EEC173B/ECS152C, Winter 2006

MANET Unicast Routing

- Proactive Protocols
  - OLSR
  - DSDV
- Hybrid Protocols

Acknowledgment: Selected slides from Prof. Nitin Vaidya

Proactive Protocols

- Most of the schemes discussed so far are reactive
- Proactive schemes based on distance-vector and link-state mechanisms have also been proposed

Link State Routing [Huitema95]

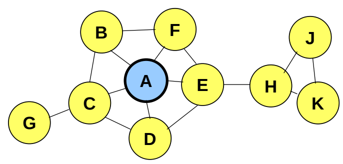
- Each node periodically floods status of its links
- Each node re-broadcasts link state information received from its neighbor
- Each node keeps track of link state information received from other nodes
- Each node uses above information to determine next hop to each destination
- Examples: IS-IS, OSPF

Optimized Link State Routing (OLSR)

- RFC 3626
  - http://hipercom.inria.fr/olsr/
- The overhead of flooding link state information is reduced by requiring fewer nodes to forward the information
- A broadcast from node X is only forwarded by its *multipoint relays*
- Multipoint relays of node X are its neighbors such that each two-hop neighbor of X is a one-hop neighbor of at least one multipoint relay of X
  - Each node transmits its neighbor list in periodic beacons, so that all nodes can know their 2-hop neighbors, in order to choose the multipoint relays

OLSR (1)

- Nodes C and E are multipoint relays of node A

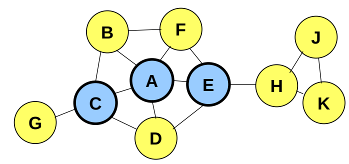


Node that has broadcast state information from A

5

OLSR (2)

- Nodes C and E forward information received from A

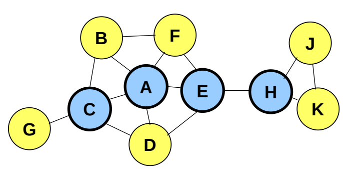


Node that has broadcast state information from A

6

OLSR (3)

- Nodes E and H are multipoint relays for each other
- Node H forwards information received to E
  - E has already forwarded the same information once, so discard



Node that has broadcast state information from A

7

OLSR (4)

- OLSR floods information through the multipoint relays
- The flooded itself is fir links connecting nodes to respective multipoint relays
- Routes used by OLSR only include multipoint relays as intermediate nodes

8

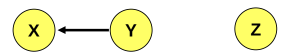
Destination-Sequenced Distance-Vector (DSDV)

- [PB94] C. E. Perkins and P. Bhagwat, "Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers, *ACM SIGCOMM*, 1994.
- Each node maintains a routing table which stores
  - Next hop towards each destination
  - A cost metric for the path to each destination
  - A destination sequence number that is created by the destination itself
  - Sequence numbers used to avoid formation of loops
- Each node periodically forwards the routing table to its neighbors
  - Each node increments and appends its sequence number when sending its local routing table
  - This sequence number will be attached to route entries created for this node

9

DSDV (1)

- Assume that node X receives routing information from Y about a route to node Z

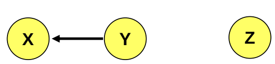


- Let S(X) and S(Y) denote the destination sequence number for node Z as stored at node X, and as sent by node Y with its routing table to node X, respectively

10

DSDV (2)

- Node X takes the following steps:



  - If S(X) > S(Y), then X ignores the routing information received from Y
  - If S(X) = S(Y), and cost of going through Y is smaller than the route known to X, then X sets Y as the next hop to Z
  - If S(X) < S(Y), then X sets Y as the next hop to Z, and S(X) is updated to equal S(Y)

11

EEC173B/ECS152C, Winter 2006

MANET Unicats Routing

- Proactive Protocols
  - OLSR
  - DSDV
- **Hybrid Protocols**

Acknowledgment: Selected slides from Prof. Nitin Vaidya

Zone Routing Protocol (ZRP)

Zone routing protocol combines

- Proactive protocol: which pro-actively updates network state and maintains route regardless of whether any data traffic exists or not
- Reactive protocol: which only determines route to a destination if there is some data to be sent to the destination

[HP98] Z. J. Haas and M. R. Pearlman, "The Performance of Query Control Schemes for the Zone Routing Protocol," *ACM SIGCOMM*, 1998.

13

ZRP: Routing Zone vs. Peripheral

- All nodes within hop distance at most *d* from a node X are said to be in the routing zone of node X
- All nodes at hop distance exactly *d* are said to be peripheral nodes of node X's routing zone

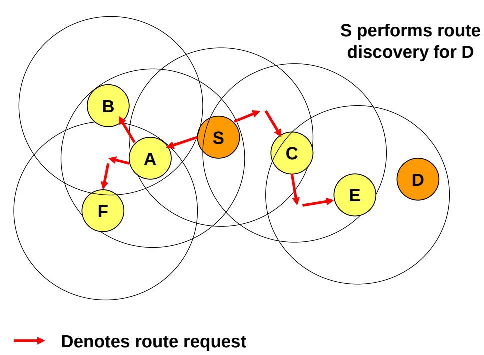
14

ZRP

- Intra-zone routing: Pro-actively maintain state information for links within a short distance from any given node
  - Routes to nodes within short distance are thus maintained proactively (using, say, link state or distance vector protocol)
- Inter-zone routing: Use a route discovery protocol for determining routes to far away nodes. Route discovery is similar to DSR with the exception that route requests are propagated via peripheral nodes.

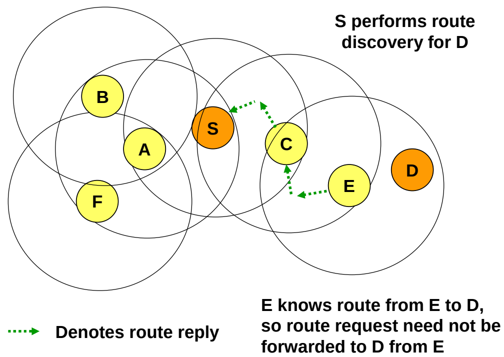
15

ZRP: Example with Zone Radius = *d* = 2



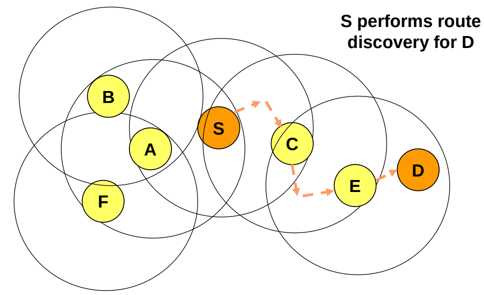
16

ZRP: Example with $d = 2$



Denotes route reply

ZRP: Example with $d = 2$



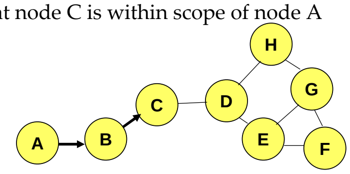
Denotes route taken by Data

Landmark Routing (LANMAR) for MANET with Group Mobility

- [PGH00] G. G. Pei, M. Gerla, and X. Hong, "ANMAR: Landmark Routing for Large Scale Wireless Ad Hoc Networks with Group Mobility," *ACM Mobihoc*, 2000.
- A *landmark* node is elected for a group of nodes that are likely to move together
- A *scope* is defined such that each node would typically be within the scope of its landmark node
- Each node propagates *link state* information corresponding only to nodes within it *scope* and *distance-vector* information for all *landmark* nodes
  - Combination of link-state and distance-vector
  - Distance-vector used for landmark nodes outside the scope
  - No state information for non-landmark nodes outside scope maintained

LANMAR Routing to Nodes Within Scope

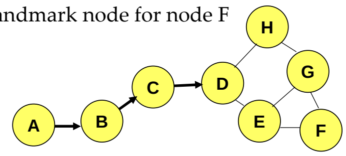
- Assume that node C is within scope of node A



- Routing from A to C: Node A can determine next hop to node C using the available link state information

LANMAR Routing to Nodes Outside Scope

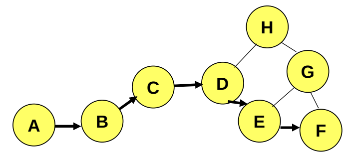
- Routing from node A to F which is outside A's scope
- Let H be the landmark node for node F



- Node A somehow knows that H is the landmark for C
- Node A can determine next hop to node H using the available distance vector information

LANMAR Routing to Nodes Outside Scope

- Node D is within scope of node F



- Node D can determine next hop to node F using link state information
- The packet for F may never reach the landmark node H, even though initially node A sends it towards H

Routing

- Protocols discussed so far find/maintain a route provided it exists
- Some protocols attempt to ensure that a route exists by
  - Power Control
  - Limiting movement of hosts or forcing them to take detours

MANET Implementation Issues

Where to Implement Ad Hoc Routing

- Link layer
- Network layer
- Application layer

Implementation Issues: Security

- How can I trust you to forward my packets without tampering?
  - Need to be able to detect tampering
- How do I know you are what you claim to be ?
  - Authentication issues
  - Hard to guarantee access to a certification authority

25

Implementation Issues

- Can we make any guarantees on performance?
  - When using a non-licensed band, difficult to provide hard guarantees, since others may be using the same band
- Must use an licensed channel to attempt to make any guarantees
- Only some issues have been addresses in existing implementations
- Security issues often ignored
- Address assignment issue also has not received sufficient attention

26

Integrating MANET with the Internet

- Mobile IP + MANET routing
- At least one node in a MANET should act as a gateway to the rest of the world
- Such nodes may be used as foreign agents for Mobile IP
- IP packets would be delivered to the foreign agent of a MANET node using Mobile IP. Then, MANET routing will route the packet from the foreign agent to the mobile host.

27

Internet Engineering Task Force (IETF)

- IETF manet (**Mobile Ad-hoc Networks)** working group
  - *http://www.ietf.org/html.charters/manet-charter.html*
- IETF mobileip (**IP Routing for Wireless/Mobile Hosts)** working group
  - *http://www.ietf.org/html.charters/mobileip-charter.html*
- IETF pilc (**Performance Implications of Link Characteristics)** working group
  - *http://www.ietf.org/html.charters/pilc-charter.html*
  - *http://pilc.grc.nasa.gov*
  - Refer [RFC2757] for an overview of related work

28

MANET Performance

- Studies comparing different routing protocols for MANET typically measure UDP performance
- UDP provides unreliable delivery
- Several performance metrics are often used
  - Routing overhead per data packet
  - Packet loss rate
  - Packet delivery delay

29

UDP Performance

- Results comparing a specific pair of protocols do not always agree, but some general (and intuitive) conclusions can be drawn
  - Reactive protocols may yield lower routing overhead than proactive protocols when communication density is low
  - Reactive protocols tend to loose more packets (assuming than network layer drops packets if a route is not known)
  - Proactive protocols perform better with high mobility and dense communication graph

30

Many variables affect performance

- Traffic characteristics
  - one-to-many, many-to-one, many-to-many
  - small bursts, large file transfers, real-time, non-real-time
- Mobility characteristics
  - low/high rate of movement
  - do nodes tend to move in groups
- Node capabilities
  - transmission range (fixed, changeable)
  - battery constraints
- Performance metrics
  - delay
  - throughput
  - latency
  - routing overhead
- Static or dynamic system characteristics (listed above)

31

UDP Performance

- Difficult to identify a single scheme that will perform well in all environments
- Holy grail: Routing protocol that dynamically adapts to all environments so as to optimize "performance"
  - Performance metrics may differ in different environments

32

Performance of TCP

Several factors affect TCP performance in MANET:

- Wireless transmission errors
- Multi-hop routes on shared wireless medium
  - For instance, adjacent hops typically cannot transmit simultaneously
- Route failures due to mobility

33

Random vs. Bursty Errors

- If number of errors is small, they may be corrected by an error correcting code
- Excessive bit errors result in a packet being discarded, possibly before it reaches the transport layer
- Random loss may cause fast retransmit
  - Reducing congestion window in response to errors is unnecessary => reduces the throughput
- Bursty errors may cause time-outs
  - If wireless link remains unavailable for extended duration, a window worth of data may be lost, e.g., driving through a tunnel or passing a truck
  - Timeout results in slow start => reduces the throughput

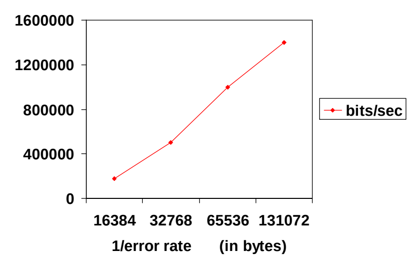
34

Congestion Response

- Sometimes Congestion Response May be Appropriate in Response to Errors
- On a CDMA channel, errors occur due to interference from other user, and due to noise [Karn99pilc]
  - Interference due to other users is an indication of congestion. If such interference causes transmission errors, it is appropriate to reduce congestion window
  - If noise causes errors, it is not appropriate to reduce window
- When a channel is in a bad state for a long duration, it might be better to let TCP backoff, so that it does not unnecessarily attempt retransmissions while the channel remains in the bad state [Padmanabhan99pilc]

35

Impact of Random Errors [Vaidya99]



Exponential error model
2 Mbps wireless full duplex link
No congestion losses

36

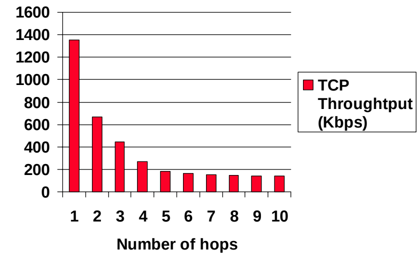
TCP Throughput over MANET

- [HV99] G. Holland and N. Vaidya, "Analysis of TCP Performance over Mobile Ad Hoc Networks," *ACM Mobicom*, 1999.
- [FPL+03] Z. Fu, P. Zerfos, H. Luo, S. Lu, L. Zhang and M. Gerla, "The Impact of Multihop Wireless Channel on TCP Throughput and Loss," *IEEE INFOCOM'03*, San Francisco, March 2003.
  - TCP performance over multi-hop wireless networks that use IEEE 802.11 access methods

- Connections over multiple hops are at a disadvantage compared to shorter connections, because they have to contend for wireless access at each hop

37

Impact of Multi-Hop Wireless Paths [HV99]



TCP Throughput using 2 Mbps 802.11 MAC

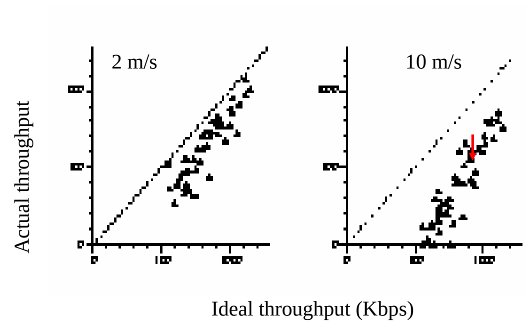
38

Throughput Degradations with Increasing Number of Hops

- Packet transmission can occur on at most one hop among three consecutive hops
  - Increasing the number of hops from 1 to 2, 3 results in increased delay, and decreased throughput
- Increasing number of hops beyond 3 allows simultaneous transmissions on more than one link, however, degradation continues due to contention between TCP Data and Acks traveling in opposite directions
- When number of hops is large enough, the throughput stabilizes due to *effective pipelining*

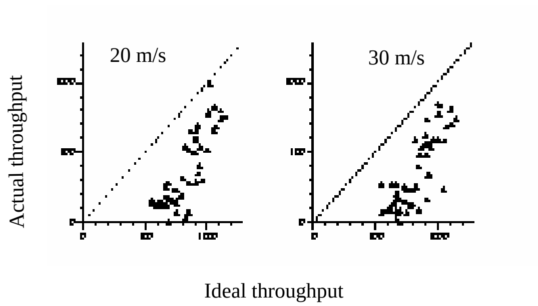
39

Impact of Mobility TCP Throughput



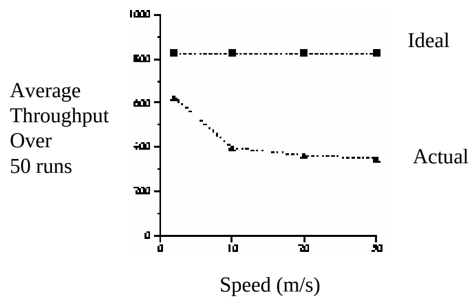
40

Impact of Mobility



41

Throughput generally degrades with increasing speed …



42

TCP Performance

Two factors result in degraded throughput in presence of mobility:

- Loss of throughput that occurs while waiting for TCP sender to timeout (as seen earlier)
  - This factor can be mitigated by using explicit notifications and better route caching mechanisms
- Poor choice of congestion window and RTO values after a new route has been found
  - How to choose *cwnd* and *RTO* after a route change?

43

Issues
Window Size After Route Repair

- Same as before route break: may be too optimistic
- Same as startup: may be too conservative
- Better be conservative than overly optimistic
  - Reset window to small value after route repair
  - Let TCP figure out the suitable window size
  - Impact low on paths with small delay-bw product

44

Issues
RTO After Route Repair

- Same as before route break
  - If new route long, this RTO may be too small, leading to timeouts
- Same as TCP start-up (6 second)
  - May be too large
  - May result in slow response to next packet loss
- Another plausible approach: new RTO = function of old RTO, old route length, and new route length
  - Example: new RTO = old RTO * new route length / old route length
  - Not evaluated yet
  - Pitfall: RTT is not just a function of route length

45

Out-of-Order Packet Delivery

- Out-of-order (OOO) delivery may occur due to:
  - Route changes
  - Link layer retransmissions schemes that deliver OOO
- Significantly OOO delivery confuses TCP, triggering fast retransmit
- Potential solutions:
  - Deterministically prefer one route over others, even if multiple routes are known
  - Reduce OOO delivery by re-ordering received packets
    - can result in unnecessary delay in presence of packet loss
  - Turn off fast retransmit
    - can result in poor performance in presence of congestion

46