Infrastructure-less Wireless Networks

- Standard Mobile IP needs an infrastructure
  - Home Agent/Foreign Agent in the fixed network
  - DNS, routing etc. are not designed for mobility
- Sometimes there is no infrastructure!
  - Remote areas, ad-hoc meetings, disaster areas
  - Cost and time may be arguments against infrastructure!
- Main issue: routing
  - No default router available
  - Every node should be able to forward
Solution: Wireless Ad-hoc Networks

- Network without infrastructure
  - Use components of participants for networking

- Examples
  - Single-hop: All partners max. one hop apart
    - Bluetooth piconet, PDAs in a room, gaming devices...
  - Multi-hop: Cover larger distances, circumvent obstacles
    - Bluetooth scatternet, police network, car-to-car networks...

- MANET: Mobile Ad-hoc Networks

MANET: Mobile Ad-hoc Networking

Focus: Routing in Ad-hoc Networks
Outline

- Routing in wired networks
  - Distance vector routing, link-state routing
- Limitations in wireless networks
- Ad-hoc routing protocols:
  - DSR, AODV, ...

Unicast Routing in Wired Networks

- Given:
  - Graph: where nodes are routers and edges are links
  - Cost: associated with each link
- Find:
  - Lowest-cost path between any two nodes
- Requirements:
  - Self-healing, traffic-sensitive, scalable
  - Dynamic and distributed algorithms

Two classes: “distance-vector” and “link-state”
Distance Vector Routing: Basics

Basics:
- Each node:
  - Constructs a vector of distances to all other nodes
    - “Distance vector”
  - Distributes to immediate neighbors
- Neighbors use the distributed information to update their own distance vectors
- This distributed exchange-update-exchange should lead to globally consistent distance vectors (and routing tables)

Distance Table Data Structure

- Each node has its own table with a...
  - Row for each possible destination
  - Column for each directly-attached adjacent node (neighbor)
- Each table entry gives cost to reach destination via that adjacent node
  - Distance = Cost

\[ D^X(Y,Z) = \text{distance from X to Y via Z as first hop} \]
\[ = c(X,Z) + \min_w \{ D^Y(Y,w) \} \]
\[ w = \{ \text{neighbors of Z} \} \]
The distance table gives the routing table.

- Just take the minimum cost per destination.

**Distance Vector Example**

\[
D^d(X,Y) = c(X,Y) + \min_w\{D^d(Y,w)\}
\]
\[
= 7 + 1 = 8
\]

\[
D^d(Y,Z) = c(Y,Z) + \min_w\{D^d(Z,w)\}
\]
\[
= 2 + 1 = 3
\]
Distance Vector Example

Time

Link Cost Changes

When a node detects a local link cost change:
The nodes updates its distance table
If the least cost path changes, the node notifies its neighbors

How long does convergence take?

"Good news travels fast"
Link Cost Changes

- Good news travels fast, but...
- “Bad news” travels slow
  - The “count to infinity” problem

Routing Loop!
Does it Terminate?

Link State Routing Approach

- Each node:
  - Floods the latest state (cost) of each attached link to all other nodes in the network
    - Ensures that flooding is reliable
  - Computes shortest-cost paths to every other node
    - Using Dijkstra’s algorithm

- Can suffer from route oscillations if cost is a function of load
CAN THESE BE APPLIED TO WIRELESS AD-HOC NETWORKS?

Wireless Networks: What’s Different?

- Varying channel quality and dynamic conditions
  - Separation (and merging) of networks
  - Asymmetric links
  - Shortest hop may be worst choice
  - Redundant links – routes need to converge quickly

![Diagram showing network topology with varying links at two different times, t₁ and t₂.]
Wireless Networks: What’s Different?

- Varying channel quality and dynamic conditions
  - Separation (and merging) of networks
  - Asymmetric links
  - Shortest hop often worst choice
  - Routes need to converge quickly

- Scarce transmission capacity
  - Overhead conspicuous; No frequent periodic updates

- Low compute power
  - No extensive route computations

- Low energy
  - Low control message overhead
  - Low control message frequency (to realize sleep mode)

- And if that’s not bad enough, add node mobility…

Routing in Wireless Mobile Networks

- Imagine hundreds of hosts moving
  - Routing algorithm needs to cope with varying wireless channel and node mobility
  - Routes may break, and reconnect later
Metrics for Routing?

- **Minimal:**
  - Number of nodes
  - Loss rate
  - Delay
  - Congestion
  - Interference
  - Overhead
  - …

- **Maximal:**
  - Stability of the logical network
  - Battery run-time
  - Time of connectivity
  - …

HOW TO DO ROUTING IN AD-HOC NETWORKS?
Routing Protocols

- **Proactive protocols**
  - Determine routes independent of traffic pattern
  - e.g., traditional link-state and distance-vector routing

- **Reactive protocols**
  - Maintain routes only if needed

- **Hybrid protocols**
  - Maintain routes to nearby nodes
  - Discover routes for far away nodes

Trade-Off

- **Latency of route discovery**
  - Proactive protocols may have lower latency
  - Reactive protocols higher because a route discovery from X to Y will be initiated only when X attempts to send to Y

- **Overhead of route discovery/maintenance**
  - Reactive protocols may have lower overhead since routes are determined only if needed
  - Proactive protocols do continuous route updating / maintenance

- **Which approach achieves a better trade-off depends on the traffic and mobility patterns**
THE CONCEPT OF FLOODING

How well does it work in a wireless network?

Data Delivery Using Flooding

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

What can go wrong?
Flooding Example

Broadcast transmission

- Represents a node that receives packet P for the first time
- Represents transmission of packet P

Flooding Example

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

- 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 Example**

- 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.

$\Rightarrow$ Packet P may not be delivered to node D at all, despite the use of flooding.
Flooding Example

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

Flooding Example

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

- 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

- **Advantages:**
  - Simplicity
  - May be more efficient if infrequent communication
    - Route setup / maintenance not worth it
    - Especially, when changing topology / mobility
  - Potentially higher robustness to path failure
    - Because of multi-path redundancy

- **Disadvantages:**
  - Potentially, very high overhead
    - Packets delivered to too many nodes who don't need them
  - Potentially lower reliability of data delivery
    - Reliable broadcast is difficult
    - Hidden terminal because no channel reservation

Flooding as a Building Block

- Many protocols perform (potentially limited) flooding of control packets, instead of data packets
  - The control packets are used to discover routes
  - Discovered routes are subsequently used to send data packet(s)

- Overhead of control packet flooding is amortized over data packets transmitted between consecutive control packet floods