18-452/18-750 Wireless Networks and Applications

Lecture 12: Mesh and Ad Hoc Networks

Peter Steenkiste

Spring Semester 2017

http://www.cs.cmu.edu/~prs/wirelessS17/

Overview

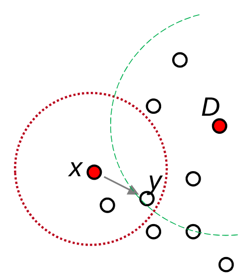
- Ad hoc networking concept
- Proactive versus reactive routing
- Proactive, table based routing: DSDV
- Reactive routing DSR
- Geographic routing: GPSR
- Other routing solutions
- Vehicular networks
- Wireless link metrics

Greedy Perimeter Stateless Routing (GPSR)

- Use *positions* of neighboring nodes and packet destination to forward packets
  - No connectivity or global topology is assumed – no forwarding or path information anywhere!
  - Nodes are assumed to know their location
  - Need some address-to-location look up
- Two forwarding techniques is used
  - ***Greedy forwarding***, if possible
  - ***Perimeter forwarding***, otherwise

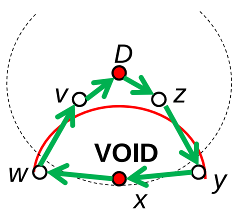
GPSR – Greedy forwarding

- A sender/forwarder x chooses to forward to a neighbor y such that $\{d_{xy} + d_{yD}\}$ is minimum



GPSR – Perimeter forwarding

- What happens if a node does not have a neighbor that is closer to the destination
- Right Hand Rule: you forward the packet to your first neighbor clockwise around yourself
  - traverse an interior region in *clockwise* edge order



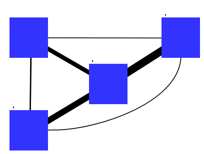
These sequence of edges traversed is termed as *PERIMETER*

Overview

- Ad hoc networking concept
- Proactive versus reactive routing
- Proactive, table based routing: DSDV
- Reactive routing DSR
- Geographic routing: GPSR
- Other routing solutions
- Wireless link metrics
- Vehicular networks

Link Metric

- Routing protocols for wired networks tend to use very simple link metrics
  - » Hop count (all links have cost of 1) or simple integers
  - » Performance of wired links is predictable!
- Wireless links can be very different and their performance can be unpredictable
  - » Hop count is a bad idea – why?
- Some links are so bad they are not really links
- Solution: Require a minimum PDR to qualify as a link
  - » PDR = Packet Delivery Rate
- Is that a sufficient solution?



Factors Influencing "Link Quality"

- Signal strength and quality: affects the bit rate used for packets
  - » Bit rate affects the transmit time of packets
- Number of retransmissions needed to deliver packets
  - » Retransmissions delay packets and use up more bandwidth
- Interference from nearby nodes
  - » Interference limits the transmission opportunities a node has, i.e., it can take longer to get channel access
  - » Some links may also face more hidden and exposed terminal problems

ETX: Minimize Number of Transmissions

- Measure each link's packet delivery probability with broadcast probes
  - » Must also measure the reverse link – ACKs must be received too for a transmission to be successful!

  P(delivery) = $1 / (d_f * d_r)$
- The link ETX is the average number of transmissions needed to deliver a packet

  Link ETX = 1 / P(delivery) = $d_f * d_r$
- Route ETX = sum of link ETX
  - » Pessimistic: not all links interfere with each other
- ETX only considers some factors: bit rate, short probes under-estimate loss rate, traffic load, hidden terminals, …

ETX: Sanity Checks

- ETX of perfect 1-hop path: 1
- ETX of 50% delivery 1-hop path: 2
- ETX of perfect 3-hop path: 3
- So, e.g., a 50% loss path is better than a perfect 3-hop path!
  - » A PDR threshold would probably fail here…

ETT: Expected Transmission Time

- The bit rate used for transmission can have a very big impact on performance
  - » E.g., 802.11a rates range from 6 to 54 Mbps
- ETT – expected *transmission time*

  ETT = ETX / Link rate

  = 1 / (P(delivery) * Bit Rate)
- Accounts for all major factors
  - » Traffic load and resulting competition for transmission time is still a factor
  - » Must update metric periodically

Overview

- Ad hoc networking concept
- Proactive versus reactive routing
- Proactive, table based routing: DSDV
- Reactive routing DSR
- Geographic routing: GPSR
- Other routing solutions
- Wireless link metrics
- Vehicular networks

Vehicular "Ad Hoc" Networks

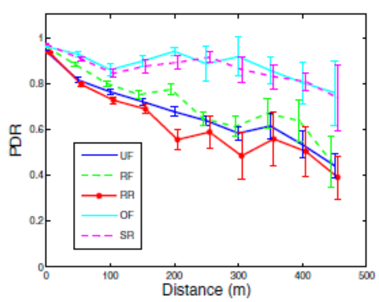
- Inter-vehicular communication
  - Emergency and military contexts
  - Everyday applications: Accident prevention, in-vehicle 'Internet', entertainment, …
- Very different from other 'ad-hoc' networks
  - Rapidly changing topology due to road and traffic conditions
  - Non-homogenous distribution of nodes
  - Constrained mobility and signal reception (obstacles?)
  - Diverse and rapidly changing physical environments
- How different from DTNs?

Background - IEEE 802.11p Standard

- IEEE 802.11p-based Dedicated Short Range Communication standard for vehicular environments
- OFDM modulation as the IEEE 802.11a/g
  - » Except carrier frequency bandwidth (5.9 GHz band)
  - » Channel bandwidth (change 20 MHz to 10 MHz)
- OFDM is an effective wireless communication scheme for non-mobile environments
  - » Both the symbols and their sub-channels are orthogonal
    - Zero ISI and zero ICI
  - » But both properties might be affected by Doppler spread/shift and fading environment

The PDR Gray-zone Phenomenon

- "Intermediate reception" with links that are bad but usable prevails
  - » True at all distances but gets worse as distance increases
  - » There is no region with a perfect reception rage
- Open Field and Suburban Roads works best
  - » Not surprising
- Rural Roads is harshest environment
  - » Remote houses, trees, cross traffic, ..



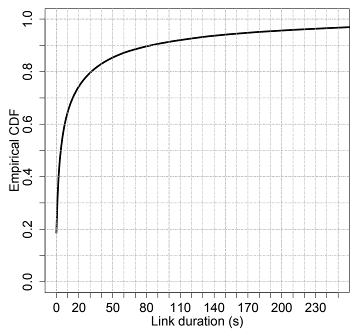
(a) PDR vs. Separation Distance

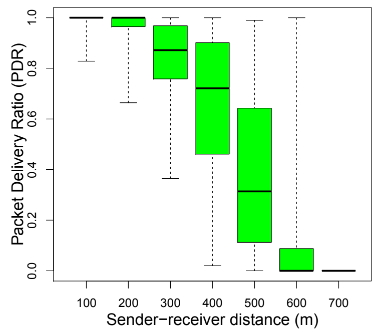
Experiment Settings

- Urban Freeway (UF)
  - » a large number of walls, tunnels and overhead bridges, as well as heavy vehicle traffic are present
- Rural Freeway (RF)
  - » The number of walls, tunnels and vehicle traffic are slightly less than its UF counterpart
- Rural Road (RR)
  - » The traffic was heavy on these routes because they lead toward a vehicle testing facility.
- Suburban Road (SR)
- controlled Open Field (OF)
  - » no buildings and other vehicles.

Dynamic Topology and Links

- Causes: high mobility, obstacles (multipath, shadowing)
- Effects: links have short life spans and partial connectivity

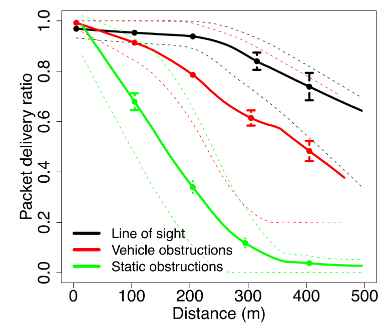




Peter A. Steenkiste

Spatial heterogeneity

- Transmission "range" is depends strongly on LOS conditions
- Line of sight blockages affect connectivity
  - » Terrain, buildings
  - » Other vehicles
- Node density varies according to location
- Pure geographic protocols assume connectivity uniformity



Peter A. Steenkiste

Idea

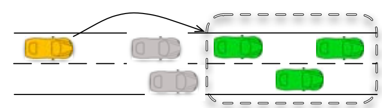
- Think of communication as connecting geographic areas instead of specific vehicles

1. Forwarding based on node diversity: Each area may have many antennas distributed across vehicles
2. Routing also uses spatial connectivity: topology graph is based on geographic areas instead of specific vehicles

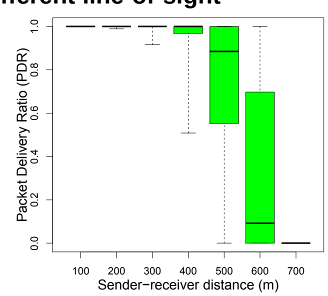
Peter A. Steenkiste

Exploiting Node Diversity

- Different vehicles experience different channels
  - » Multipath diversity due to physical separation
  - » Shadowing diversity due to different line-of-sight conditions



3 receivers

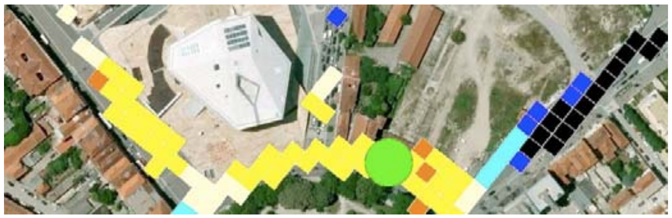


- DAZL – Density-Aware Zone-based forwarding

Peter A. Steenkiste

Spatial Connectivity Heuristic

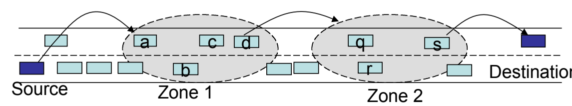
- Collect spatially-indexed connectivity data
- Create map of delivery probability between areas



- LASP – Look-Ahead Spatial Protocol

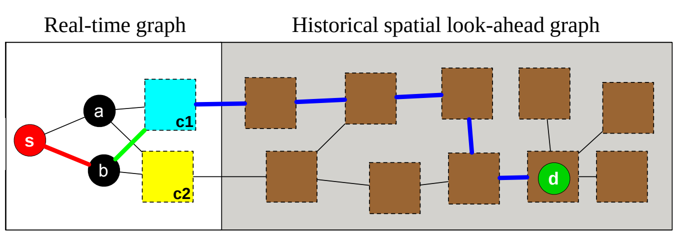
DAZL Forwarding

- Forwarding only
- Packets addressed to a geographic forwarding zone
  - » Reliability from node diversity
- Forwarder coordination and prioritization
  - » Minimizes congestion, maximizes distance traveled

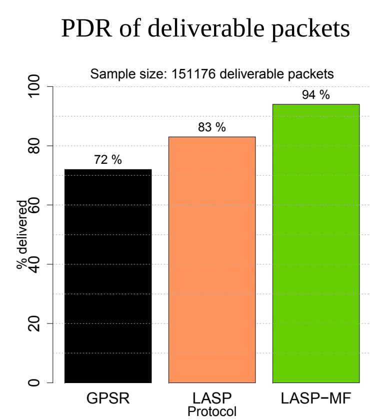


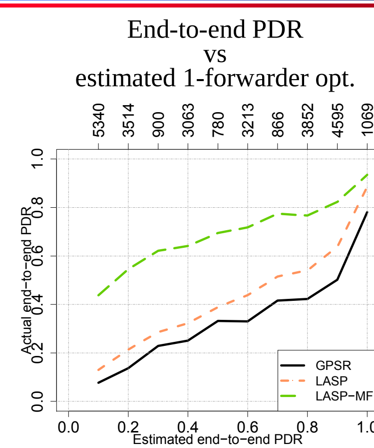
How about Routing? Use a Spatial Connectivity Graph

- Each node in the graph represents a geographic area
  - » Accounts for all vehicles in the area that can be used by zone-based forwarding algorithm
- Can use traditional routing protocols to find path
- Graph can use historical data or recent measurements



Experimental evaluation





Summary

- Ad hoc networks face many challenges
  - » Bad links, interference, mobility, …
  - » Makes routing very challenging
- Many proposals!
  - » Proactive routing: variants of "wired" routing protocols
  - » Reactive routing: only establish a path when it is needed
  - » Geographic routing: forwarding based on a node's location – no need for access to network topology
  - » Many variants and extensions
- Vehicular networks are especially challenging
  - » High speed mobility, very unstable links and topologies
  - » Active area of research

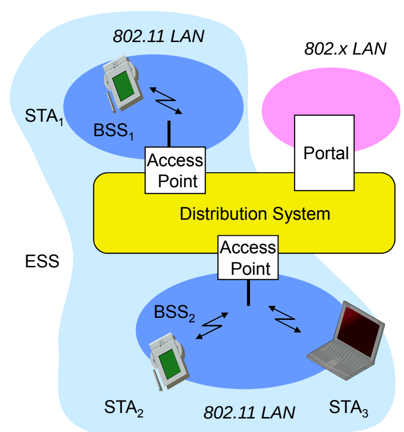
Outline

- Brief history
- 802 protocol overview
- Wireless LANs – 802.11 – overview
- 802.11 MAC, frame format, operations
- 802.11 management
- 802.11 security
- 802.11 power control
- 802.11*
- 802.11 QoS

Management and Control Services

- Association management
- Handoff
- Security: authentication and privacy
- Power management
- QoS

802.11: Infrastructure Reminder



- Station (STA)
  - » terminal with access mechanisms to the wireless medium and radio contact to the access point
- Access Point
  - » station integrated into the wireless LAN and the distribution system
- Basic Service Set (BSS)
  - » group of stations using the same AP
- Portal
  - » bridge to other (wired) networks
- Distribution System
  - » interconnection network to form one logical network (ESS: Extended Service Set) based on several BSS

Service Set Identifier - SSID

- Mechanism used to segment wireless networks
  - » Multiple independent wireless networks can coexist in the same location
  - » Effectively the name of the wireless network
- Each AP is programmed with a SSID that corresponds to its network
- Client computer presents correct SSID to access AP
- Security Compromises
  - » AP can be configured to "broadcast" its SSID
  - » Broadcasting can be disabled to improve security
  - » SSID may be shared among users of the wireless segment

Association Management

- Stations must associate with an AP before they can use the wireless network
  - » AP must know about them so it can forward packets
  - » Often also must authenticate
- Association is initiated by the wireless host – involves multiple steps:
  1. Scanning: finding out what access points are available
  2. Selection: deciding what AP (or ESS) to use
  3. Association: protocol to "sign up" with AP – involves exchange of parameters
  4. Authentication: needed to gain access to secure APs – manyoptions possible
- Disassociation: station or AP can terminate association

Association Management: Scanning

- Stations can detect AP based by scanning
- Passive Scanning: station simply listens for Beacon and gets info of the BSS
  - » Beacons are sent roughly 10 times per second
  - » Power is saved
- Active Scanning: station transmits Probe Request; elicits Probe Response from AP
  - » Saves time + is more thorough
  - » Wait for 10-20 msec for response
- Scanning all available channels can become very time consuming!
  - » Especially with passive scanning
  - » Cannot transmit and receive frames during most of that time – not a big problem during initial association

Association Management: Selecting an AP and Joining

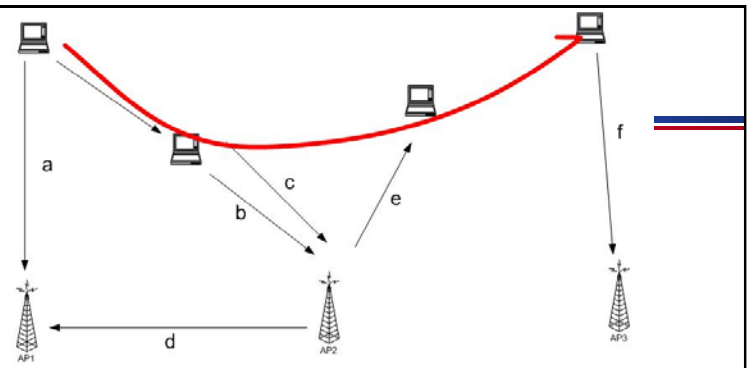
- Selecting a BSS or ESS typically must involve the user
  - » What networks do you trust? Are you willing to pay?
  - » Can be done automatically based on stated user preferences (e.g. the "automatic" list in Windows)
- The wireless host selects the AP it will use in an ESS based on vendor-specific algorithm
  - » Uses the information from the scan
  - » Typically simply joins the AP with the strongest signal
- Associating with an AP
  - » Synchronization in Timestamp Field and frequency
  - » Adopt PHY parameters
  - » Other parameters: BSSID, WEP, Beacon Period, etc.

Association Management: Roaming

- **Reassociation: association is transferred from active AP to a new target AP**
  - » Supports mobility in the same ESS – layer 2 roaming
- **Reassociation is initiated by wireless host based on vendor specific algorithms**
  - » Implemented using an Association Request Frame that is sent to the new AP
  - » New AP accepts or rejects the request using an Association Response Frame
- **Coordination between APs is defined in 802.11f**
  - » Allows forwarding of frames in multi-vendor networks
  - » Inter-AP authentication and discovery typically coordinated using a RADIUS server
  - » "Fast roaming" support (802.11r) also streamlines authentication and QoS, e.g. for VoIP

Association Management: Reassociation Algorithms

- **Failure driven: only try to reassociate after connection to current AP is lost**
  - » Typically efficient for stationary clients since it not common that the best AP changes during a session
  - » Mostly useful for nomadic clients
  - » Can be very disruptive for mobile devices
- **Proactive reassociation: periodically try to find an AP with a stronger signal**
  - » Tricky part: cannot communicate while scanning other channels
  - » Trick: user power save mode to "hold" messages
  - » Throughput during scanning is still affected though
    - – Mostly affects latency sensitive applications



(a) ---- The station finds AP1, it will authenticate and associate.

(b) ---- As the station moves, it may pre-authenticate with AP2.

(c) ---- When the association with AP1 is no longer desirable, it may reassociate with AP2.

(d) ---- AP2 notify AP1 of the new location of the station, terminates the previous association with AP1.

(e) ---- At some point, AP2 may be taken out of service. AP2 would disassociate the associated stations.

(f) ---- The station find another access point and authenticate and associate.