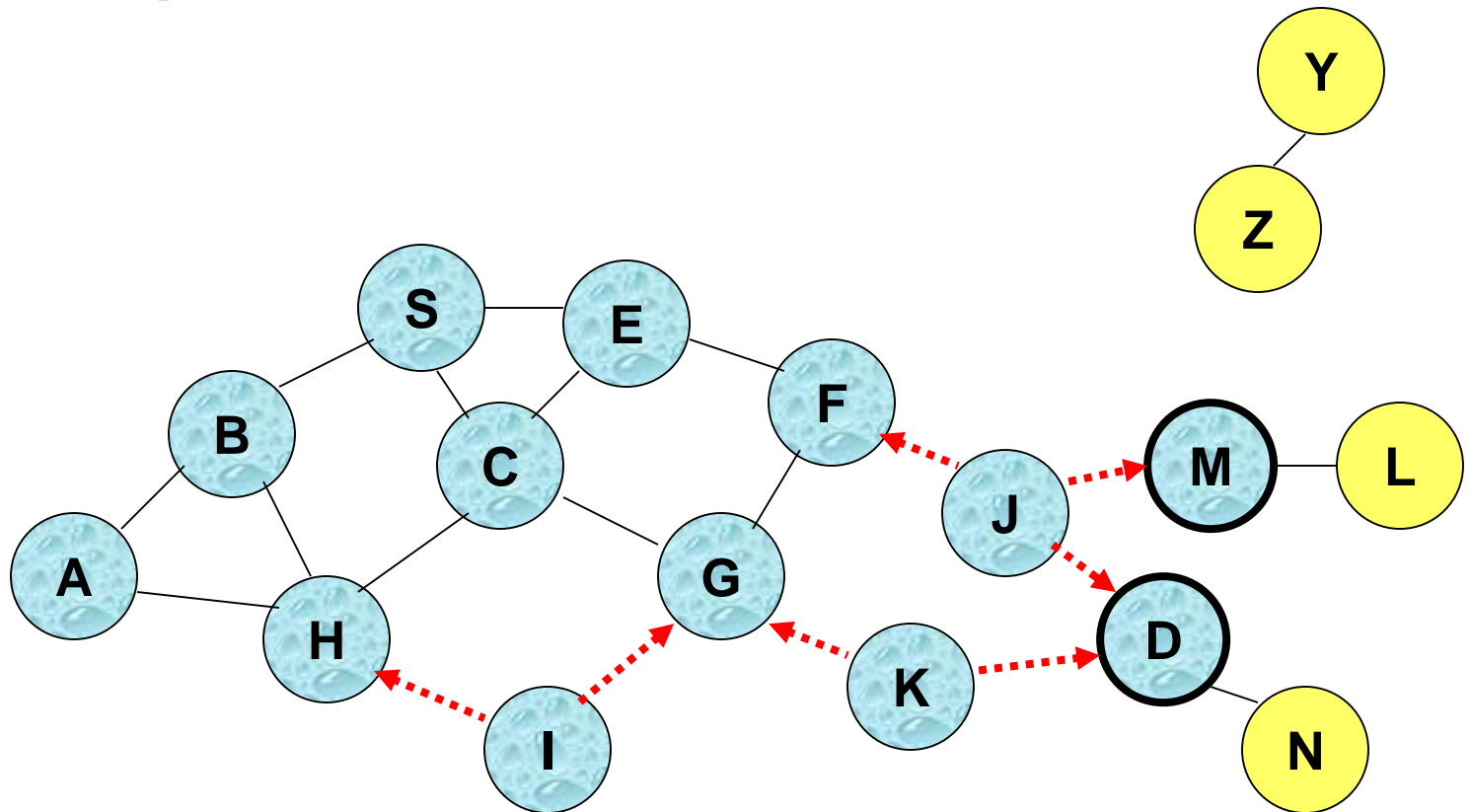


Flooding for Data Delivery



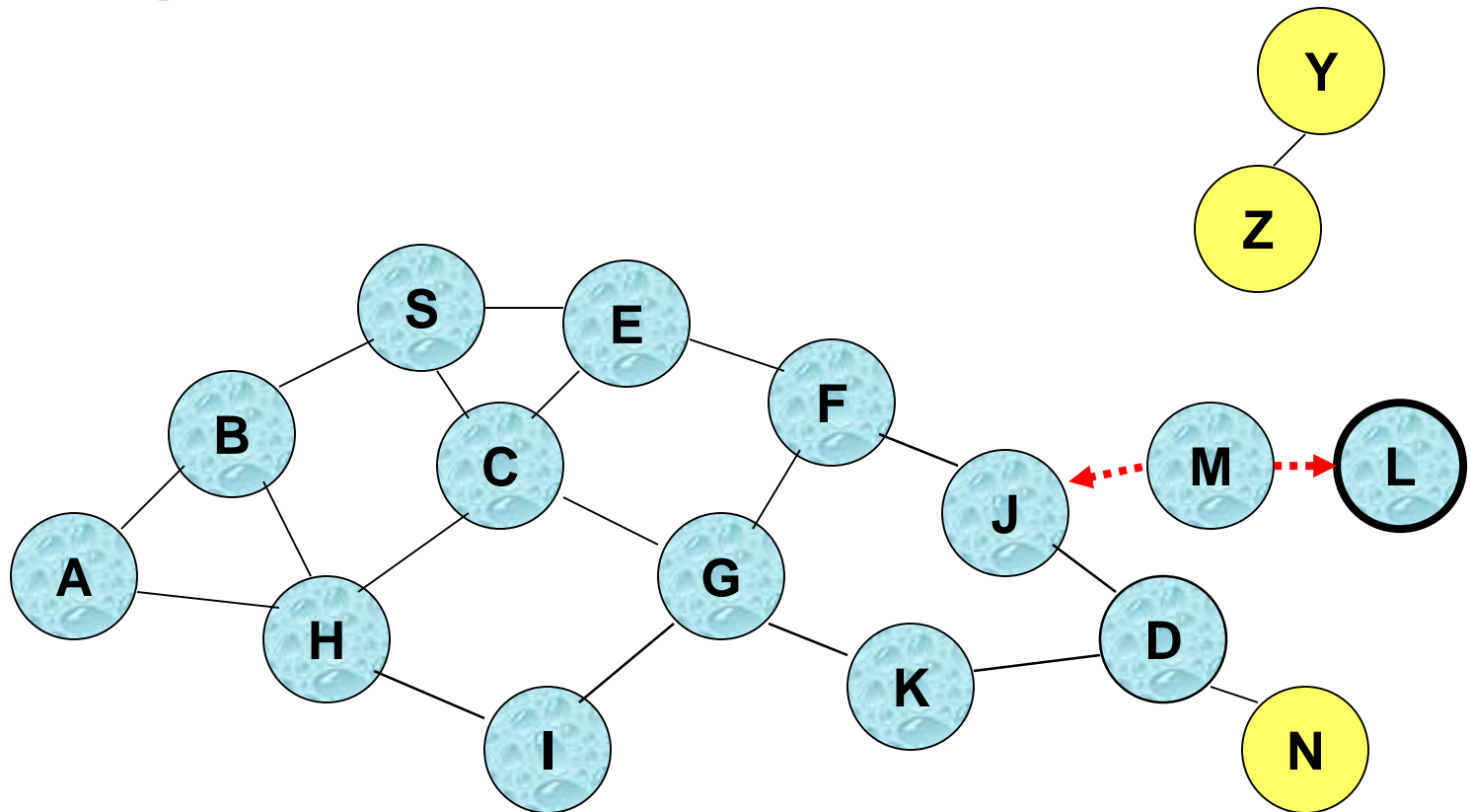
- Node C receives packet P from G and H, but does not forward it again, because node C has **already forwarded packet P** once

Flooding for Data Delivery



- Nodes J and K both broadcast packet P to node D
- Since nodes J and K are **hidden** from each other, their transmissions may collide
=> **Packet P may not be delivered to node D at all, despite the use of flooding**

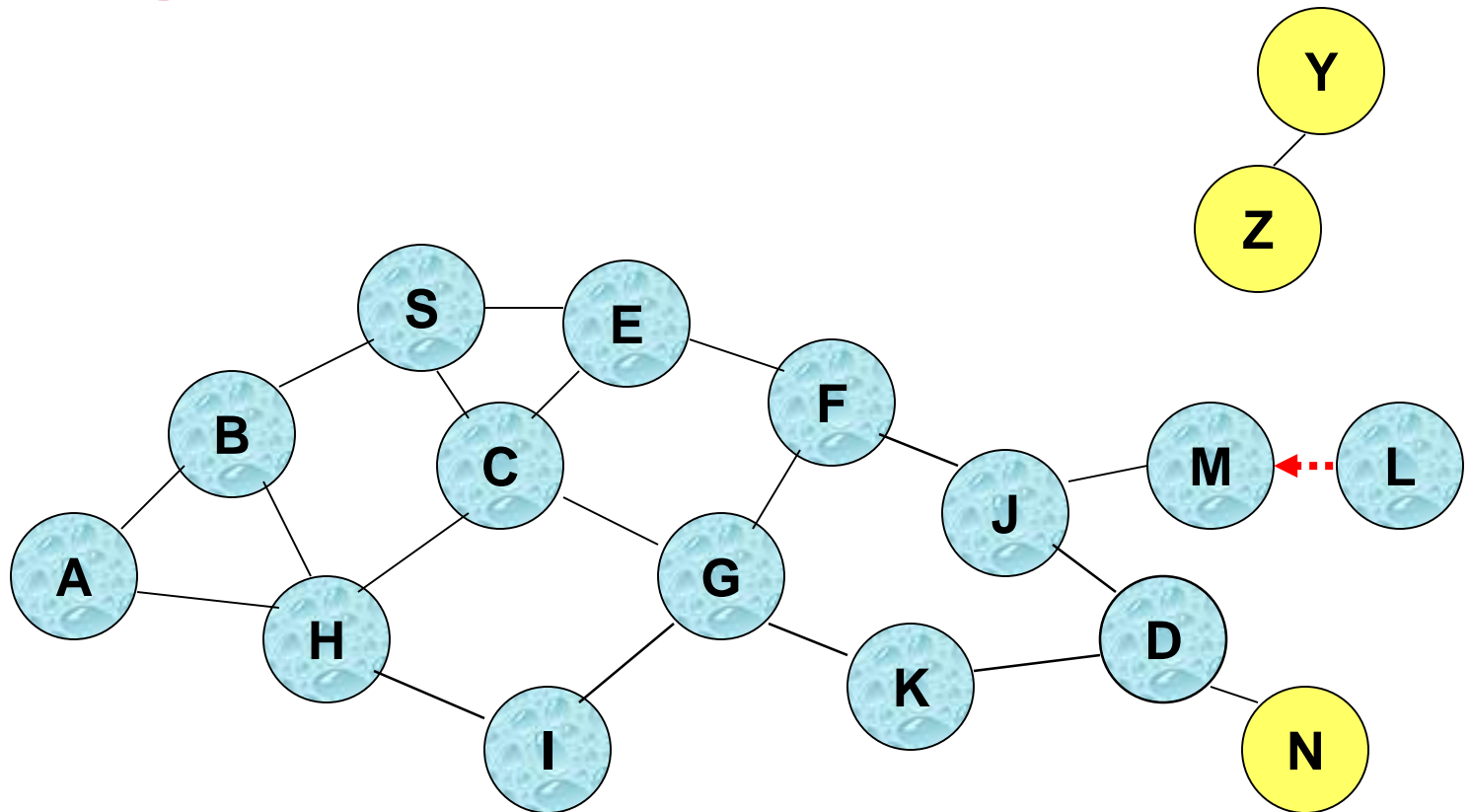
Flooding for Data Delivery



- Node D **does not forward** packet P, because node D is the **intended destination of packet P**

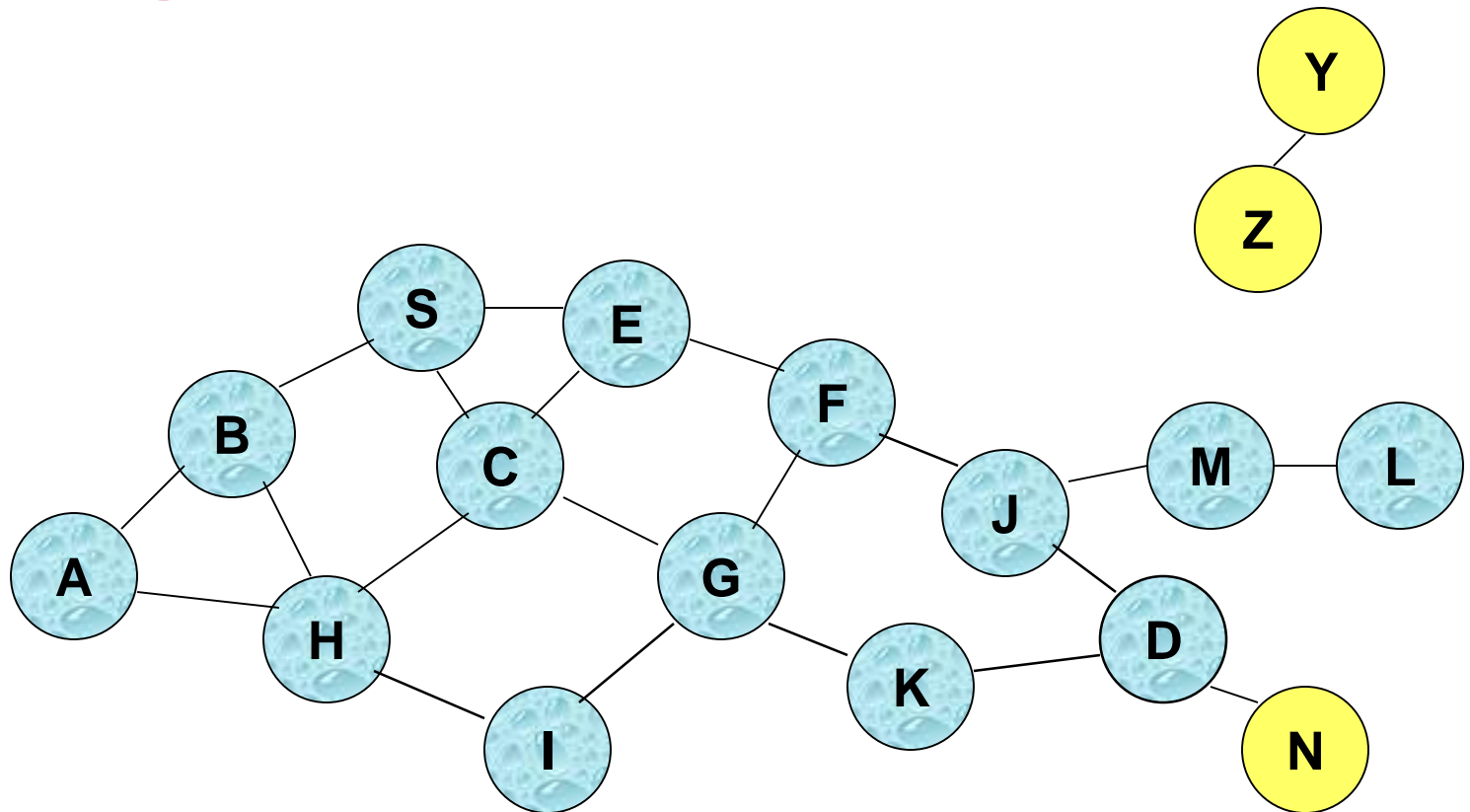


Flooding for Data Delivery



- Flooding completed
- Nodes **unreachable** from S do not receive packet P (e.g., node Z)
- Nodes for which all paths from S go through the destination **D** also do not receive packet P (example: node N)

Flooding for Data Delivery



- Flooding may deliver packets to too many nodes (in the **worst case**, all nodes reachable from sender may receive the packet)



Flooding for Data Delivery: Advantages

- o Simplicity
- o May be more efficient than other protocols when rate of information transmission is low enough that the overhead of explicit route discovery/maintenance incurred by other protocols is relatively higher
 - this scenario may occur, for instance, when nodes transmit **small data packets** relatively infrequently, and many topology **changes occur** between consecutive packet transmissions
- o Potentially higher reliability of data delivery
 - Because packets may be delivered to the destination on **multiple paths**



Flooding for Data Delivery: Disadvantages

- o Potentially, very high overhead
 - Data packets may be delivered to too many nodes who do not need to receive them
- o Potentially lower reliability of data delivery
 - Flooding uses broadcasting -- hard to implement reliable broadcast delivery without significantly increasing overhead
 - Broadcasting in IEEE 802.11 MAC is unreliable
 - In our example, nodes J and K may transmit to node D simultaneously, resulting in loss of the packet
 - in this case, destination would not receive the packet at all

Flooding of Control Packets

- o Many protocols perform (potentially *limited*) flooding of **control** packets, instead of **data** packets
- o The control packets are used to discover routes
- o Discovered routes are subsequently used to send data packet(s)
- o Overhead of control packet flooding is **amortized** over data packets transmitted between consecutive control packet floods

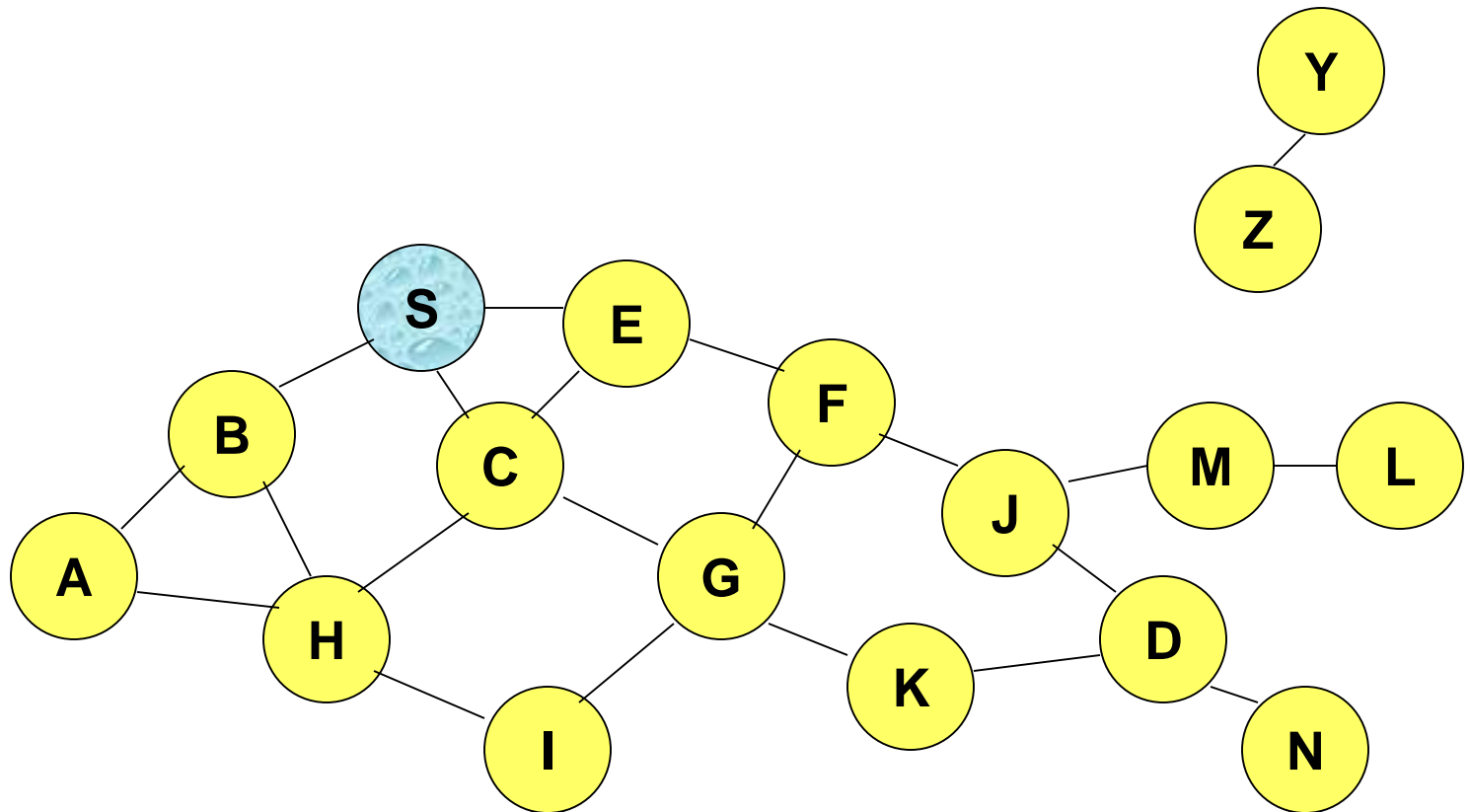


Dynamic Source Routing (DSR) [Johnson96]

- o When node S wants to send a packet to node D, but does not know a route to D, node S initiates a route discovery
- o Source node S floods Route Request (RREQ)
- o Each node appends own identifier when forwarding RREQ



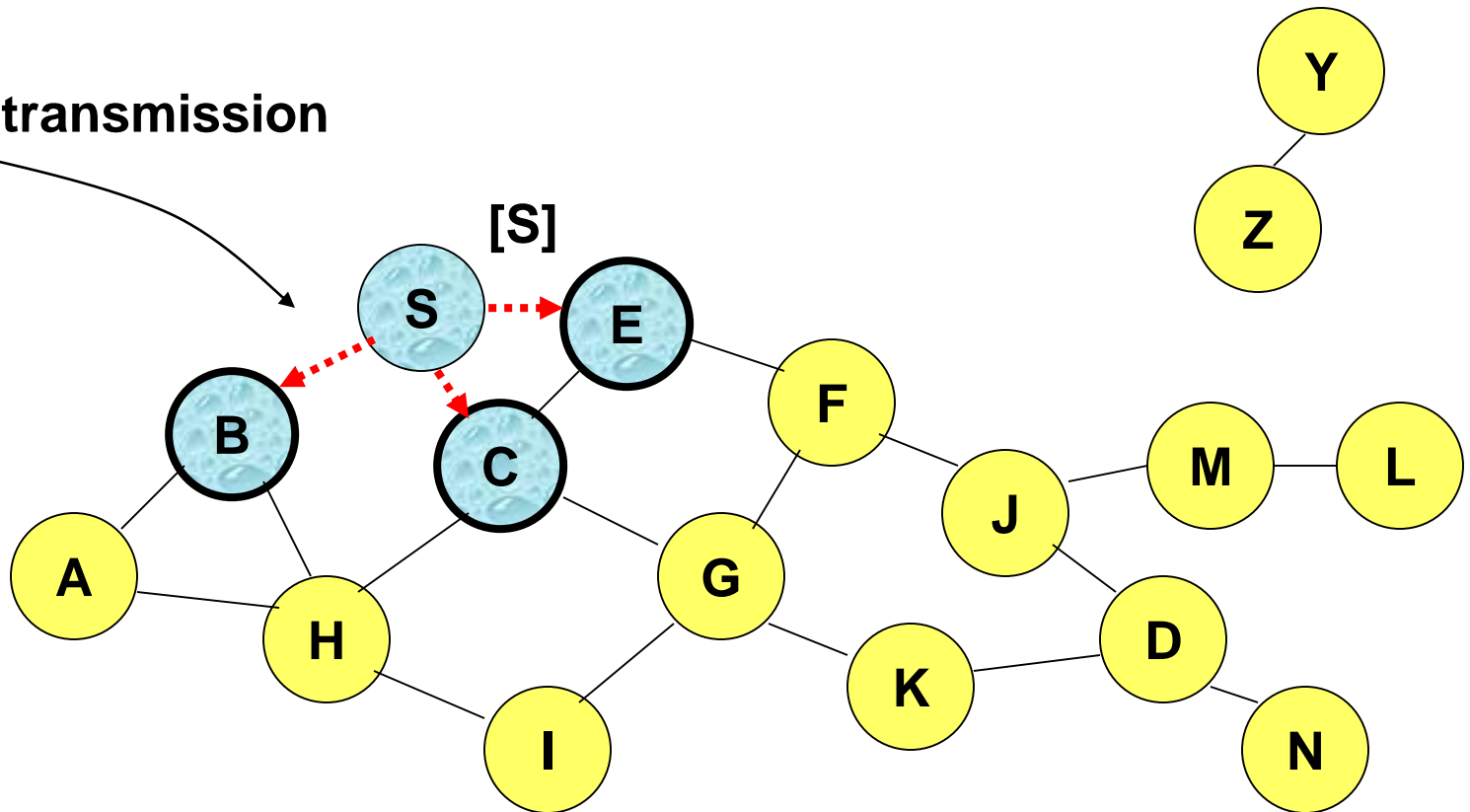
Route Discovery in DSR



Represents a node that has received RREQ for D from S

Route Discovery in DSR

Broadcast transmission

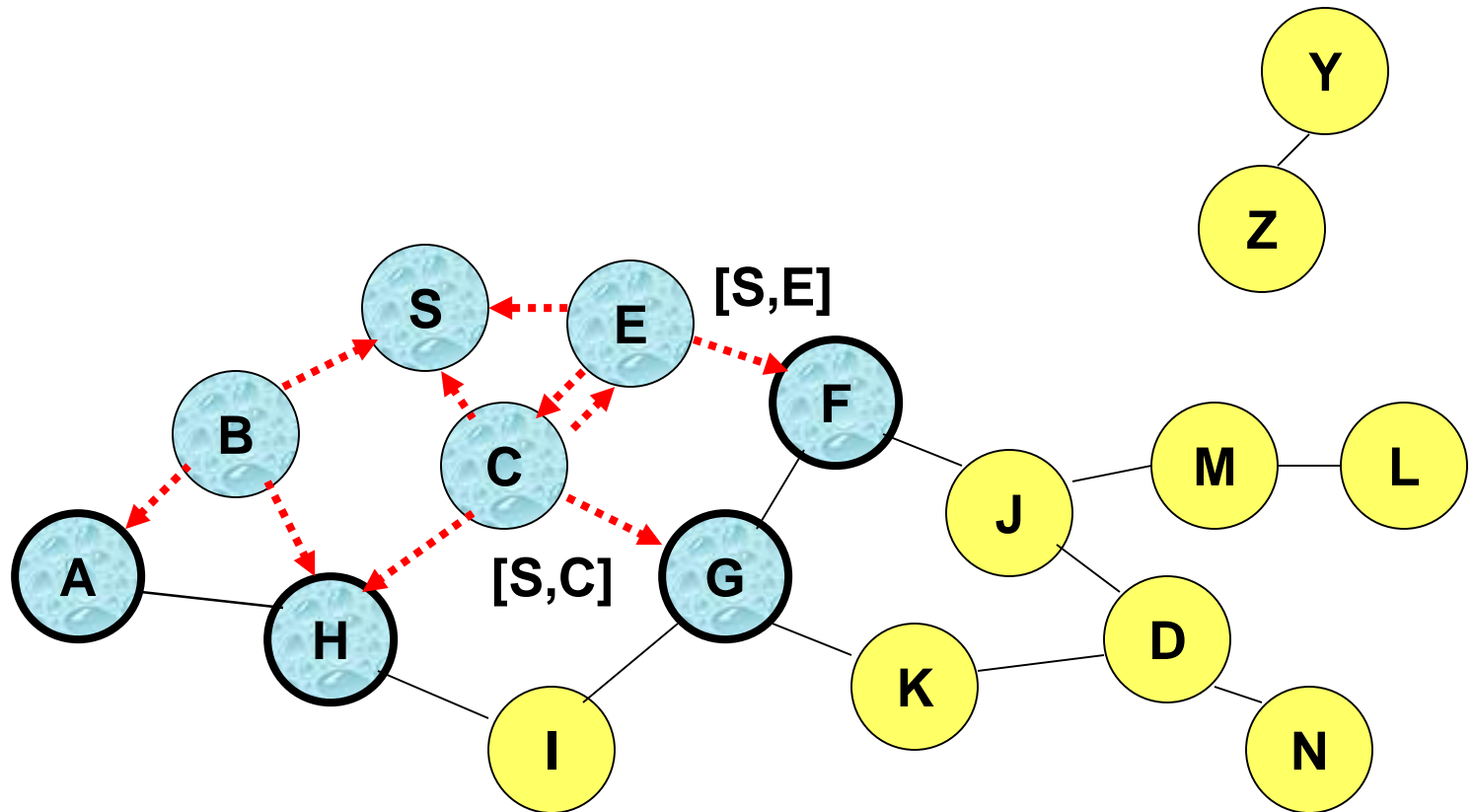


.....➔ Represents transmission of RREQ

[X,Y] Represents list of identifiers appended to RREQ



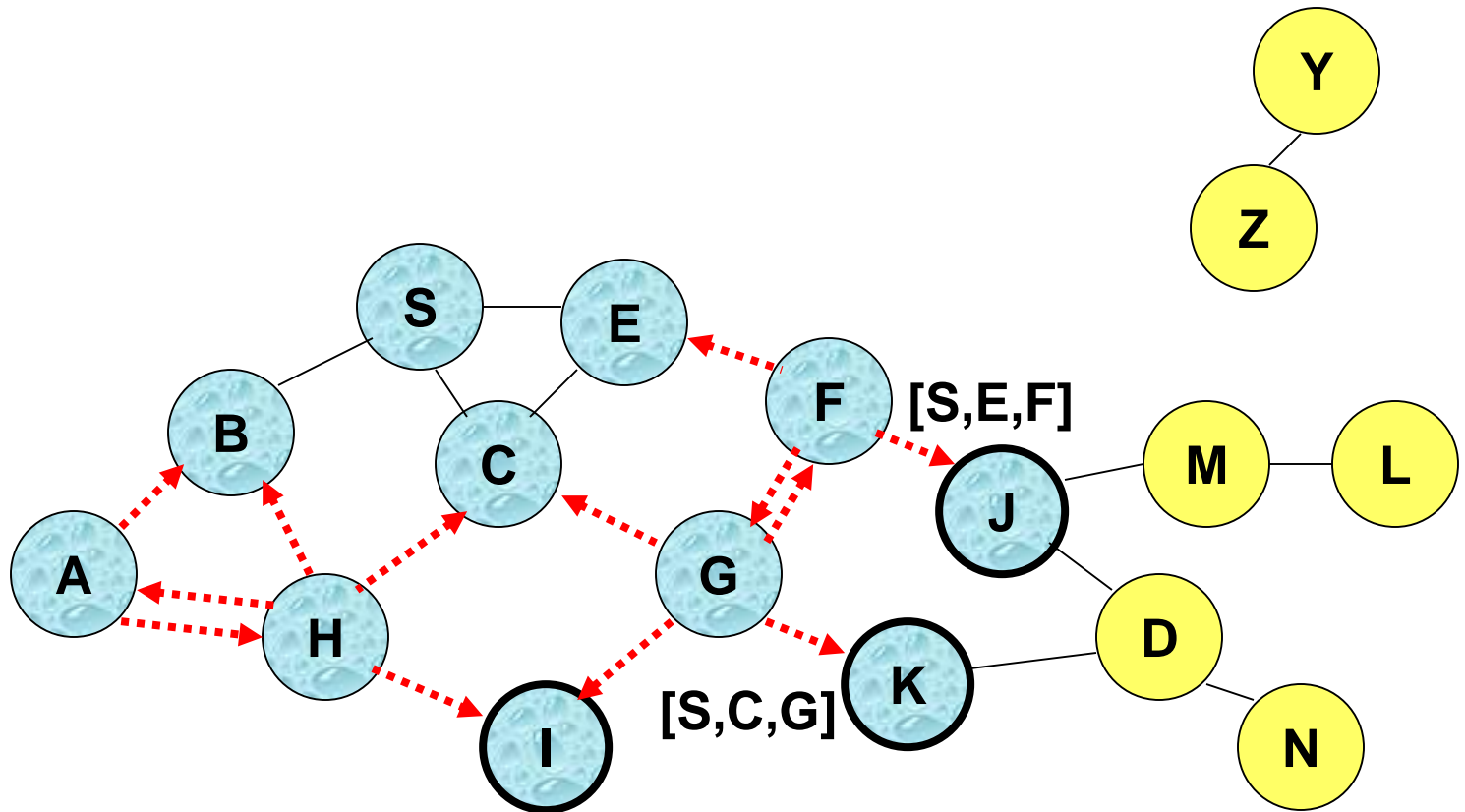
Route Discovery in DSR



- Node H receives packet RREQ from two neighbors:
potential for collision

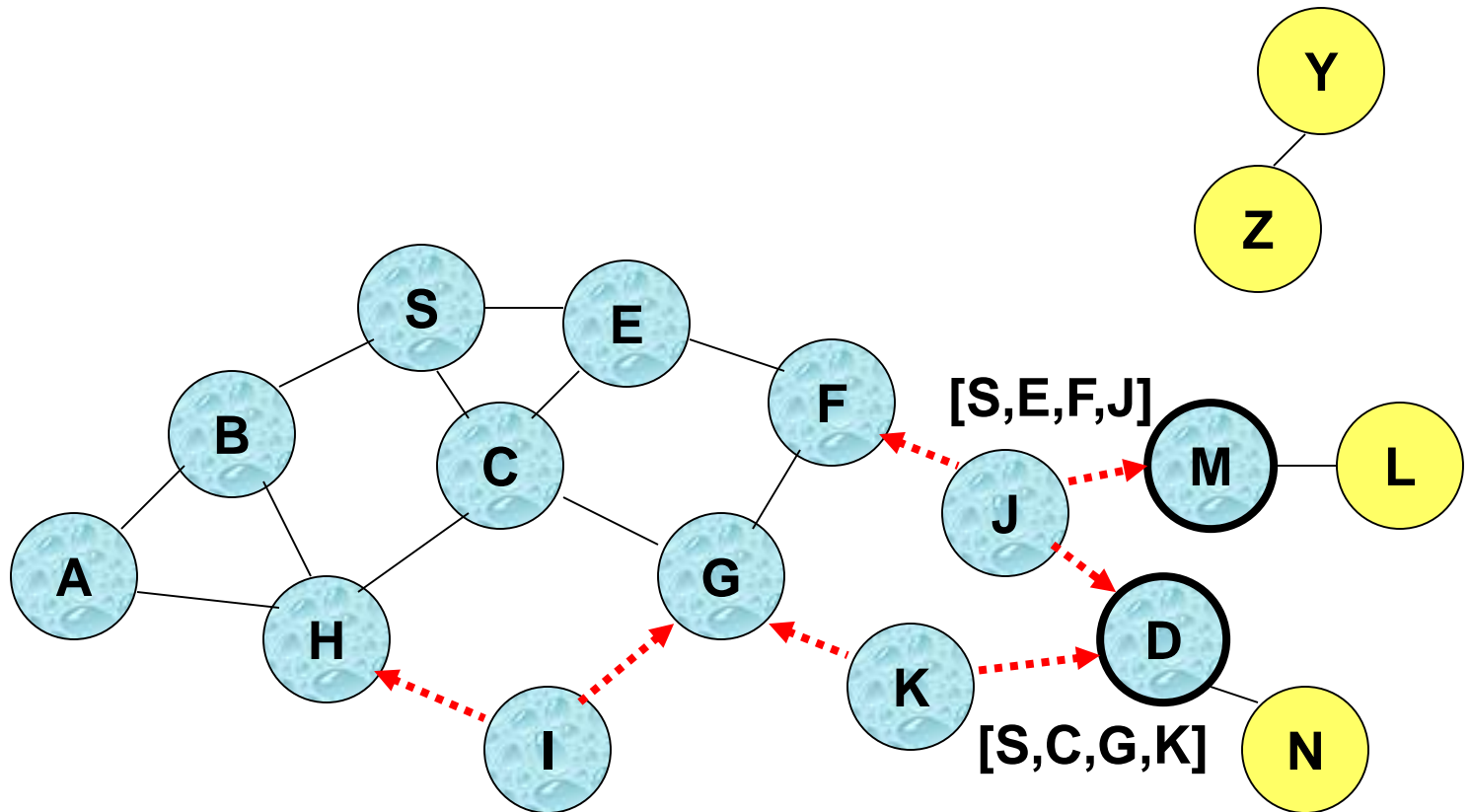


Route Discovery in DSR



- Node C receives RREQ from G and H, but does not forward it again, because node C has **already forwarded RREQ once**

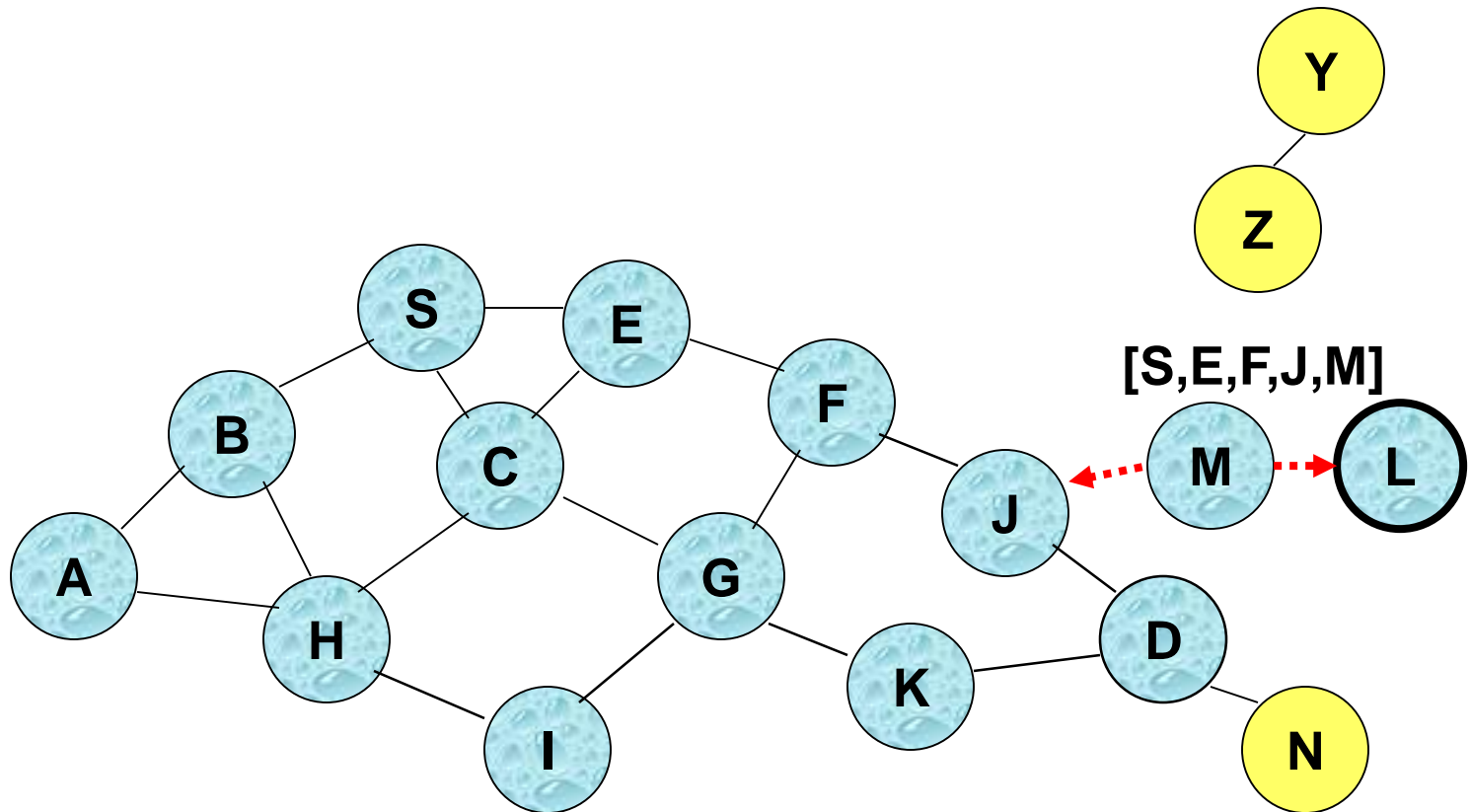
Route Discovery in DSR



- Nodes J and K both broadcast RREQ to node D
- Since nodes J and K are **hidden** from each other, their **transmissions may collide**



Route Discovery in DSR



- Node D **does not forward** RREQ, because node D is the **intended target** of the route discovery

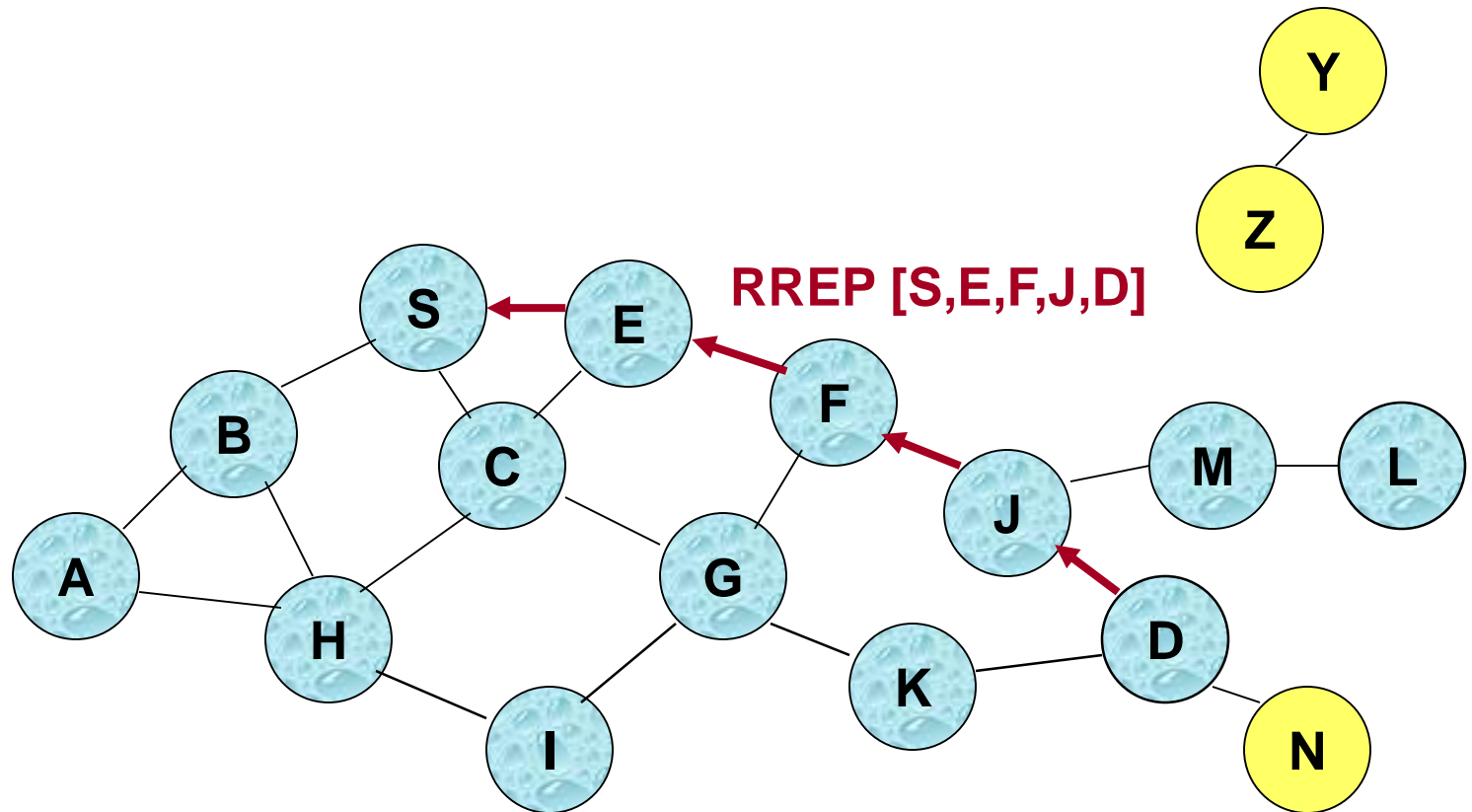


Route Discovery in DSR

- o Destination D on receiving the first RREQ, sends a **Route Reply (RREP)**
- o RREP is sent on a route obtained by **reversing** the route appended to received RREQ
- o RREP includes the route from S to D on which RREQ was received by node D



Route Reply in DSR



← Represents RREP control message

Route Reply in DSR

- o Route Reply can be sent by reversing the route in Route Request (RREQ) only if links are guaranteed to be bi-directional
 - To ensure this, RREQ should be forwarded only if it received on a link that is known to be bi-directional
- o If unidirectional (asymmetric) links are allowed, then RREP may need a route discovery for S from node D
 - Unless node D already knows a route to node S
 - If a route discovery is initiated by D for a route to S, then the Route Reply is piggybacked on the Route Request from D.
- o If IEEE 802.11 MAC is used to send data, then links have to be bi-directional (since Ack is used)

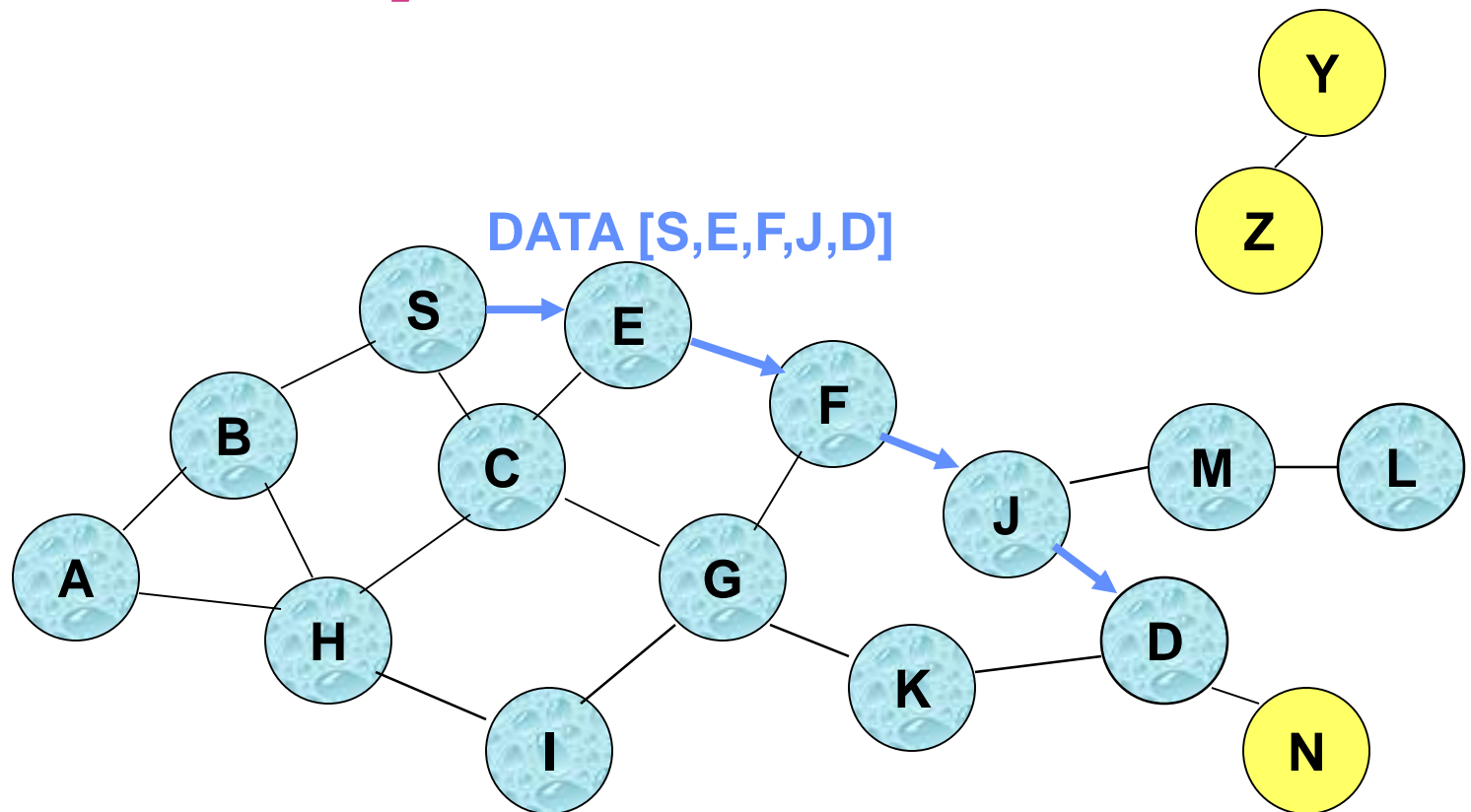


Dynamic Source Routing (DSR)

- o Node S on receiving RREP, caches the route included in the RREP
- o When node S sends a data packet to D, the entire route is included in the packet header
 - hence the name **source routing**
- o Intermediate nodes use the **source route** included in a packet to determine to whom a packet should be forwarded



Data Delivery in DSR



Packet header size grows with route length

Dynamic Source Routing: Advantages

- o Routes maintained only between nodes who need to communicate
 - reduces overhead of route maintenance
- o Route caching can further reduce route discovery overhead
- o A single route discovery may yield many routes to the destination, due to intermediate nodes replying from local caches



Dynamic Source Routing: Disadvantages

- o Packet header size grows with route length due to source routing
- o Flood of route requests may potentially reach all nodes in the network
- o Care must be taken to avoid collisions between route requests propagated by neighboring nodes
 - insertion of random delays before forwarding RREQ
- o Increased contention if too many route replies come back due to nodes replying using their local cache
 - Route Reply *Storm* problem
 - Reply storm may be eased by preventing a node from sending RREP if it hears another RREP with a shorter route



Ad Hoc On-Demand Distance Vector Routing (AODV)

[Perkins99Wmcsa]

- o DSR includes source routes in packet headers
- o Resulting large headers can sometimes degrade performance
 - particularly when data contents of a packet are small
- o AODV attempts to improve on DSR by maintaining routing tables at the nodes, so that data packets do not have to contain routes
- o AODV retains the desirable feature of DSR that routes are maintained only between nodes which need to communicate

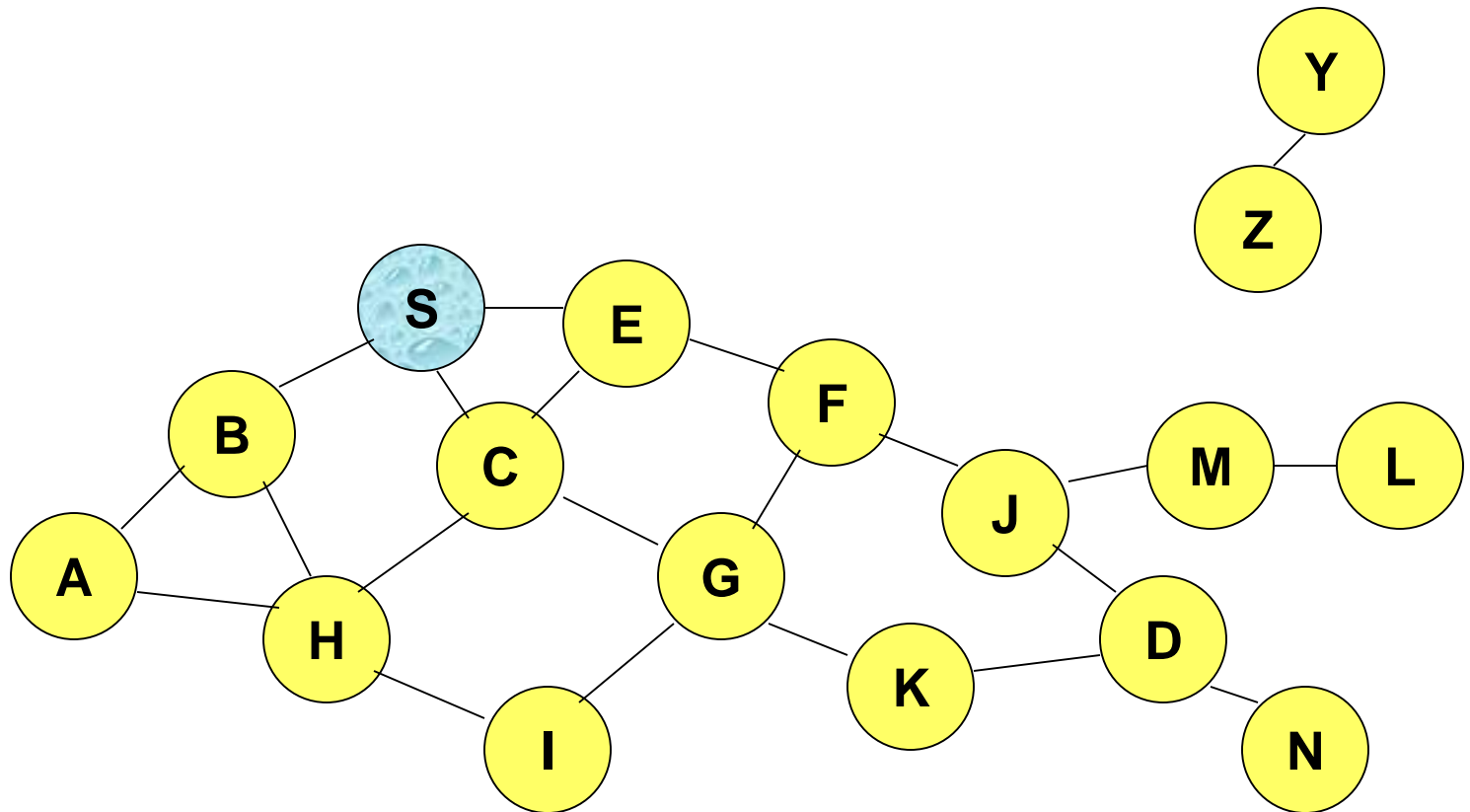


AODV

- o Route Requests (RREQ) are forwarded in a manner similar to DSR
- o When a node re-broadcasts a Route Request, it sets up a reverse path pointing towards the source
 - AODV assumes symmetric (bi-directional) links
- o When the intended destination receives a Route Request, it replies by sending a Route Reply
- o Route Reply travels along the reverse path set-up when Route Request is forwarded



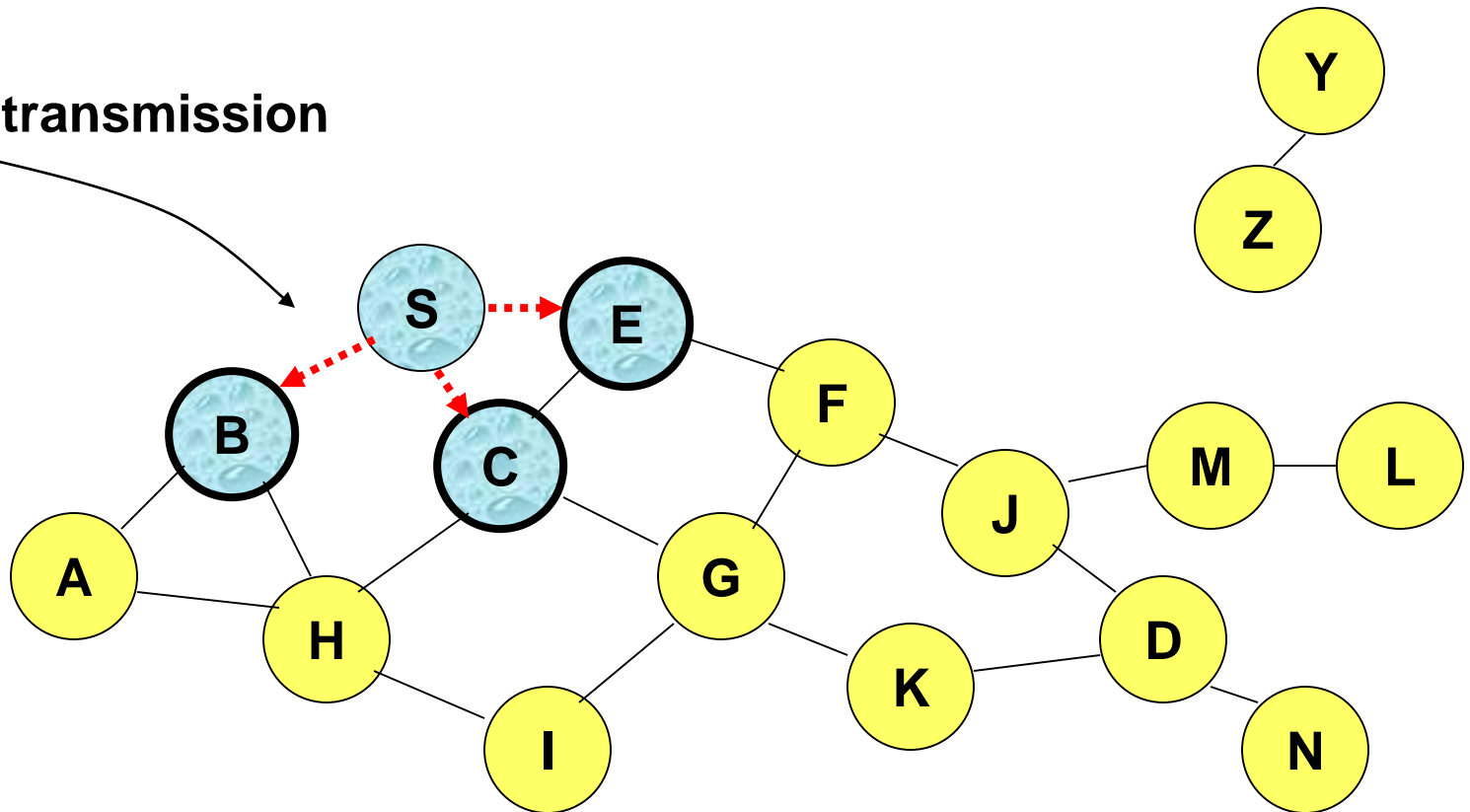
Route Requests in AODV



Represents a node that has received RREQ for D from S

Route Requests in AODV

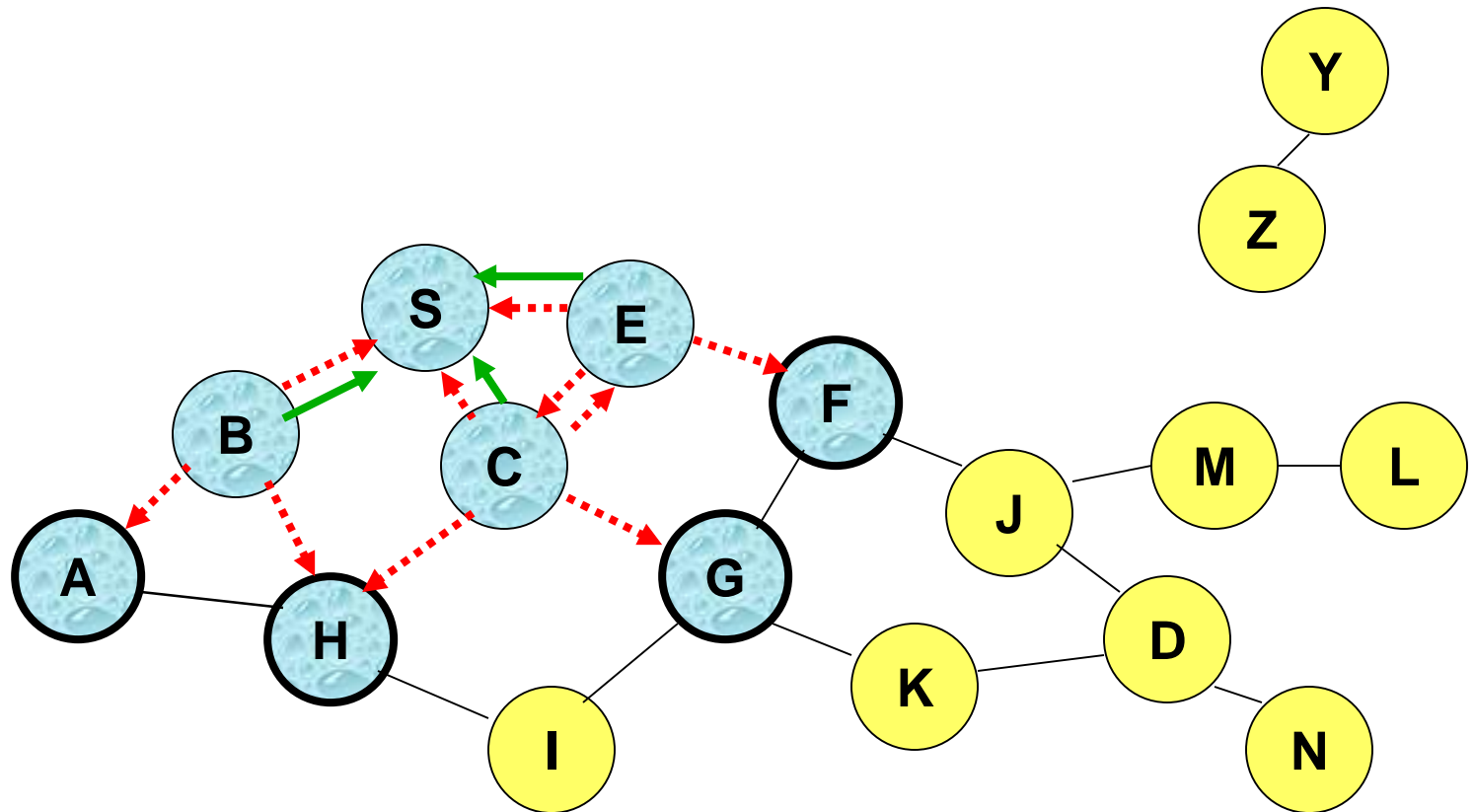
Broadcast transmission



.....➔ Represents transmission of RREQ



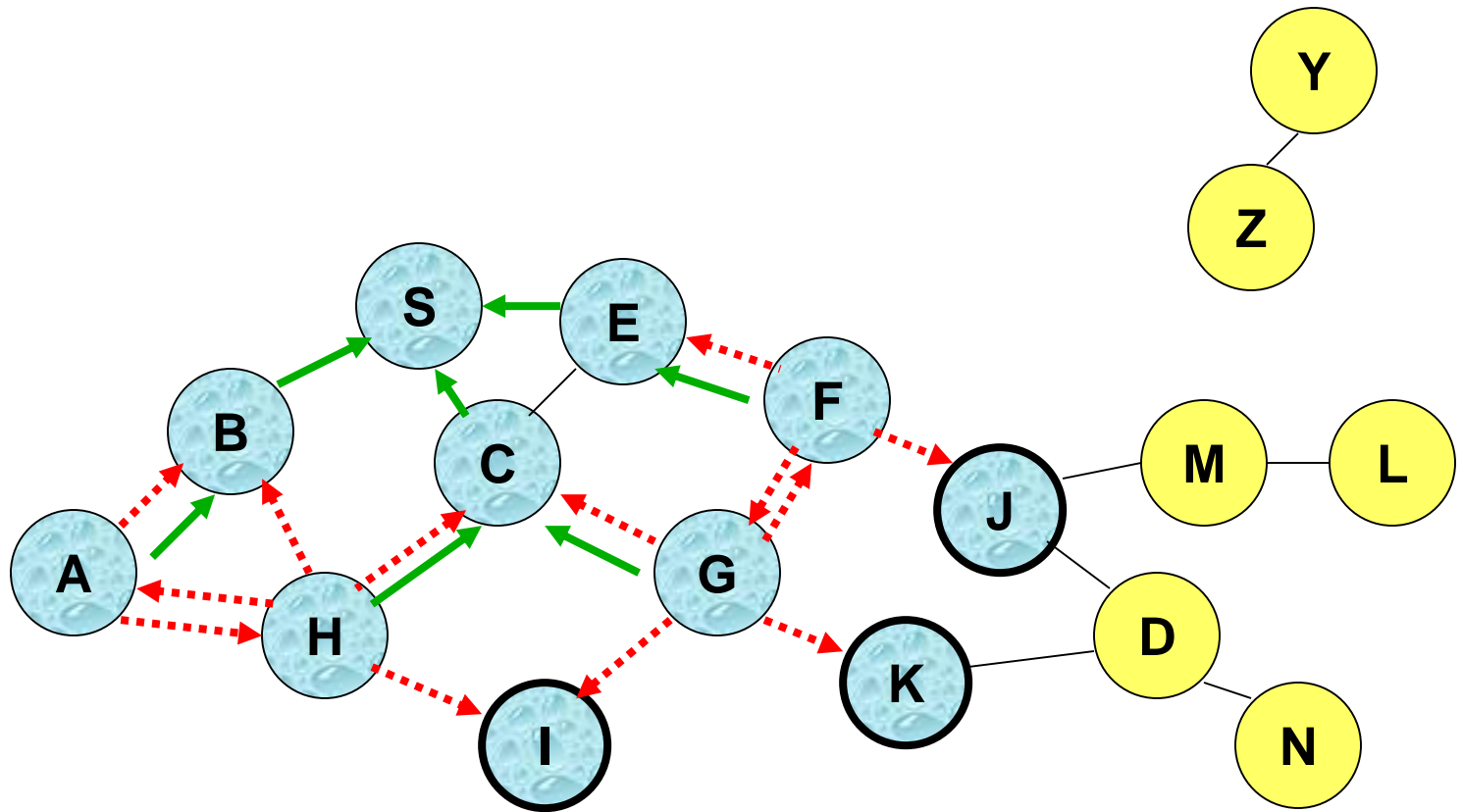
Route Requests in AODV



← Represents links on Reverse Path

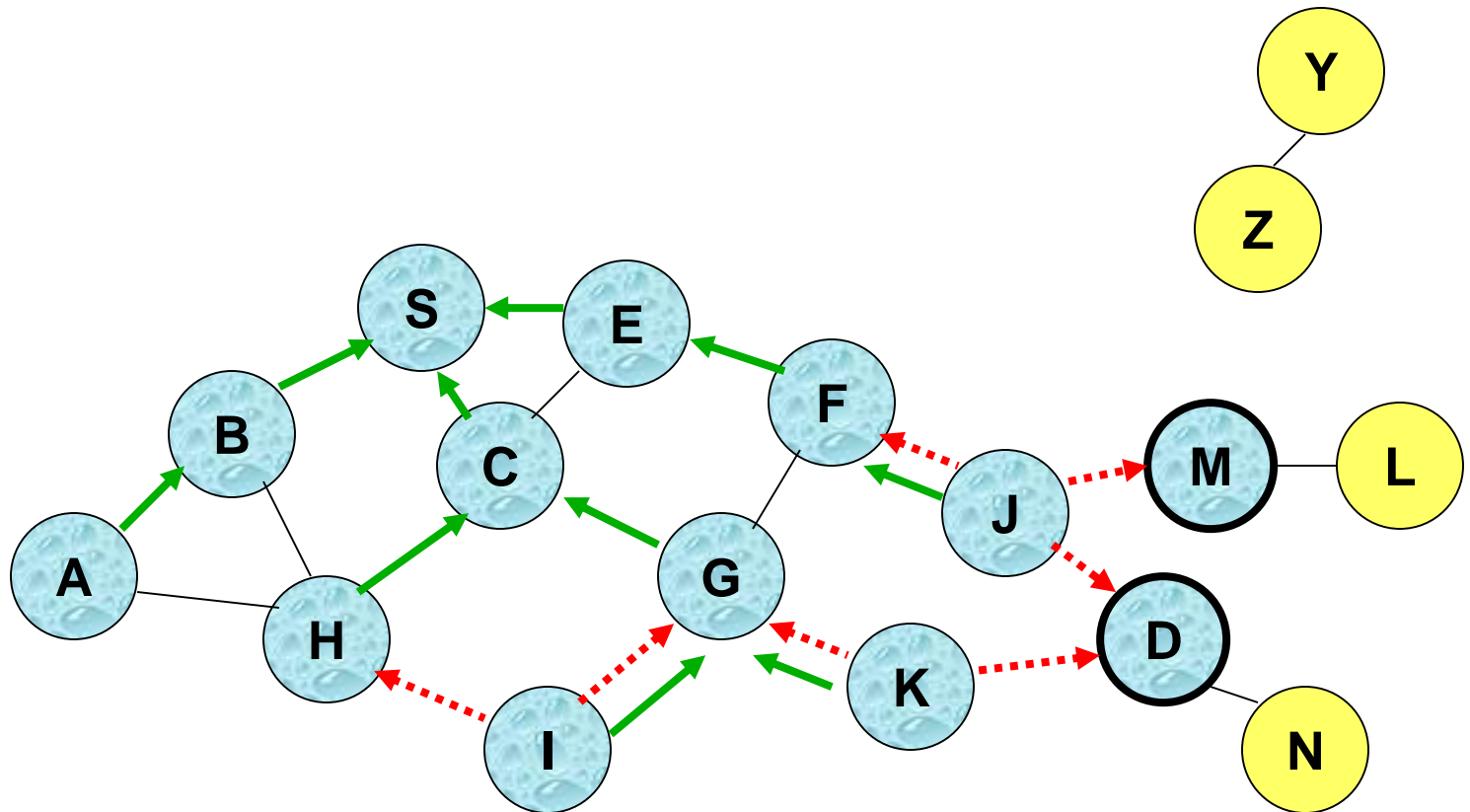


Reverse Path Setup in AODV

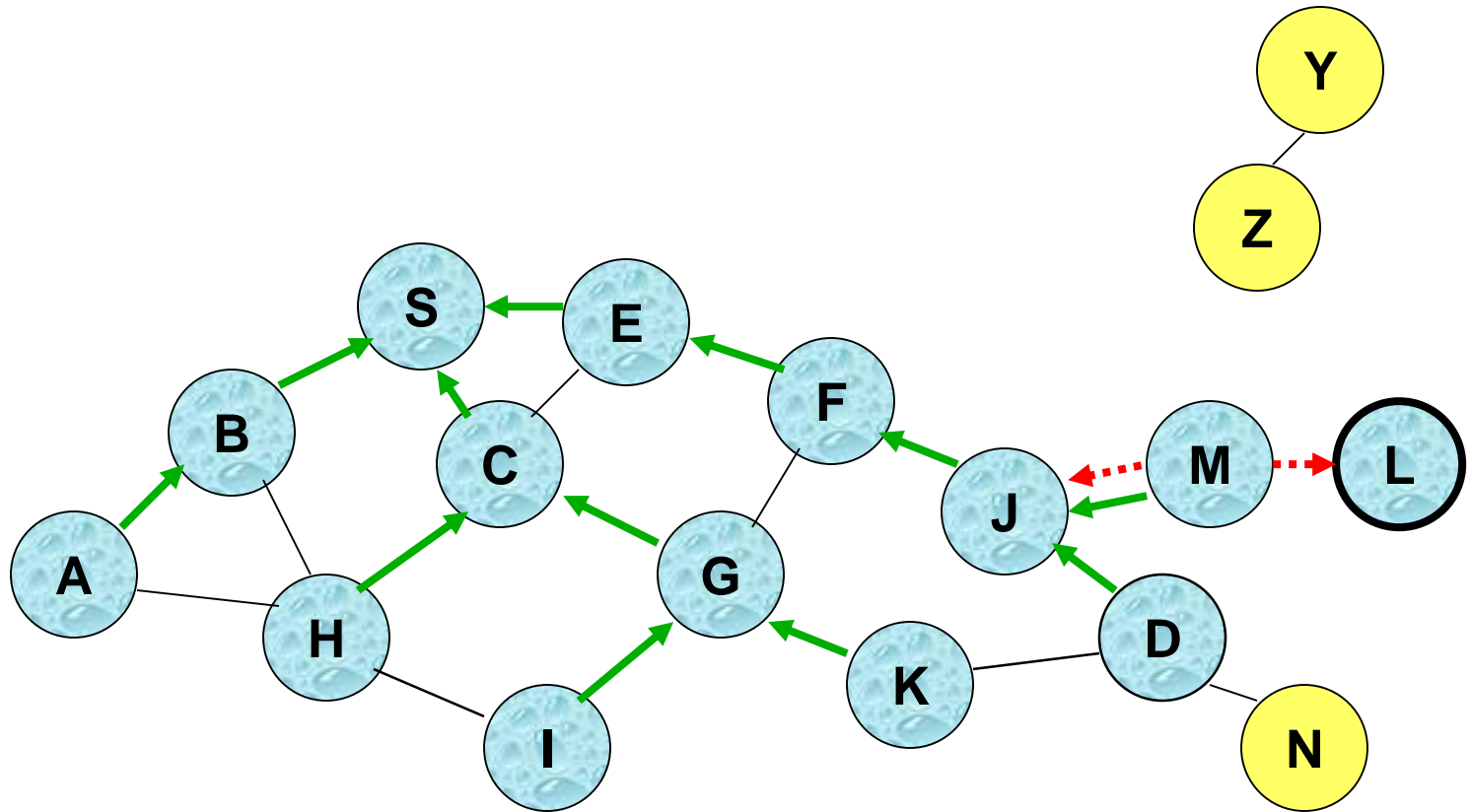


- Node C receives RREQ from G and H, but does not forward it again, because node C has **already forwarded RREQ once**

Reverse Path Setup in AODV



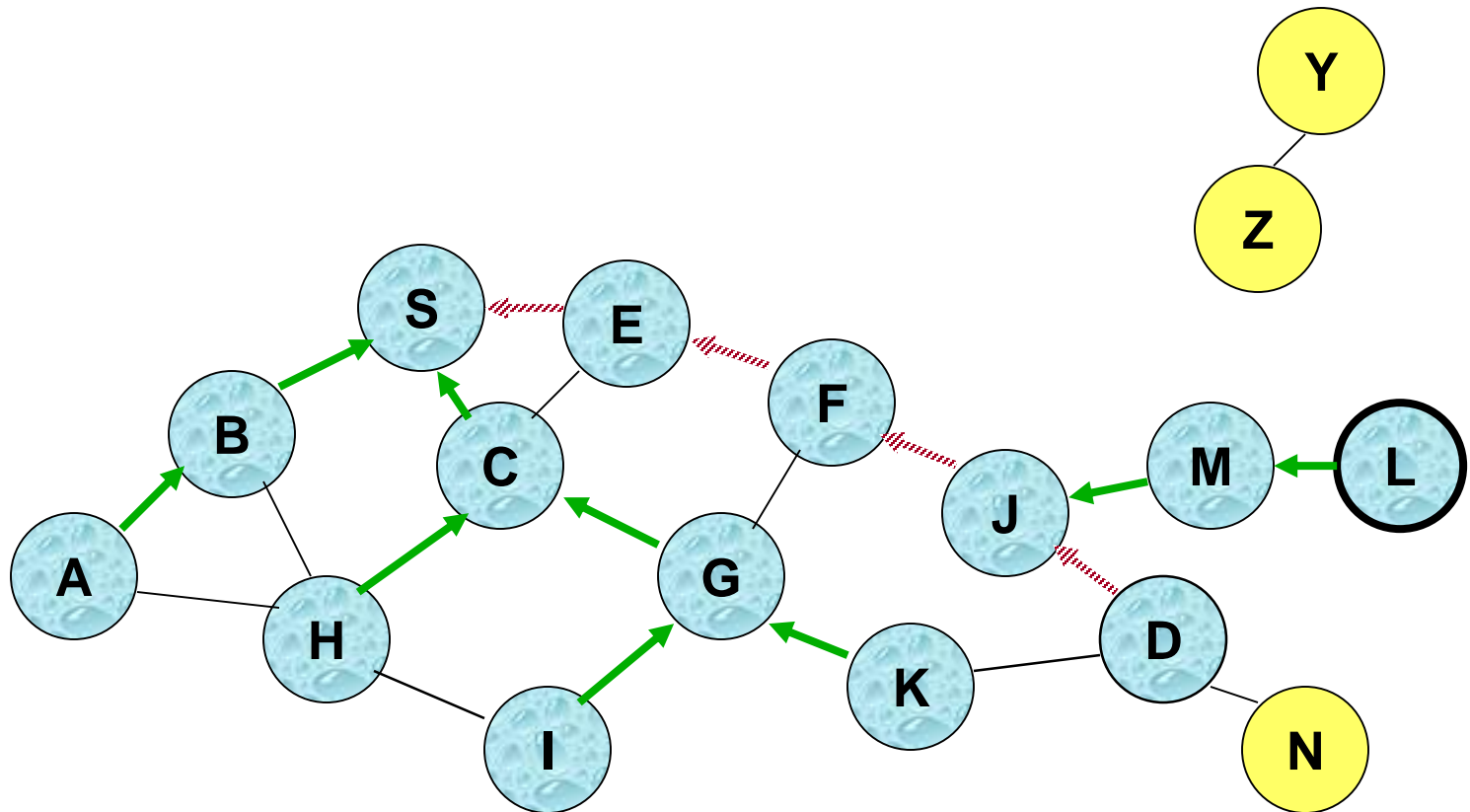
Reverse Path Setup in AODV



- Node D **does not forward** RREQ, because node D is the **intended target** of the RREQ



Route Reply in AODV



 Represents links on path taken by RREP

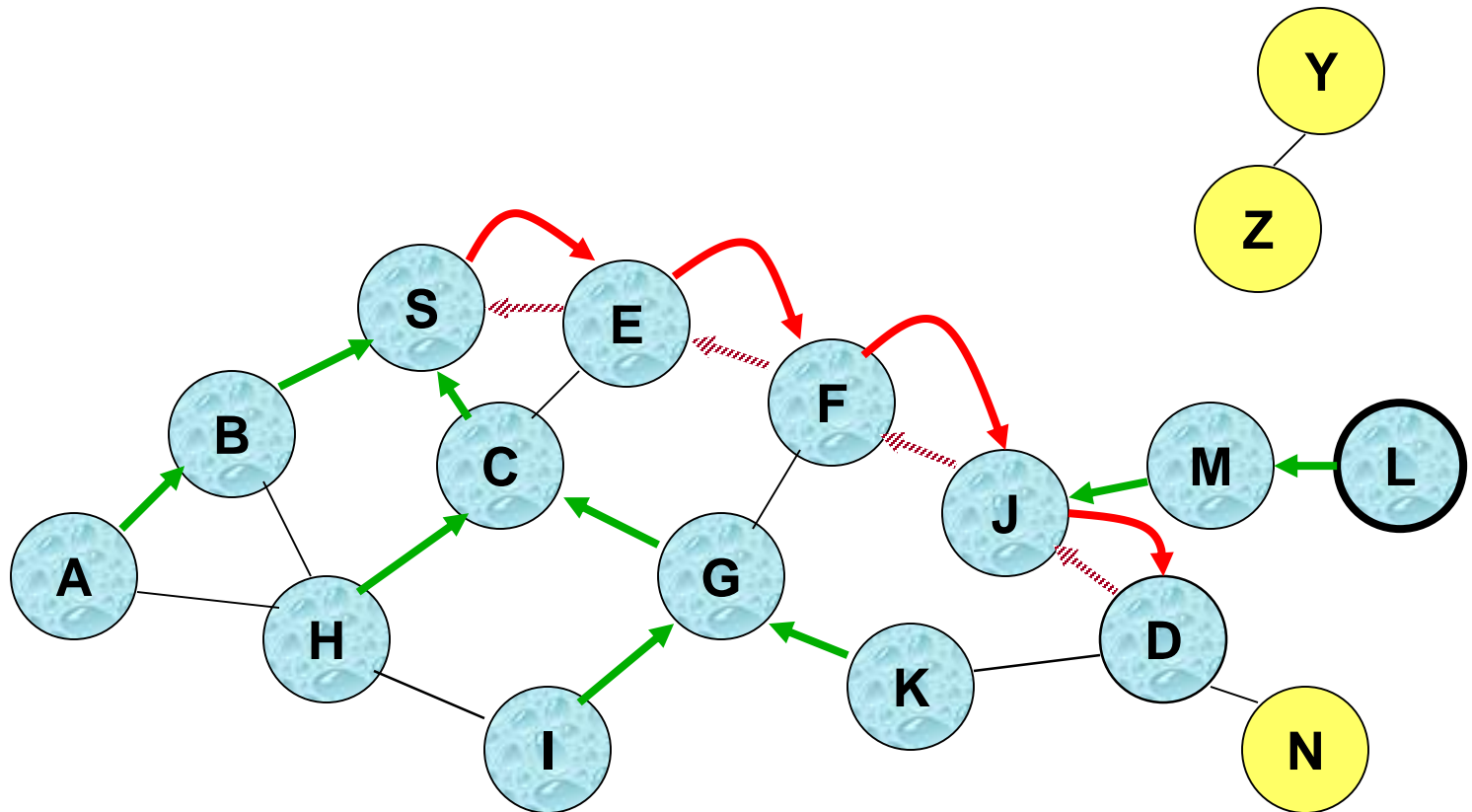


Route Reply in AODV

- o An **intermediate node** (not the destination) may also send a **Route Reply (RREP)** provided that it knows a **more recent path** than the one previously known to sender S
- o To determine whether the path known to an intermediate node is more recent, *destination sequence numbers* are used
- o The likelihood that an intermediate node will send a Route Reply when using AODV is not as high as DSR
 - A new Route Request by node S for a destination is assigned a higher destination sequence number. An intermediate node, which knows a route, but with a smaller sequence number, **cannot send** Route Reply



Forward Path Setup in AODV



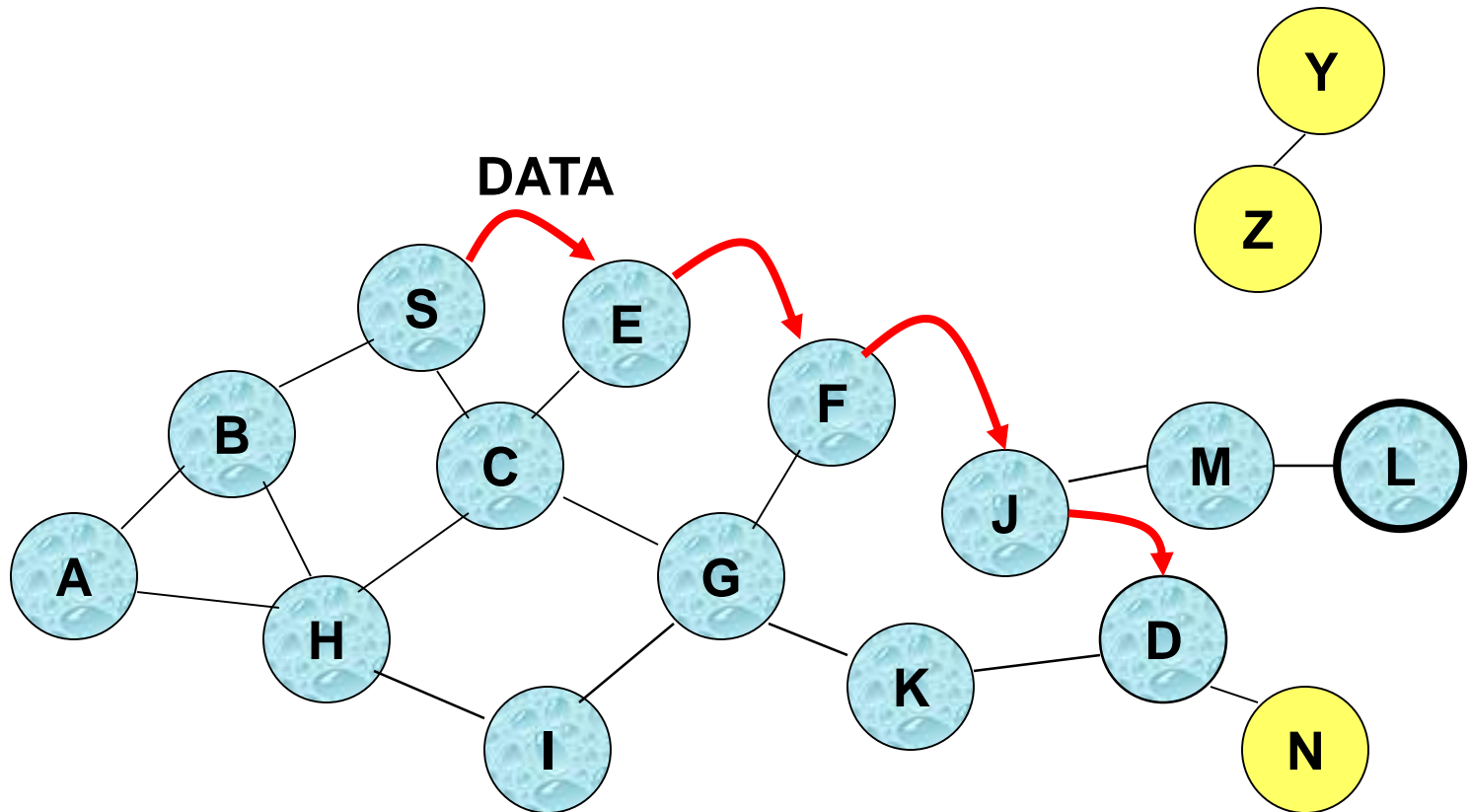
Forward links are setup when RREP travels along the reverse path



Represents a link on the forward path



Data Delivery in AODV



Routing table entries used to forward data packet.
Route is *not* included in packet header.



Summary: AODV

- o Routes need not be included in packet headers
- o Nodes maintain routing tables containing entries only for routes that are in active use
- o At most one next-hop per destination maintained at each node
 - Multi-path extensions can be designed
 - DSR may maintain several routes for a single destination
- o Unused routes expire even if topology does not change



Link State Routing [Huitema95]

- o Each node periodically floods status of its links
- o Each node re-broadcasts link state information received from its neighbor
- o Each node keeps track of link state information received from other nodes
- o Each node uses above information to determine next hop to each destination



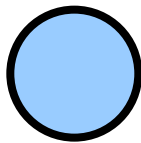
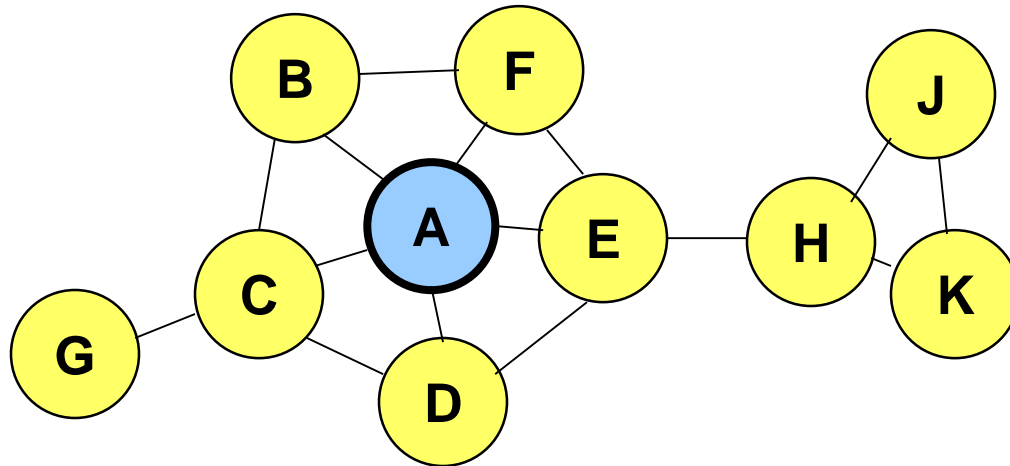
Optimized Link State Routing (OLSR)

- o The overhead of flooding link state information is reduced by requiring fewer nodes to forward the information
- o A broadcast from node X is only forwarded by its *multipoint relays*
- o Multipoint relays of node X are its neighbors such that each two-hop neighbor of X is a one-hop neighbor of at least one multipoint relay of X
 - Each node transmits its neighbor list in periodic beacons, so that all nodes can know their 2-hop neighbors, in order to choose the multipoint relays



Optimized Link State Routing (OLSR)

o Nodes C and E are multipoint relays of node A

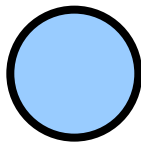
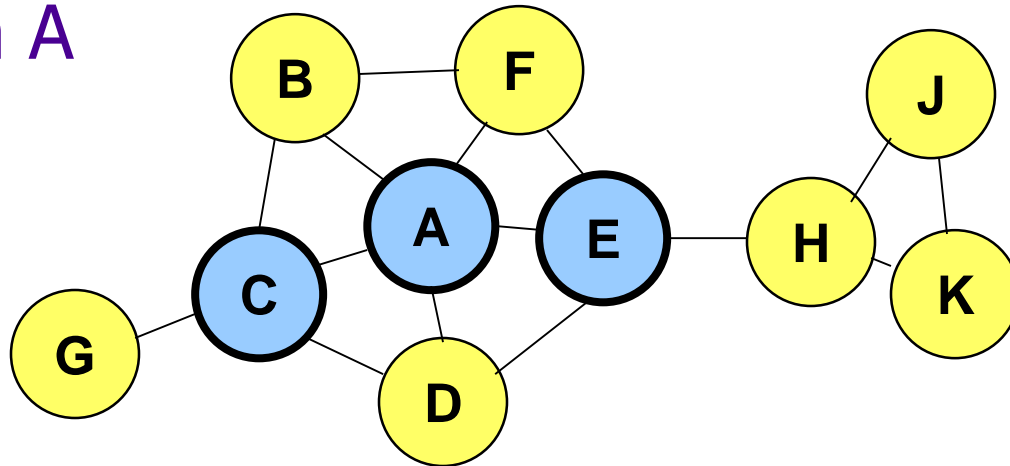


Node that has broadcast state information from A



Optimized Link State Routing (OLSR)

o Nodes C and E forward information received from A

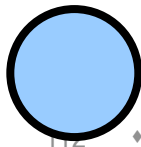
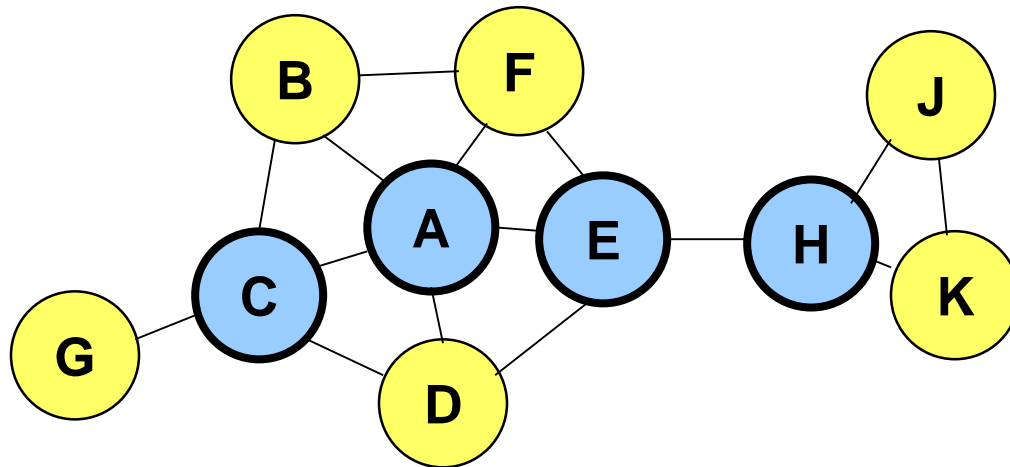


Node that has broadcast state information from A



Optimized Link State Routing (OLSR)

- o Only node E is a multipoint relay for node H
- o E has already forwarded the same information once



Node that has broadcast state information from A



Summary: OLSR

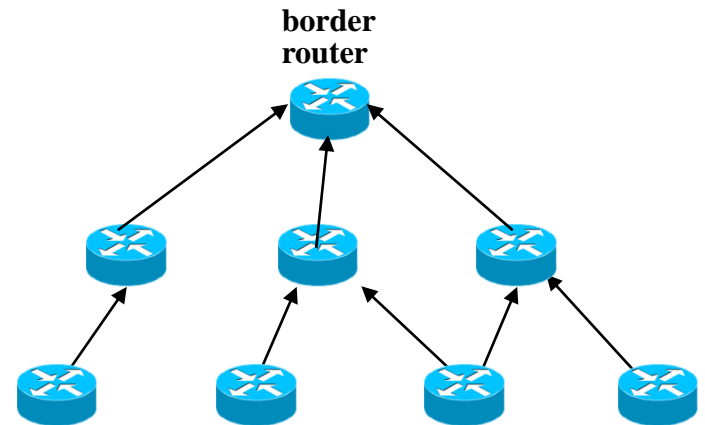
- o OLSR floods information through the multipoint relays
- o The flooded information itself is for links connecting nodes to respective multipoint relays
- o Nodes need to calculate routes (shortest path trees) based on link-state knowledge, typically using the Dijkstra algorithm
- o Routes used by OLSR only include multipoint relays as intermediate nodes



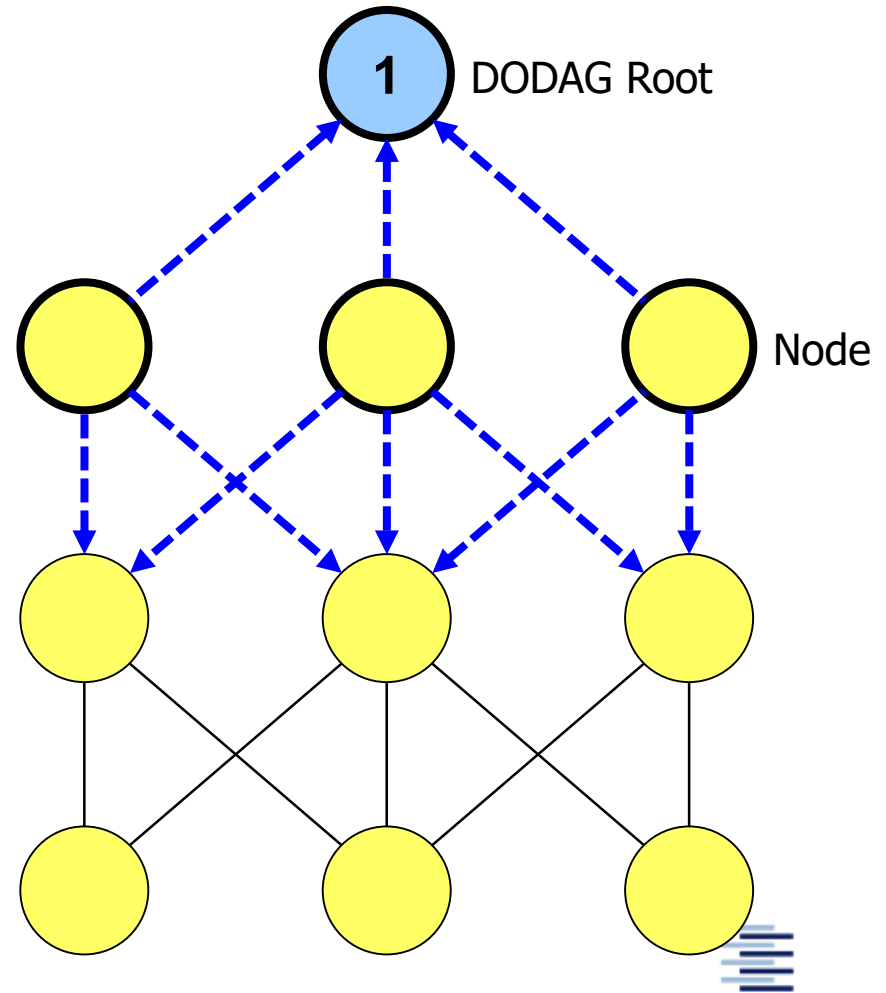
RPL - Routing Protocol for Low Power and Lossy Networks (LLN)

– RFC 6550

- ▶ Optimized for low-energy networks (without mobility)
- ▶ Destination Oriented Directed Acyclic Graph (DODAG)
- ▶ Routing state propagation
 - ▶ Conventional:
 - ▶ Link-state: scoped flooding
 - ▶ Distance-vector: periodic routing beacons
 - ▶ Trickle:
 - ▶ adaptive exchange rate
- ▶ Spatial diversity
 - ▶ A router maintains multiple potential parents
- ▶ Expressive link metrics
 - ▶ ETX: Estimated Number of Transmissions



RPL Topology Creation - Upward



RPL Topology Creation - Upward



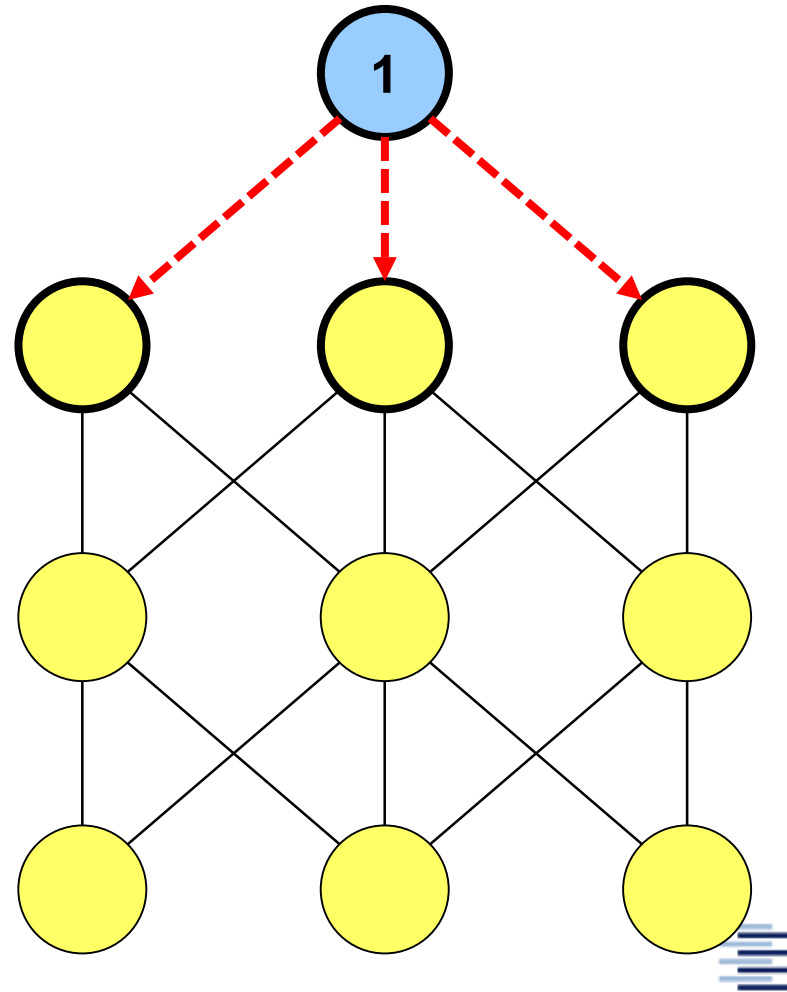
Node in DODAG



DODAG Information Solicitation (DIS)



DODAG Information Object (DIO)



RPL Topology Creation - Upward



Node in DODAG



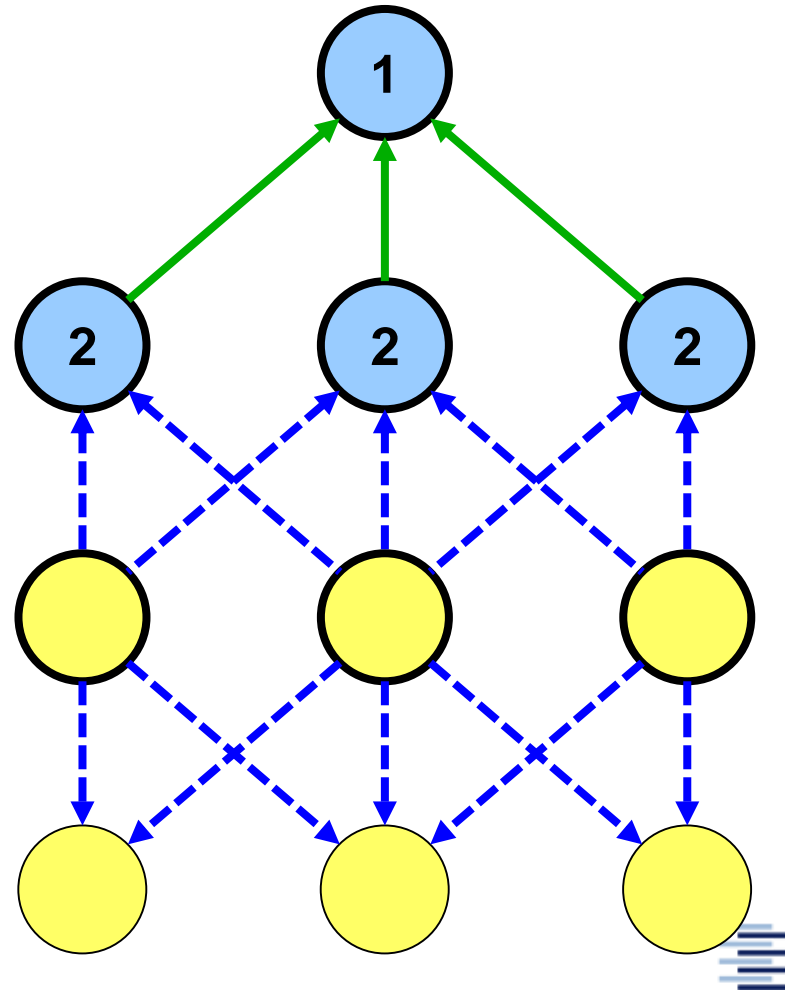
DODAG Information Solicitation (DIS)



DODAG Information Object (DIO)



DODAG Upward Link



RPL Topology Creation - Upward



Node in DODAG



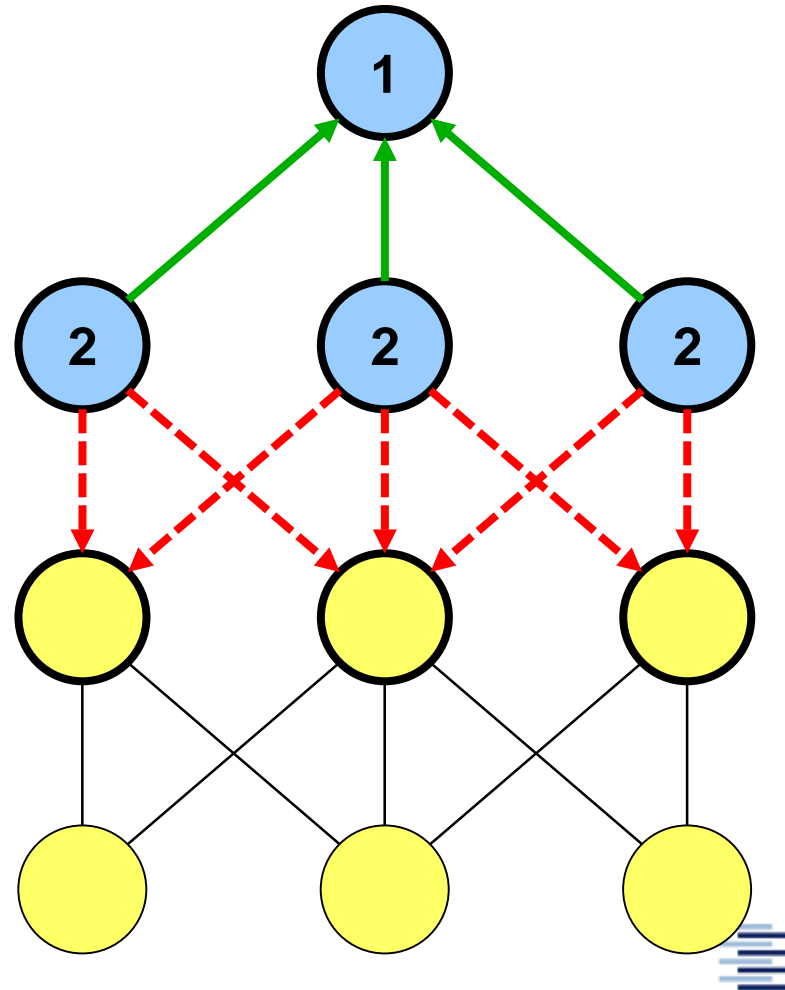
DODAG Information Solicitation (DIS)



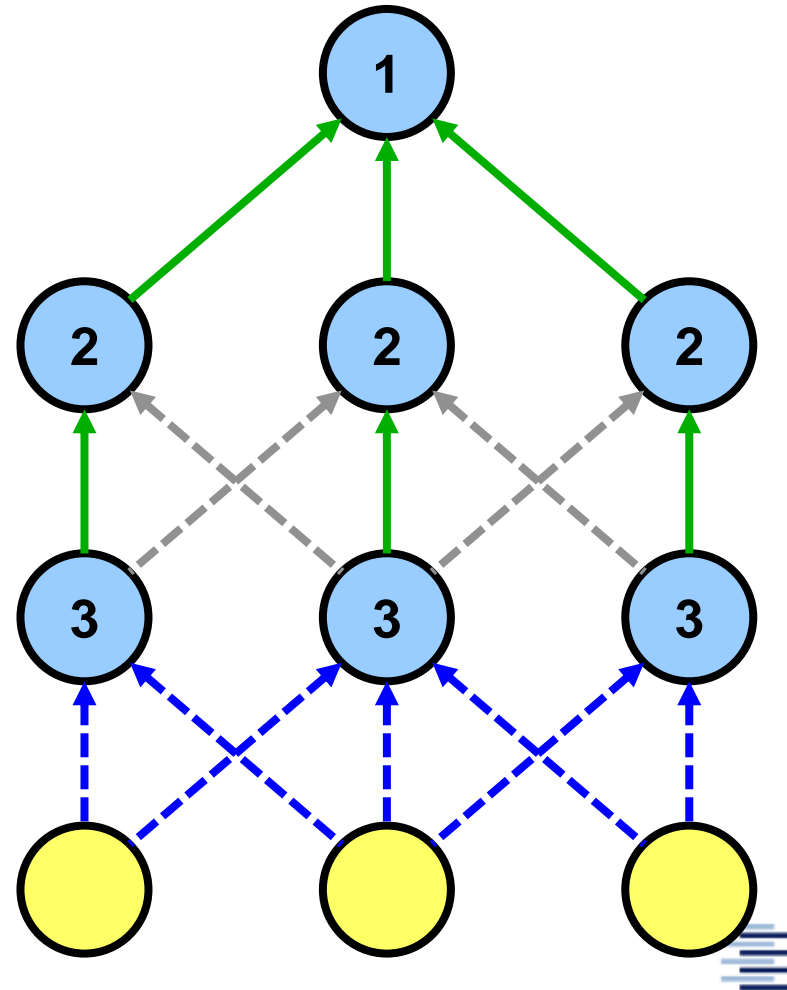
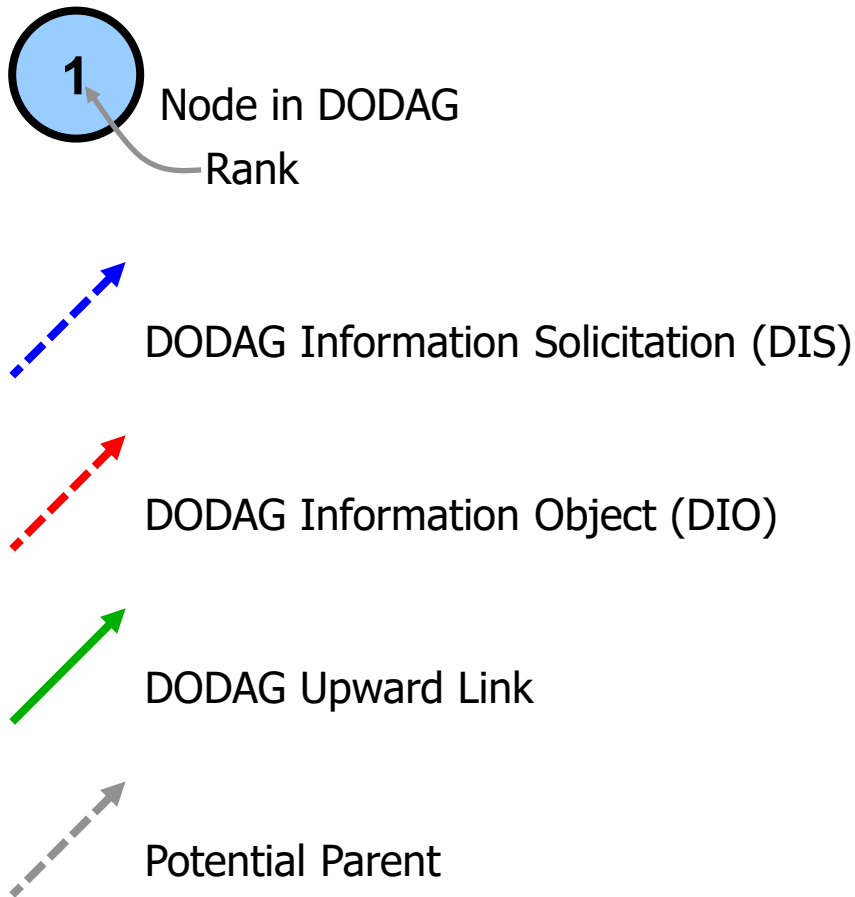
DODAG Information Object (DIO)



DODAG Upward Link



RPL Topology Creation - Upward



RPL Topology Creation - Upward



Node in DODAG



DODAG Information Solicitation (DIS)



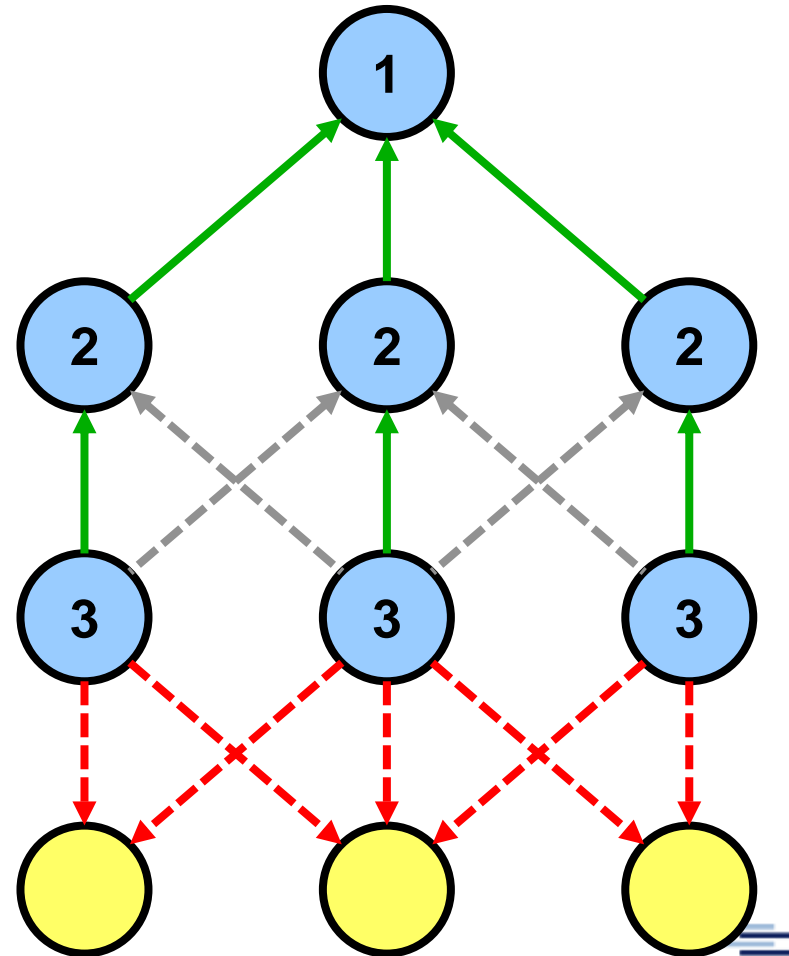
DODAG Information Object (DIO)



DODAG Upward Link



Potential Parent



RPL Topology Creation - Upward



Node in DODAG



DODAG Information Solicitation (DIS)



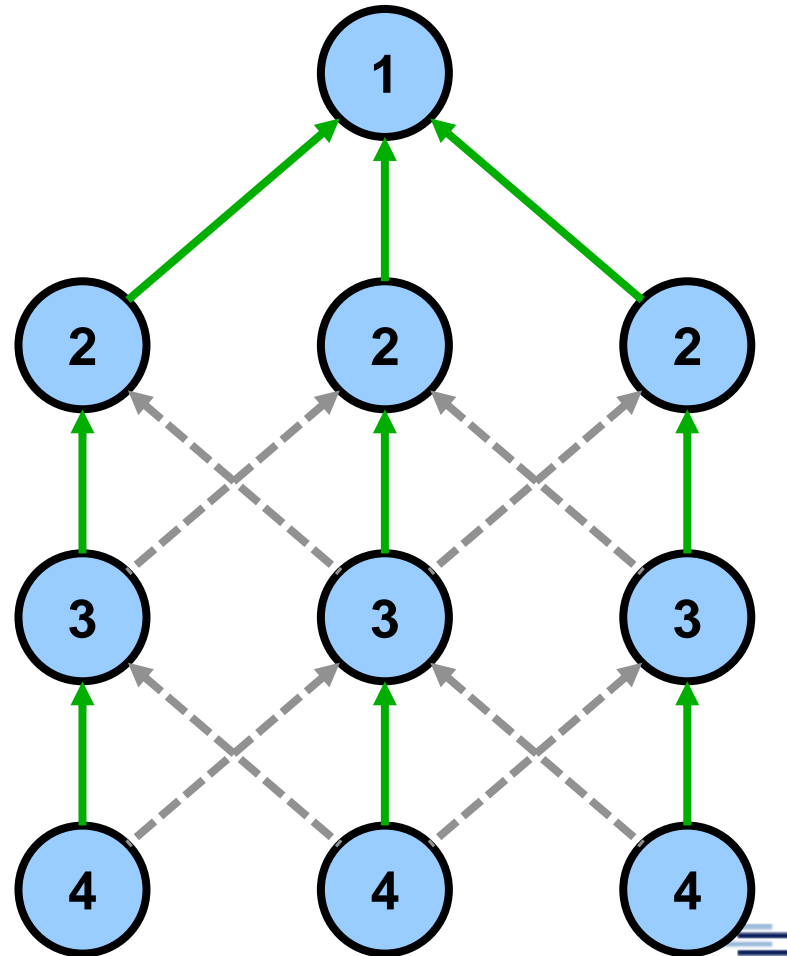
DODAG Information Object (DIO)



DODAG Upward Link



Potential Parent



RPL Topology

- o Downward routes created analogously
- o Two routing modes
 - Non-storing: without local routing tables
 - Local routing: Uptree (default) to root
 - Source routes issued at root
 - Storing: with local routing tables
 - Local routing decisions forward directly into subtrees
- o Topology maintenance: New DAG version created on request



Further Routing Approaches

- o Improvements & Optimisations of Previous Protocols
- o Location Aided Routing
- o Clustering after Landmarking
- o Hierarchic / Anchored Routing
- o Power-Aware Routing
- o ...



Bibliography

- o Internet Society: *The Internet of Things: An Overview*, White Paper, Oct. 2015
<http://www.internetsociety.org/doc/iot-overview>
- o Zach Shelby, Carsten Bormann: *6LoWPAN: The Wireless Embedded Internet*, Wiley & Sons, 2009.
- C. Murthy and B. Manoj: *Ad Hoc Wireless Networks*, Pearson Prentice Hall, 2004.
- Charles Perkins: *Ad Hoc Networking*, Addison-Wesley, 2001.
- S. Sarkar, T. Basavaraju, C. Puttamadappa: *Ad Hoc Mobile Wireless Networks*, Auerbach Publications, 2008.
- Nitin H. Vaidya: *Mobile Ad Hoc Networks*, Tutorial at InfoCom 2006,
<http://www.crhc.uiuc.edu/wireless/talks/2006.Infocom.ppt>.
- P. Gupta and P. R. Kumar, “The capacity of wireless networks,” *IEEE Transactions on Information Theory*, vol. 46, no. 2, pp. 388–404, 2000.
- o Drafts, RFCs: tools.ietf.org, <http://www.rfc-editor.org>

