Mobile Ad Hoc Networks
What is a MANET (Mobile Ad Hoc Networks)?

- Formed by wireless hosts which may be mobile
- No pre-existing infrastructure
- Routes between nodes may potentially contain multiple hops
  - Nodes act as routers to forward packets for each other
  - Node mobility may cause the routes to change
Why MANET?

• Advantages: low-cost, flexibility
  – Ease & Speed of deployment
  – Decreased dependence on infrastructure

• Applications
  – Military environments
    • soldiers, tanks, planes
  – Civilian environments
    • vehicle networks
    • conferences / stadiums
    • outside activities
  – Emergency operations
    • search-and-rescue / policing and fire fighting
Challenges

• Collaboration
  – Collaborations are necessary to maintain a MANET and its functionality.
  – How to collaborate effectively and efficiently?
  – How to motivate/enforce nodes to collaborate?

• Dynamic topology
  – Nodes mobility
  – Interference in wireless communications
Routing Protocols: Overview

- **Proactive protocols**
  - Determine routes independent of traffic pattern
  - Traditional link-state and distance-vector routing protocols are proactive
  - Examples:
    - DSDV (Dynamic sequenced distance-vector)
    - OLSR (Optimized Link State Routing)

- **Reactive protocols**
  - Maintain routes only if needed
  - Examples:
    - DSR (Dynamic source routing)
    - AODV (on-demand distance vector)

- **Hybrid protocols**
  - Example: Zone Routing Protocol (intra-zone: proactive; inter-zone: on-demand)
Routing Protocols: Tradeoff

- 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 may be found 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 can (but not necessarily) result in higher overhead due to continuous route updating

- Which approach achieves a better trade-off depends on the traffic and mobility patterns
Dynamic Source Routing


- When node S wants to send a packet to node D, but does not know a route to D, node S initiates a routing process.

- Runs in three phases
  - Route Discovery → Route Reply → Path Establishment

- Route Discovery
  - Source node S floods *Route Request (RREQ)*
  - 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

[S]

Represents transmission of RREQ

[X,Y] Represents list of identifiers appended to RREQ
Route Discovery in DSR
Route Discovery in DSR
Route Reply in DSR

• Destination D on receiving 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
Route Reply in DSR

Represents RREP control message
Route Reply in DSR

- Node S on receiving RREP, caches the route included in the RREP

- 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 Delivery in DSR

Packet header size grows with route length
Some Other Routing Protocols

- Location information aided protocols
- Power-aware protocols
- Others …
  - e.g., considering the stability of topology
Location-Aided Routing (LAR)


• Exploits location information to limit scope of route request flood
  ▪ Location information may be obtained using GPS

• *Expected Zone* is determined as a region that is expected to hold the current location of the destination
  ▪ Expected region determined based on potentially old location information, and knowledge of the destination’s speed

• Route requests limited to a *Request Zone* that contains the Expected Zone and location of the sender node

Power-Aware Routing

- Modification to DSR to make it power aware (for simplicity, assume no route caching):
  - Route Requests aggregate the weights of all traversed links
  - Destination responds with a Route Reply to a Route Request if
    - it is the first RREQ with a given ("current") sequence number, or
    - its weight is smaller than all other RREQs received with the current sequence number
Geography Adaptive Fidelity

- Each node associates itself with a square in a *virtual grid*
- Node in each grid square coordinate to determine who will sleep and how long

Research in Other Layers

• Transport layer

• Application layer
  ▪ Data management
  ▪ Distributed algorithms
    • clock synchronization
    • mutual exclusion
    • leader election
    • Byzantine agreement
MAC Layer Misbehavior

- Nodes are required to follow Medium Access Control (MAC) rules
- Misbehaving nodes may violate MAC rules
Some Possible Misbehavior

• Causing collisions with other hosts’ RTS or CTS
• “Impatient transmitter”
  ▪ Smaller backoff intervals
  ▪ Shorter Inter-frame Spacings
Solutions

• Diagnose node misbehavior
  ▪ Catch misbehaving nodes

• Discourage misbehavior
  ▪ Punish misbehaving nodes

• Details will be discussed later in this course
Network Layer Misbehavior: Drop/Corrupt/Misroute

• A node “agrees” to join a route (for instance, by forwarding route request in DSR) but fails to forward packets correctly

• A node may do so to conserve energy, or to launch a denial-of-service attack, due to failure of some sort, or because of overload

• Solutions
  • Opt I: Detect the attacks → tolerate them
  • Opt II: Avoid some attacks
Watchdog Approach

- Verify whether a node has forwarded a packet or not

B sends packet to C
Watchdog Approach

- Verify whether a node has forwarded a packet or not
- B can learn whether C has forwarded packet or not
- B can also know whether packet is tampered with if no per-link encryption

C forwards packet to D

B overhears C
Forwarding the packet
Watchdog + Pathrater

- “Pathrater” is run by each node. Each node assigns a rating to each known node
  - Previously unknown nodes assigned “neutral” rating of 0.5
  - Rating assigned to nodes suspected of misbehaving are set to large negative value
  - Other nodes have positive ratings (between 0 and 0.8)

- Ratings of well-behaved nodes increase over time up to a maximum
  - So a temporary misbehavior can be overcome by sustained good behavior

- Routes with larger cumulative node ratings preferred