Internet of Things

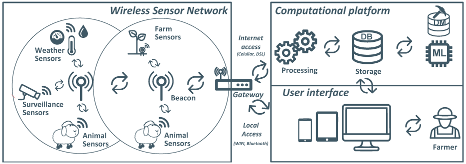
Mesh Networking

Ioannis Chatzigiannakis

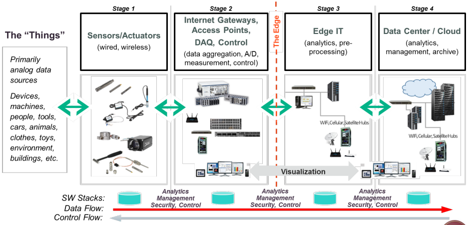
Sapienza University of Rome
Department of Computer, Control, and Management Engineering (DIAG)

Lecture 14:
Mesh Networking

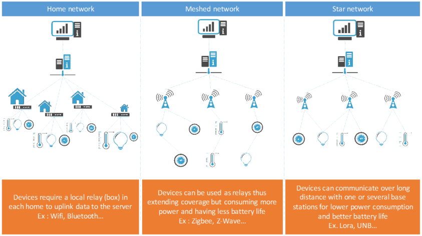
Cloud-Based Architecture



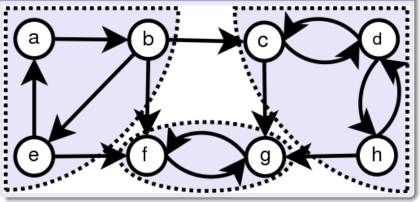
Edge-enabled Architecture



Different Topologies



Generic Mesh Network Topology



- Gateway – Allow to pass messages between networks.
- Repeater – Forward messages between end devices.
- End Point – Mesh-only devices that do not route messages for other devices in the network.

Mesh Networks – Concepts

- Do not rely on existing, pre-deployed infrastructure.
- No need for a centralized administration.
- Using Wireless communication channels.
- Communication among nodes is possible through intermediate nodes that act as Repeaters.
- Instant Networking – Adhoc Networking.
- Possibly short-lived networks.
- Nodes position might change – Dynamic networks
- Nodes might be mobile:
  - Passive Mobility – Nodes are attached to mobile objects, e.g., Smartphone, Car sensors, no control on the motion.
  - Active Mobility – Nodes are mobile objects, e.g., Robots, Drones, they can control their motion.

Mesh Networks – Variations

- Fully Symmetric Environment:
  - All nodes have identical capabilities and responsibilities
- Asymmetric Capabilities:
  - Transmission ranges and radios may differ.
  - Some nodes battery operated other connected to power supply.
  - Battery life at different nodes may differ.
  - Processing capacity may be different at different nodes.
  - Some nodes may be fixed other may be mobile.
  - Speed of movement.
  - ...
- Asymmetric Responsibilities:
  - Some nodes act as repeaters.
  - Some nodes act as leaders of nearby nodes.
  - Some nodes have multiple network interfaces – act as gateways.
  - ...

Mesh Networks – More Variations

- Traffic characteristics may differ in different mesh networks:
  - Bit rate.
  - Timeliness constraints.
  - Reliability requirements.
  - Unicast / multicast / geocast.
  - Host-based addressing / content-based addressing / capability-based addressing.
- May co-exist (and co-operate) with an infrastructure-based network.
- ...

Mesh Networks – Even more Variations

- Mobility patterns may be different:
  - People sitting at an airport lounge.
  - City Taxi.
  - Children playing.
  - Military movements.
  - Personal area network.
  - ...
- Mobility characteristics:
  - Speed.
  - Predictability.
  - Directison of movement.
  - Pattern of movement.
  - Uniformity (or lack thereof) of mobility characteristics among different nodes.
  - ...

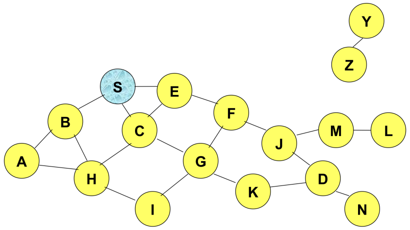
Basic Communication Problem

- We assume a source node S
- We assume a destination node D
- How can S send a data packet P to D ?
- Simple/Basic Version:
  - Fully symmetric environment.
  - Static nodes.
  - Nodes act as repeaters.
  - Nodes have unique identities.
  - No wireless interferance.
  - No node failures.

Simple Solution: Flooding

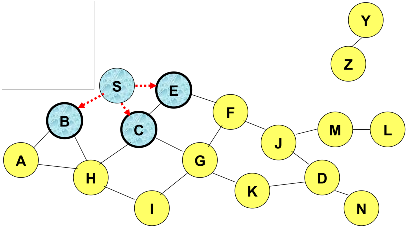
- Source node S broadcasts data packet P to all neighboring nodes.
- Each node receiving P forwards P to its neighbors.
- Packet P reaches destination node D provided that D is reachable from sender S.
- Destination node D does not forward the packet.
- Packet format:
  - Source node address.
  - Destination node address.
  - Sequence number used to avoid the possibility of forwarding the same packet more than once.
  - Payload – Actual data.

Flooding for Data Delivery



- Black lines – wireless "link"
- Red lines – wireless broadcast transmission

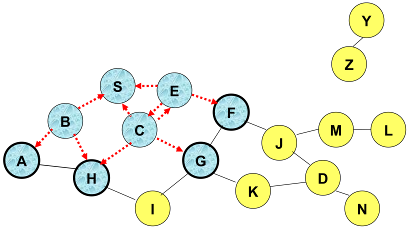
Flooding for Data Delivery



- Black lines – wireless “link”
- Red lines – wireless broadcast transmission

Mesh Networking
Basic Communicaton in Mesh Networks

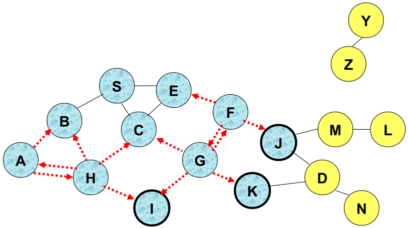
Flooding for Data Delivery



- Black lines – wireless “link”
- Red lines – wireless broadcast transmission

Mesh Networking
Basic Communicaton in Mesh Networks

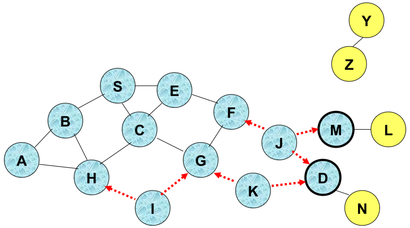
Flooding for Data Delivery



- Black lines – wireless “link”
- Red lines – wireless broadcast transmission

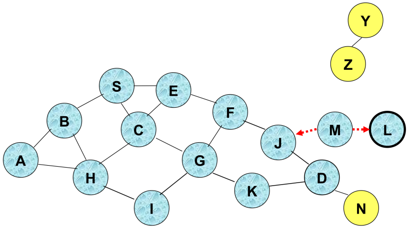
Mesh Networking
Basic Communicaton in Mesh Networks

Flooding for Data Delivery



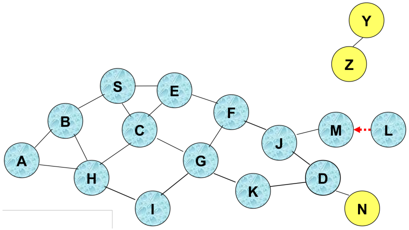
- Black lines – wireless “link”
- Red lines – wireless broadcast transmission

Flooding for Data Delivery



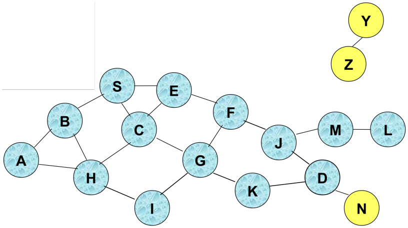
- Black lines – wireless "link"
- Red lines – wireless broadcast transmission

Flooding for Data Delivery



- Black lines – wireless "link"
- Red lines – wireless broadcast transmission

Flooding for Data Delivery



- Black lines – wireless "link"
- Red lines – wireless broadcast transmission

Characteristics of Flooding

- Complete network is "flooded" with the network packet P.
- Use of sequence numbers creates a "wave" like flow towards the periphery of the network.
- Nodes possibly receiving same packet from multiple neighbors.
- Packet may not be delivered to destination node.
- Nodes unreachable from S do not receive the packet.
- Nodes for which all paths from S go through destination D also do not receive the packet.

Characteristics of Flooding

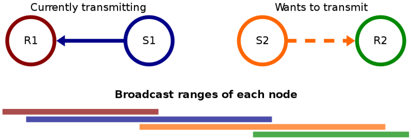
Advantages:

- Simplicity.
- No need to know/learn topology of network.
- Potentially high reliability – packets may be delivered to the destination on multiple paths.
- When transmission rate is low works well.

Disadvantages:

- Potentially, very high overhead – packets may be delivered to too many nodes who do not need to receive them.
- Potentially lower reliability of data delivery – hard to implement reliable broadcast without significantly increasing overhead.

Exposed terminal problem



- Packet transmission fails due to co-channel interferance.
- RTS/CTS mechanisms help to solve this problem only if:
  - Nodes are sychronized.
  - Packet sizes are fixed.
  - Data rates are the same for both the transmitting nodes.

Network Discovery & Routing

- If we discover the topology of the network, we may identify routes between Source and Destination.
- We use Flooding to discover the topology.
- If topology does not change often then Flooding is performed for a limited amount of time.
- We use special Control packets.
- Control packets are usually: small, "reliable", "infrequent" → good candidates for flooding.
- Nodes keep internal records of discovered routes.
- Discovered routes are subsequently used to send data packet(s) – without using flooding.
- Overhead of control packet flooding is amortized over data packets transmitted between consecutive control packet floods.

Unicast Routing

- Forward packets from a single source to a single destination – the "source-destination pairs".
- Unicast routing is a network protocol that "guides" packets through "discovered" paths.
- Two main functions:
  - Select route for various source-destination pair.
  - Delivery of messages to their destination.
- Routing is a complex problem:
  - Requires the coordination of nodes.
  - Must cope with failures: wireless channel and node failures.
  - Avoid network congestions.
  - Identify potential security breaches.

Main issues in Routing

- Routing involves a collection of algorithms:
  - Work more or less independently.
  - Support each other.
- Selection of routes affects network performance. Main performance measures:
  - Throughput: quantity of service.
  - Average packet delay: quality of service.
- Performance measures for Wireless Sensor Networks:
  - Energy Efficiency
  - Reliability

Many Routing Protocols exist

- Centralized vs Distributed routing decisions:
  - Routing decisions are taken at source node or at each intermediate repeater node.
- Stateless vs Stateful routing decisions:
  - Routing decisions may be made for each individual packet or use "virtual circuits" with fixed routing decisions.
- Static vs Adaptive routing decisions:
  - Routing decisions are affected by traffic conditions.
- Pro-active vs Reactive routing decisions:
  - Routing decisions for predetermined set of source-destination pairs or "setup" of routes only if needed (on demand).
- Hybrid Protocols.
- Hierarchical Protocols.

Dynamic Source Routing (DSR)

- Reactive Protocol:
  - 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.
- Stateful routing decisions:
  - Discovered route used for all packet exchanges for a given source-destination pair.
- Adaptive routing decisions:
  - Routing discovery re-initiated when routing paths are broken.
- Each Node maintains a Routing Table, each row contains:
  - Destination node address.
  - Ordered list of nodes that make up path.

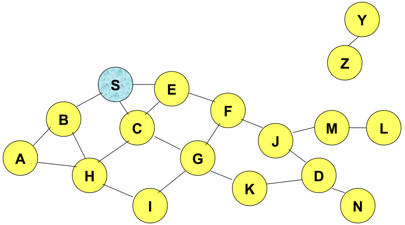
DSR: Routing Table

- Each Node maintains a dictionary:
  - KEY: Destination node address.
  - VALUE: Ordered list of nodes that make up route.

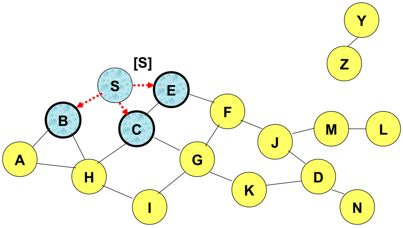
DSR: Route Discovery

- Source node S wants to send a packet to node D.
- If dictionary (routing table) does contain an entry for D, node S initiates a route discovery.
- S floods control message Route Request (RREQ) that contains:
  - Source node address.
  - Destination node address.
  - List of nodes that make up route, initially set to S.
- Each node appends own identifier when forwarding RREQ
- When D receives the first RREQ, sends a Route Reply (RREP)
- RREP is sent on a route obtained by reversing the route appended to received RREQ
- RREP includes the route from S to D on which RREQ was received by node D

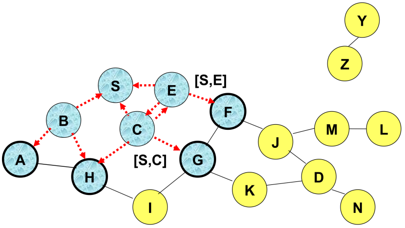
DSR: Route Discovery Example



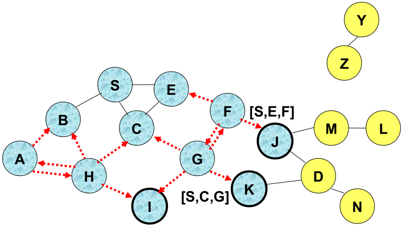
DSR: Route Discovery Example



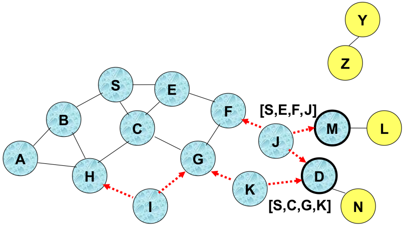
DSR: Route Discovery Example



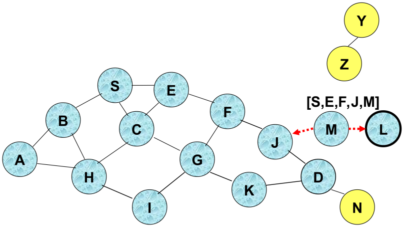
DSR: Route Discovery Example



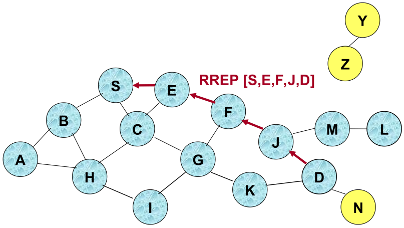
DSR: Route Discovery Example



DSR: Route Discovery Example



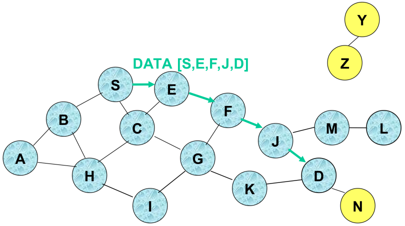
DSR: Route Discovery Example



DSR: Data Delivery

- Node S on receiving RREP, adds the route included in the RREP in Dictionary (routing table).
- When node S sends a data packet to D, the entire route is included in the packet header.
  - Hence the name source routing.
- Intermediate nodes use the source route included in a packet to determine to whom a packet should be forwarded.
- Data packet format:
  - Packet Header:
    - Source node address.
    - Destination node address.
    - List of node address that make up route.
  - Payload (data).

DSR: Data Delivery Example



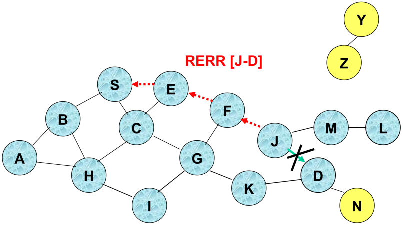
Route Reply in Asymmetric Networks

- Route Reply can be sent by reversing the route in Route Request (RREQ) only if links are guaranteed to be bi-directional.
- 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.

DSR: Adapting Route

- While transmitting a packet from an intermediate node X to the next intermediate node Y, an error might occur.
- After retrying a fixed amount of times, node X determines that Y is no longer available.
- Node X sends a route error (RERR) message to S following the reverse route found in the data packet.
- Node S upon receiving RERR remove from the dictionary (routing tables) the entry for D.

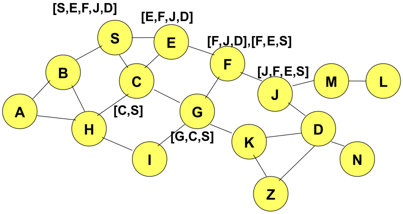
DSR: Routing Error Example



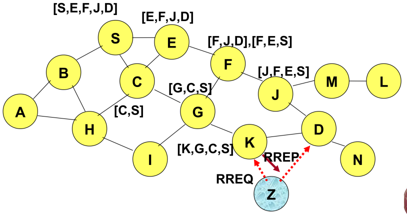
DSR: Route Caching

- Optimization to speed up route discovery.
- Take advantage of any route discovery happening within the network neighborhood.
- Potentially reduce propagation of route requests.
- Each node caches a new route it learns by any means:
  - Upon receiving a RREQ: learn a path to S.
  - Upon receiving a RREP: learn a path to D.
  - Upon overhearing a RREQ/RREP/DATA packet: learn a path to S, D.

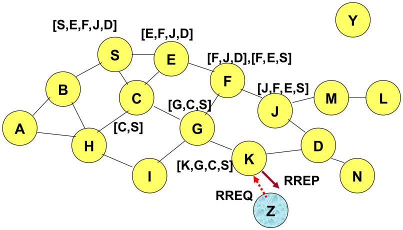
DSR: Routing Cache Example



DSR: Routing Cache Example



DSR: Routing Cache Example



DSR: Advantages

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

DSR: Disadvantages

- Packet header grows with route length due to source routing
  - Particularly when data are small.
- Flood of RREQ may potentially reach all nodes in the network.
- Must avoid collisions while propagating RREQ
  - Exposed terminal problem.
  - Insertion of random delays before forwarding RREQ.
- Increased contention if too many route replies come back due to nodes replying using their local cache
  - Route Reply susceptible to Exposed terminal problem.
  - May be fixed if a node does not reply if it hears another RREP with a shorter route.
- An intermediate node may send Route Reply using a stale cached route, thus polluting other caches.

Ad Hoc On-Demand Distance Vector Routing (AODV)

- Decentralized Protocol: AODV attempts to improve performance of DSR by following a next-hop routing technique.
- Each Node maintains a Routing Table, each row contains:
  - Destination node address.
  - Next-hop node address.
  - Destination sequence number.
  - Life time.
- Sequence numbers are used to determine the fressness of the entry.

AODV: Route Request

- When a route to a new destination is needed, the node uses a broadcast RREQ to find a route to the destination.
- When a node re-broadcasts a RREQ, it sets up a reverse path pointing towards the source
- A route can be determined when the RREQ reaches either the destination itself, or an intermediate node with a "fresh enough" route to the destination.
- The Destination Sequence Number filed in the RREQ message is the last known destination sequence number for this destination.

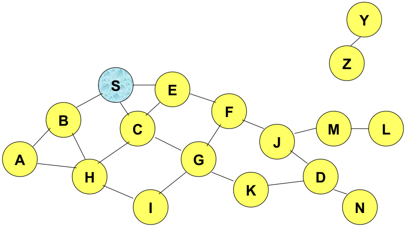
AODV: Route Reply

- From destination or intermediate node with a fresh route.
- The route is made available by unicasting a RREP back to the source of the RREQ.
- Since each node receiving the request caches a route back to the source of the request, the RREP can be unicast back from the destination to the source.
- An intermediate node (not the destination) may also send a RREP provided that it knows a more recent path than the one previously known to sender S.
- To determine whether the path known to an intermediate node is more recent, destination sequence numbers are used.

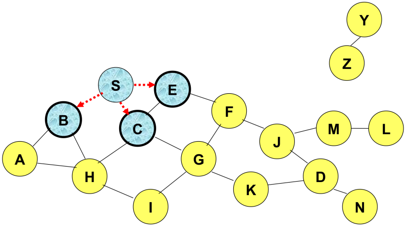
AODV: Route Error

- Nodes monitor the link status of next hops in active routes.
- When a link break in an active route is detected, a RERR message is used to notify other nodes that the loss of that link has occurred.
- The RERR message indicates which destinations are now unreachable due to the loss of the link.

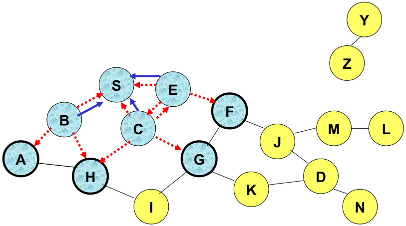
AODV: Route Discovery Example



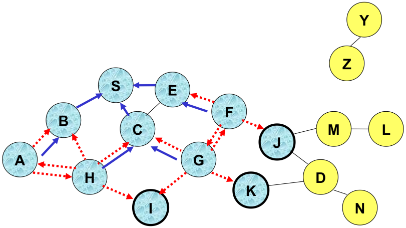
AODV: Route Discovery Example



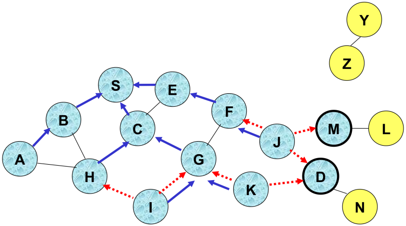
AODV: Route Discovery Example



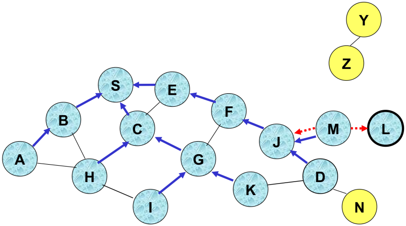
AODV: Route Discovery Example



AODV: Route Discovery Example



AODV: Route Discovery Example



Mesh Networking
Ad Hoc On-Demand Distance Vector Routing (AODV)

AODV: Route Discovery Example