Wireless environments and architectures

CS 444N, Spring 2002

Instructor: Mary Baker

Computer Science Department

Stanford University

Diversity of wireless environments

- Differ in
  - Mobility
  - Type of application
  - Type of environment
  - Media characteristics
  - Pervasiveness of hosts
  - Level of infrastructure
  - Visibility of infrastructure
  - Coverage
  - Cost
- Examples
  - Cellular telephony
  - Satellite
  - Metropolitan-area data networks
  - Local-area networks
  - Personal-area networks
  - Ubiquitous computing environments
  - Infostations
  - Ad hoc networks

Ubiquitous computing

- Idea: environment outfitted with invisible helpful computing infrastructure and peripherals
- Both mobile and stationary hosts/displays
  - Components you carry with you
  - Components in infrastructure with which you interact
- Variety of applications – whatever you need
- Variety of media, both wired and wireless
- Lots of infrastructure – it's all around you
- Infrastructure is invisible
  - It helps us where we need help in the context in which we need help
  - We do not need to cater to it
- Coverage appropriate to the context
- Your personal information/applications go with you through the network

Ubiquitous computing, continued

- Often called pervasive/invisible computing
- Augmented reality
  - Ability to query your environment
  - Ability to ask for non-intrusive guidance
- May include variety of wearable devices
- Interesting privacy and sociological questions
- Can we really build security that is equivalent but no stronger than what we are accustomed to currently?
  - This definition varies greatly across cultures/governments

Ubiquitous computing, continued

- No clear definition of ubiquitous computing now
- What is it really good for?
- How practical is it really?
- Is it a superset of mobile computing?

Infostations

- Mobile hosts traveling through fixed network
- Good for periodic download or upload of bulky data
- Wireless islands (interconnected by wired network)
  - Gas stations
  - Here and there on the freeway
- Possibly an invisible infrastructure with mobile-aware applications
  - In reality, you may need to know to go to it
  - Original paper assumes this: information kiosks
- Coverage is spotty
- Cost is lower than complete coverage

Infostations, continued

- Example: incremental map download
  - Prefetching at infostations
  - Know path and speed of traveler
- In reality will need to combine this with another more pervasive wireless network
- One study [Ye, Mobicom'98] shows performance is better with many smaller-range infostations rather than fewer longer-range ones density of infostations
  - But this misses the whole point of infostations
- I envision traffic snarls

Ad hoc networks

- Collection of wireless mobile nodes dynamically forming a temporary network without the use of any existing network infrastructure or centralized administration.
- Hop-by-hop routing due to limited range of each node
- Nodes may enter and leave the network
- Usage scenarios:
  - Military
  - Disaster relief
  - Temporary groups of participants (conferences)

Ad hoc networks, continued

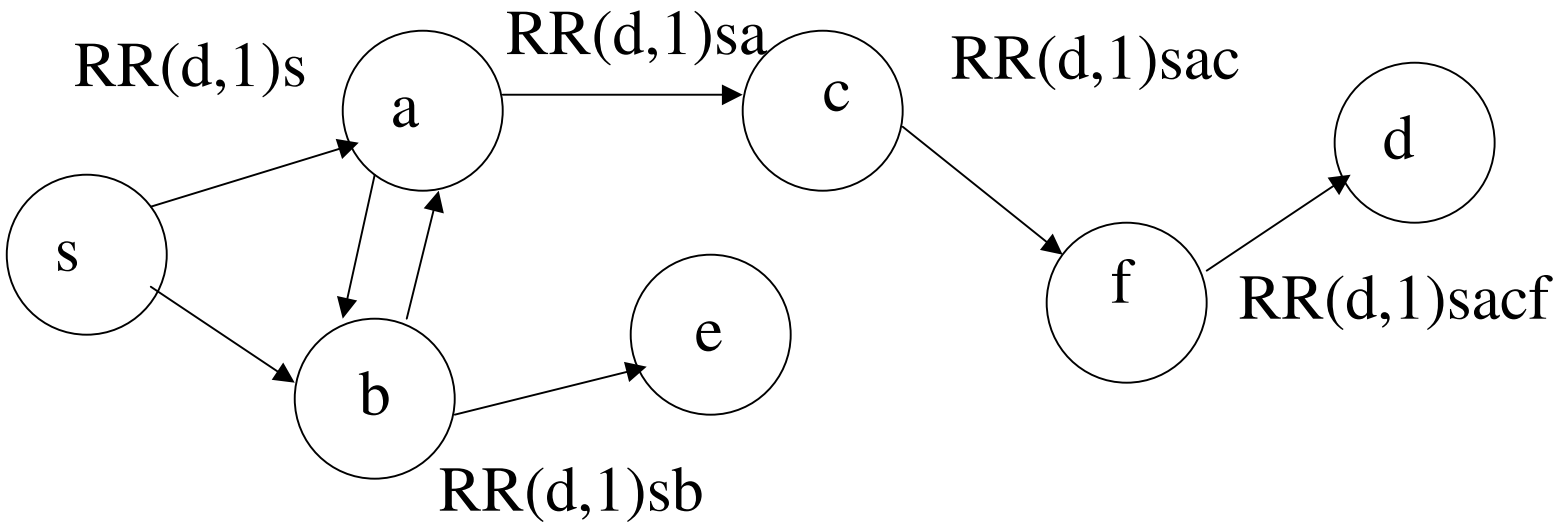
- Very mobile – whole network may travel
- Applications vary according to purpose of network
- No pre-existing infrastructure. Do-it-yourself infrastructure
- Coverage may be very uneven

Issues in ad hoc networks

- Routing performance
  - Routes change over time due to node mobility
  - Would like to avoid long delays when sending packets
  - But would like to avoid lots of route maintenance overhead
  - Want as many participating nodes as possible for greater aggregate throughput, shorter paths, and smaller chance of partition
- Security - interesting new vulnerabilities and complexities
  - Routing denial of service
    - Nodes may agree to route packets
    - Nodes may then fail to do so
    - Broken, malicious, selfish
  - Key distribution and trust issues

Example routing protocol: DSR

- Dynamic Source Routing (DSR) is one of most popular
- On-demand routing



Security issues in ad hoc networks

- Routing advertisements
  - Come shoot me here
  - Particularly awkward in algorithms that give location information in route ads
- A priori trust of nodes?
  - In some environments you know ahead of time the nodes you can trust
  - Route only through these nodes?
  - But maybe some other nodes would be helpful?
- Radio medium affects what you can do
  - Promiscuous mode and broadcast not available for all wave forms
  - Assumptions of bidirectional links

Encryption issues

- With advance planning can give all good nodes known keys
  - This still doesn't guarantee a node isn't compromised
- What to encrypt?
  - Payload – can do this end-to-end
  - Headers – requires link-to-link encryption and decryption - expensive
- Still important to identify misbehaving nodes

Mitigating routing misbehavior - theme

- It is impossible to build a perfect network
  - Use of legacy software
  - Unexpected events
  - Bugs
- Incorporate tools within the network to detect and report on misbehavior

Possible solutions

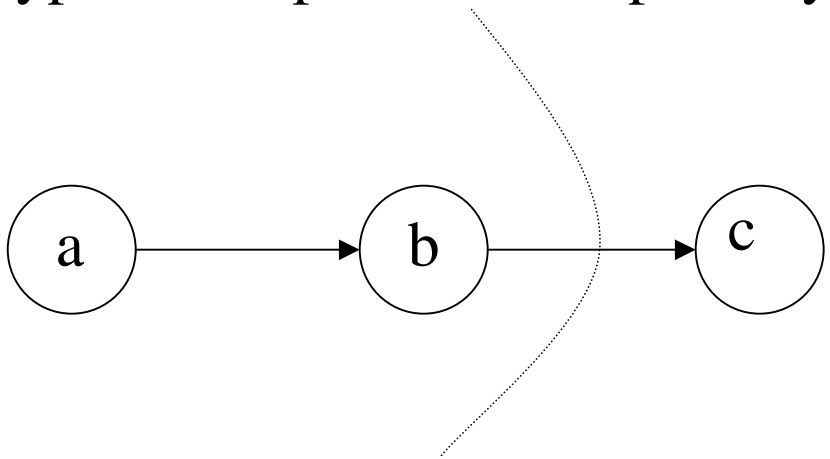
- Route only through trusted nodes
  - Requires a priori trust relationship
  - Requires key distribution
  - Trusted nodes may still be overloaded or broken or compromised
  - Untrusted nodes might perform well
- Detect and isolate misbehaving nodes
  - *Watchdog* detects the nodes
  - *Pathrater* avoids routing packets through these nodes

Assumptions

- On-demand routing protocol
  - Route discovered at time source sends packet to destination for which it has no cached route
  - Neighbors forward route request & append their addresses
- Bidirectional communication symmetry on every link
  - 802.1, MACAW and others assume this
- Wireless interface supports promiscuous mode
  - Only works with certain waveforms
  - WaveLAN and 802.11 networks support this

Watchdog technique

- Each node may host a watchdog
- Watchdog listens promiscuously to next node's transmissions
- Detects if next node does not forward packet
- Can sometimes detect tampering with payload
  - If encryption not performed separately for each link



Watchdog, continued

- Node keeps buffer of recently sent packets
- Removes packet from buffer if it overhears forwarding
- If packet in buffer for too long, increment failure tally for next node
- If failure tally exceeds threshold, notify source node of possible misbehavior
- Watchdog weaknesses
  - Ambiguous collisions
  - Receiver collisions
  - Limited transmission power
  - Misbehavior falsely reported
  - False positives
  - Collusion
  - Partial dropping

Pathrater

- Run by each node
- Combines watchdog info with link reliability data
- Each node maintains rating for each other node it knows
- Calculates path metric by averaging node ratings in the path
- New nodes assigned neutral rating
- Calculation can pick shortest-path in absence of node data
- Good behavior increments rating
- Link breaks decrement node rating a little
- Misbehavior decrements rating a lot
- Send extra route request when all known paths include misbehaving node

Results

- NS simulator & Dynamic Source Routing algorithm
- With and without watchdog/pathrater/extra route requests
- Throughput: percentage of sent data packets actually received by intended destinations
  - In absence of misbehaving nodes, all achieve 95% throughput
  - With misbehaving nodes, new techniques up to 30% better
- Overhead: Ratio of routing–related transmissions
  - Doubles from 12% to 24%
  - Due to extra route requests that don't help
  - Watchdog itself is very low overhead
- Effect of false positives on throughput
  - Doesn't seem to hurt – may even help!
  - Some nodes flaky due to location/collisions: avoid them anyway

Discussion

- What do you see as the next interesting things in mobile computing?
- What potential do you see for wireless networks?
- What do you see as the hardest things for us to address?
- If you could wish for one key piece of technology to come true (for mobility), what would it be?