Announcements

- Proposal for project 2 due today.

Today

- Finish MACs.
- PAMAS.
- Mobile IP.
- Unicast routing.

DVCS [Observations]
DNAV

- Directional network allocation vector.
- NAV: omnidirectional version.
- When node receives frame different than ACK, defers until end of transmission.
- With directional antennas, DNAV: reserves channel for others in specific range of directions.

DNAV Example

Example:

- If omni-directional transmission: all communication must be done serially.
- If all nodes have directional antennas but use NAV: A→B and C→D (A-B's RTS/CTS not heard by C-D, and vice-versa); but E cannot talk to F.
- With DNAV, E sets DNAVs for A, B, C, and D; so it can talk to F.

PAMAS

- Goal: energy efficiency.
- Approach:
  - Contention-based (based on MACA).
  - Low power radio mode when node is idle.
  - Separate signaling channel for RTS-CTS.
Energy model

- Idle mode consumes orders of magnitude less power than transmission or receiver modes.
- Overhearing!

PAMAS Protocol

Observations

- RTS-CTS exchange on separate signaling channel.
  - Does not affect data exchange.
- Busy tone also on signaling channel.
  - Sent by data receiver when receiving data.
  - Protects receiver from transmissions by neighbors.
  - Collides with RTS-CTS exchange from interfering nodes.
  - Is sent any time during data reception.

Overhearing

- Power off radio to avoid overhearing.
- Nodes power off if:
  - No packets to transmit, and neighbor begins transmitting.
  - Packet to send, but at least one neighbor is receiving (neighbor sends busy tone).
Powering off

- Transmission to a sleeping node?
- Node powers off if it overhears transmission.
- For how long?
- Use probes to determine duration of idle mode.

Duration of Idle Period

- If node has empty queue, powers off for duration of transmission.
  - When node comes up, if its queue still empty and channel busy, uses probes to do binary search to determine time last transmission will end.
  - If node has non-empty queue, transmits RTS (separate channel) when comes up.
    - If busy tone received, it contains duration of transmission.
    - If no response (e.g., if busy tone collides), binary search.

Duration of Idle Period (cont’d)

- If probes get corrupted: node stays on.

Performance Trade-off

- Power savings versus delay/throughput.
  - If node is off because it cannot transmit or receive, delay not impacted.
  - But, length of off-time should be no longer than needed.
  - PAMAS favor delay/throughput over energy efficiency.
Mobile IP

Where is mobility managed?

- Application
- Session
- Transport
- Network
- Data-link
- Physical
- Mobile-IP: extension to IP architecture.
  - Manages mobility at the IP layer.
  - Hides mobility from upper layers.

Mobile IP: Goals

- Nodes can receive datagrams no matter where they attach to the Internet.
- IMHP (Internet Mobile Host Protocol) as Mobile IP precursor.
- Problem with IP:
  - IP address uniquely identifies host’s PoA.
  - Host must attach to network specified by its IP address to send/receive datagrams.

Mobile IP

- Internet standard for "last-hop" mobility support in IP networks (RFC 2290).
- How do we deliver IP packets when the endpoints move?
  - Mobile host must be able to communicate after changing its link-layer point-of-attachment to the Internet.
  - Mobile host must be able to communicate using its permanent (home) IP address.
Mobile IP: Design Issues

- Issues:
  - Impact on IP addressing.
  - Impact on routing.

- Key design considerations:
  - Scale.
  - Routing updates (size and frequency).
  - Simplicity.
  - Incremental deployment.

Terminology

- Home Agent (HA): router on MN's HN that tunnels datagrams to MH when away and keeps MH's current location info.
- Foreign Agent (FA): router on foreign network; delivers datagrams to MH while on FN.
- Home Address (HoA) and Care-of Address (CoA):
  - HoA: MH's permanent address on HN.
  - CoA: MH's temporary address on FN.
Mobile-IP: Basic Operation

- MH normally uses its home address HoA.
- When MH visits a foreign network,
  - Registration with FA.
  - Discover mobile agent and CoA.
  - Registration with HA.
  - Binding update (HoA -> CoA).
- Communicating with MN: use HoA.
- HA forwards packet from HoA to CoA.

Discovering Agents

Agents periodically beacon advertisements

Agent Discovery

- Agent advertisement (beaconing):
  - Mobile agent broadcast agent advertisement at regular intervals (“I am here”).
- Agent solicitation:
  - MH can poll (“anyone here?”).
  - Mobile agent responds to poll.

Discovering Agents

MH polls; agent responds.
Agent Advertisement
- Allow for the detection of mobility agents.
- Follows ICMP router advertisement message.
- Let the MH know whether the agent is a HA, or a FA.
- List one or more available care-of addresses.
- Inform the MN about special features provided by FA.
  - Example: Alternative encapsulation techniques, header compression.

Registration
- When away, MH registers its CoA with HA (binding update).
- Binding: (HoA->CoA)
  - Binding has a lifetime.
- Registration process
  - MH sends a registration request with CoA.
  - HA authenticates request.
  - HA approves or disapproves the request.
  - HA adds necessary information to its routing table.
  - HA sends registration reply back to MH.

CoA
- Two types of CoA:
  - FA's IP address.
  - MH's temporary address
    - Locally-assigned address in the foreign network
    - E.g., DHCP address
- Advantages/disadvantages?
Tunneling

- HA tunnels datagrams destined to MH when MH is away.
- Datagrams sent to MH, intercepted by HA and tunneled to its CoA.
- Tunnel terminates at MH CoA (either the MH or the FA).

Encapsulation

- Tunneling requires encapsulation.
  - Sending the original packet (CH->MH) in another packet (HA->CoA).
- Default encapsulation mechanism:
  - IP-within-IP (tunnel).
  - Tunnel header: new IP header inserted by the tunnel source (home agent).
  - Destination IP: CoA

Tunneling in Mobile IP
The Triangle Routing Problem
- Aka, "dogleg" routing.
- MH->CH: direct.
- CH->MH: CH->HA->MH
- Inefficient
- Solution: route optimization.
- Deliver binding updates directly to CH.

Route Optimization
- Binding caches:
  - Nodes can keep caches with CoA for MHs.
  - If node has entry for MH, sends data directly.
  - Otherwise, "triangulates" with HA.
  - Binding cache entries have TTL.
  - HA, FA, or MH can send binding cache updates to CH.

"Smooth" Handoffs
- MH moving among FN.
- New CoA registered with HA.
- Previous FA not necessarily notified.
  - Old registration will expire.
- New data delivered to new CoA.
- In-flight data?
  - Dropped and retransmitted by upper layers, or
  - FA notified of new CoA; FA forwards data to new CoA.

Authentication
- Malicious nodes can infiltrate FNs.
- Mobile IP registration includes authentication info exchange.
  - MH-HA.
  - MH-FA.
  - HA-FA.
- Protection against replay attacks.
  - Timestamp and nonces.
Mobility Support in IPv6
- FA’s functionality performed by MH.
- Node support for address auto-configuration.
- MH can obtain CoA for current PoA.
- MH informs CH of its new CoA.
  - IPv6’s destination options.
  - Piggybacked in data packet from MH to CH.

IPv6 Mobility Support (Cont’d)
- HA functionality practically unchanged.
  - Keeps MH CoA information.
  - Tunneling using IPv6 encapsulation.
    - MH then sends IPv6 encapsulation.
    - Acknowledgement of CoA information reception.

IPv6 Mobility Support (Cont’d)
- IPv6 destination options used to deliver mobility-related information.
  - Binding update option: MH->CH and ->HA.
    - Bindings need updating or refreshing.
  - Binding ACK option: HA->MH.
  - Binding request option: CH->MH.
    - CH may solicit binding update from MH.

Handoffs
- Overlapping cells:
  - MH should still accept packets at previous CoA even after reporting new CoA.
  - Why?
- Router-assisted handoffs:
  - No overlap.
  - MH sends binding update to router for previous CoA.
  - Routers as HA for node’s previous CoA.
TCP Performance in Mobile-IP (Choong)

- Source of overhead: triangle routing.
  - Additional processing at HA and FA.
  - Additional delay due to "triangulation".
  - Additional delay due to fragmentation (extra IP header).
  - Handoffs.

Goal

- Determine the impact on TCP performance of
  - Combined overhead sources.
  - Individual overhead sources.

Methodology

- Several scenarios that compound or isolate overhead sources.
- Compare performance of between scenario pairs.
- FTP transfer between MH and CH.
- Metric: TCP throughput.

Summary of Results

- Dogleg routing as main cause of TCP throughput degradation.
  - Solution: route optimization.
- Handoff is second.
  - Mobile-IP's inherent delay in re-establish connectivity with new FA.
  - Solutions:
    - Increase frequency of router advertisements.
    - Use link-layer information to trigger handoff.
Unicast Routing in MANETs

MANETs
- No fixed infrastructure!
- Multiple hops to reach destinations.
  - Route changes because of node movements.
- Radio used for communication.
  - Variable transmission.
  - Broadcast nature of radio.
  - Interference, fading, etc.

Mobility
- Many variations in mobility patterns:
  - Almost fixed (sensors, actuators).
  - Highly mobile (vehicles).
  - Discrete movements.
  - Continuous movements.
- Mobility Characteristics
  - Speed.
  - Direction.

Ad-Hoc Routing Requirements
- Distribution paths
  - Multi hop paths.
  - Loop free.
  - Minimal transmission data overhead.
- Self starting and adaptive to dynamic topology.
- Low consumption of memory, bandwidth, power.
  - Scalable with number of nodes.
  - Localized effects of link failure.
Many protocols have been proposed. Some have been invented specifically for MANET. Others adapted from protocols for wired networks. No single protocol works well in all MANET environments! Adaptive protocols?

Problems using DV or LS

- **DV protocols:**
  - May form loops: wasteful in wireless environment
  - Bandwidth and power.
  - Loop avoidance may be complex
- **LS protocols:**
  - Higher storage and communication overhead.

Unicast routing classification

- **Proactive protocols:**
  - Determine routes independent of traffic pattern.
  - Traditional link-state and distance-vector routing protocols are proactive.
- **Reactive protocols:**
  - Maintain routes only if needed.
  - Hybrid protocols.
Trade-Offs

- 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.

Trade-offs (Cont’d)

- Overhead of route discovery/maintenance.
  - Reactive protocols may have lower overhead since routes are determined only if needed.
  - Proactive protocols typically result in higher overhead due to continuous route updating.

- Which approach achieves a better trade-off depends on the traffic and mobility patterns.

Flooding for Data Delivery

- 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; why?
- P reaches D if it is reachable from S.
- Node D does not forward P.

Flooding for Data Delivery

Represents nodes that are within each other's transmission range.
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.

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

Flooding of Data: Advantages
- Simplicity.
- May be more efficient when rate of information transmission is low compared to topology changes.
  - This scenario may occur, for instance, when nodes transmit small data packets relatively infrequently, and many topology changes occur between consecutive packet transmissions.
- Potentially higher reliability of data delivery
  - Because packets may be delivered to the destination on multiple paths.
Flooding: Disadvantages

- Potentially, very high overhead.
- Data packets may be delivered to too many nodes who do not need to receive them.
- 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, D would not receive the packet at all.

Flooding of Control Packets

- Many protocols perform (potentially limited) flooding of control packets.
- Control packets are used for route discovery/maintenance.
- 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.