Lecture 4: Mobile Ad Hoc and Sensor Networks (I)

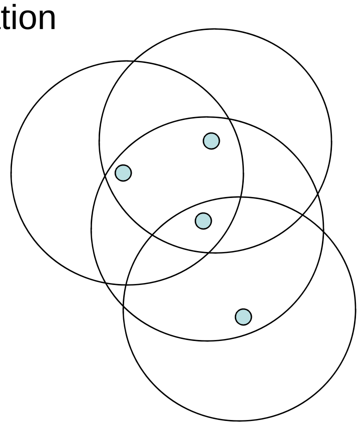
Ing-Ray Chen

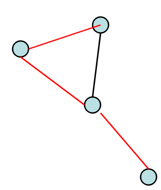
CS 6204 Mobile Computing
Virginia Tech

Courtesy of G.G. Richard III for providing some of the slides

Mobile Ad Hoc Networks

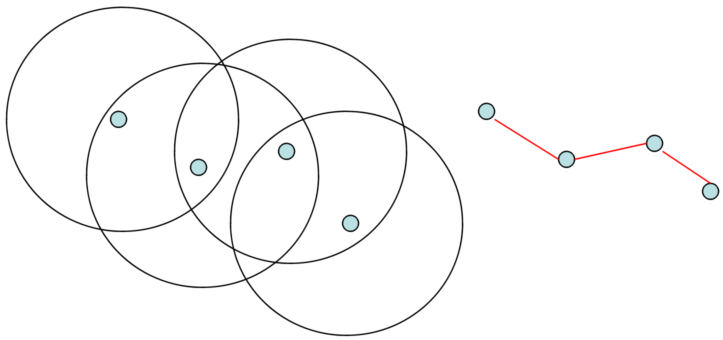
- May need to traverse multiple links to reach a destination





Mobile Ad Hoc Networks

- Mobility causes route changes



Mobile Ad Hoc Networks

- Formed by wireless hosts which may be mobile
- Don't need a pre-existing infrastructure
  - ie, don't need a backbone network, routers, etc.
- Routes between nodes potentially contain multiple hops
- Why MANET?
  - Ease, speed of deployment
  - Decreased dependence on infrastructure
  - Can use in many scenarios where deployment of a wired network is impractical or impossible
  - Lots of military applications, but there are others…

Many Applications

- Personal area networking
  - cell phone, laptop, ear phone, wrist watch
- Civilian environments
  - meeting rooms
  - sports stadiums
  - groups of boats, small aircraft (wired REALLY impractical!!)
- Emergency operations
  - search-and-rescue
  - policing and fire fighting
- Sensor networks
  - Groups of sensors embedded in the environment or scattered over a target area

Many Variations

- Fully Symmetric Environment
  - all nodes have identical capabilities and responsibilities
- Asymmetric Capabilities
  - transmission ranges and radios may differ
  - battery life at different nodes may differ
  - processing capacity may be different at different nodes
  - speed of movement different
- Asymmetric Responsibilities
  - only some nodes may route packets
  - some nodes may act as leaders of nearby nodes (e.g., “cluster head”)

Many Variations

- Traffic characteristics may differ
  - bandwidth
  - timeliness constraints
  - reliability requirements
  - unicast / broadcast / multicast / geocast
- May co-exist (and co-operate) with an infrastructure-based network

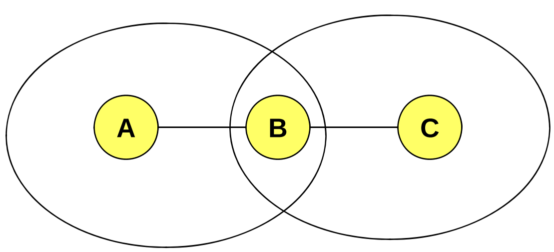
Many Variations

- Mobility patterns may be different
  - people sitting at an airport lounge (little mobility)
  - taxi cabs (highly mobile)
  - military movements (mostly clustered?)
  - personal area network (again, mostly clustered?)
- Mobility characteristics
  - speed
  - predictability
    - direction of movement
    - pattern of movement
  - uniformity (or lack thereof) of mobility characteristics among different nodes

Challenges

- Limited wireless transmission range
- Broadcast nature of the wireless medium
- Packet losses due to transmission errors
- Environmental issues ("chop that tree!!")
- Mobility-induced route changes
- Mobility-induced packet losses
- Battery constraints
- Potentially frequent network partitions
- Ease of snooping on wireless transmissions (security hazard)
- Sensor networks: <u>very</u> resource-constrained!

Hidden Terminal Problem



Nodes A and C cannot hear each other

Transmissions by nodes A and C can collide at node B

On collision, both transmissions are lost

Nodes A and C are <u>hidden</u> from each other

First Issue: Routing

- Why is Ad hoc Routing Different?
- Host mobility
  - link failure/repair due to mobility may have different characteristics than those due to other causes
  - traditional routing algorithms assume relatively stable network topology, few router failures
- Rate of link failure/repair may be high when nodes move fast
- New performance criteria may be used
  - route stability despite mobility
  - energy consumption

Routing Protocols

- Proactive protocols
  - Determine routes independent of traffic pattern
  - Traditional routing protocols for wired networks are proactive
- Reactive protocols
  - Discover/maintain routes only if needed

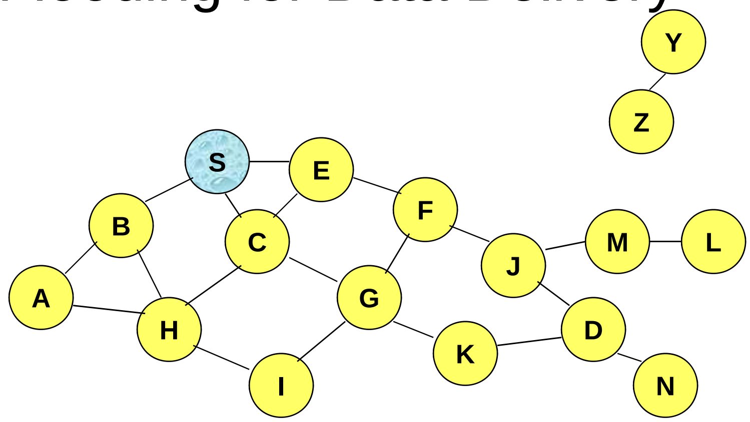
Trade-Off: Proactive vs. Reactive

- 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
- 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 tradeoff 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 will be used to avoid the possibility of forwarding the same packet more than once
- Packet P reaches destination D provided that D is reachable from sender S
- Node D does not forward the packet

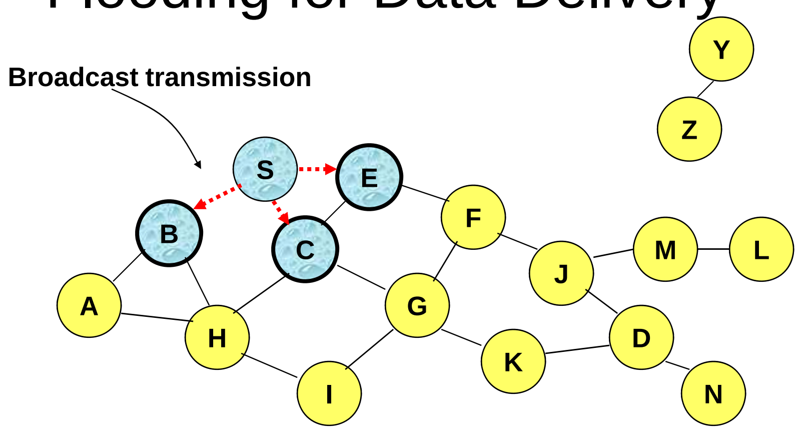
Flooding for Data Delivery



Represents a node that has received packet P

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

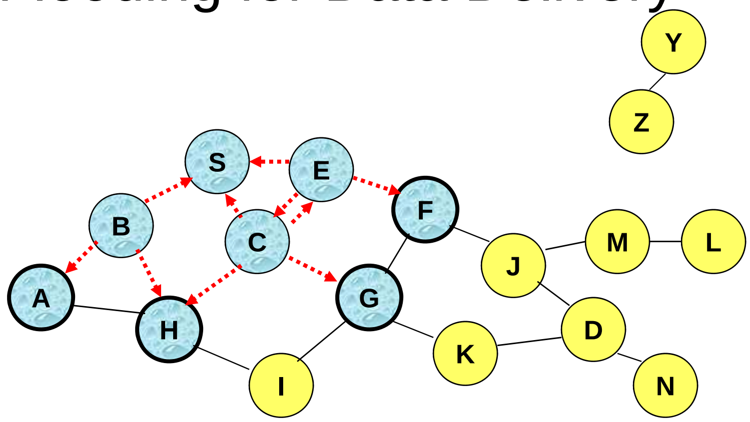
Flooding for Data Delivery



Represents a node that receives packet P for the first time

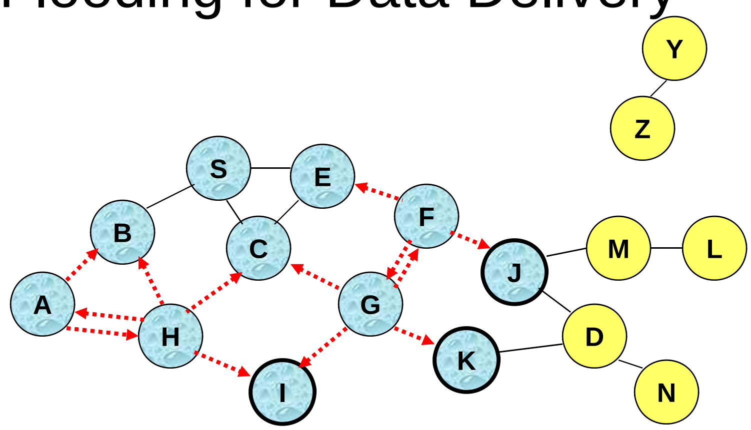
Represents transmission of packet P

Flooding for Data Delivery



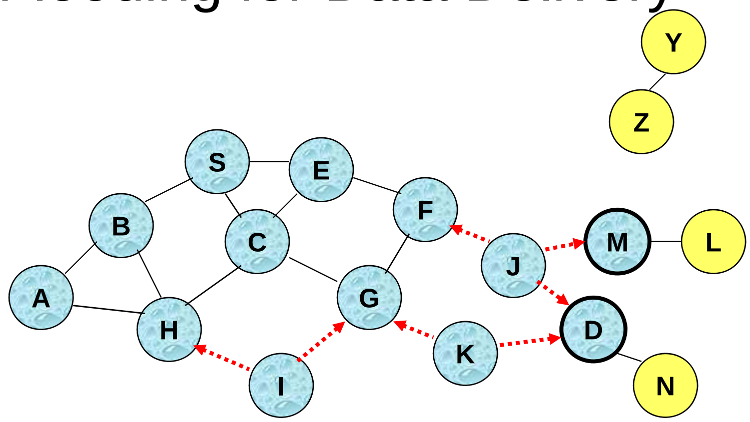
Node H receives packet P from two neighbors:
potential for collision

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

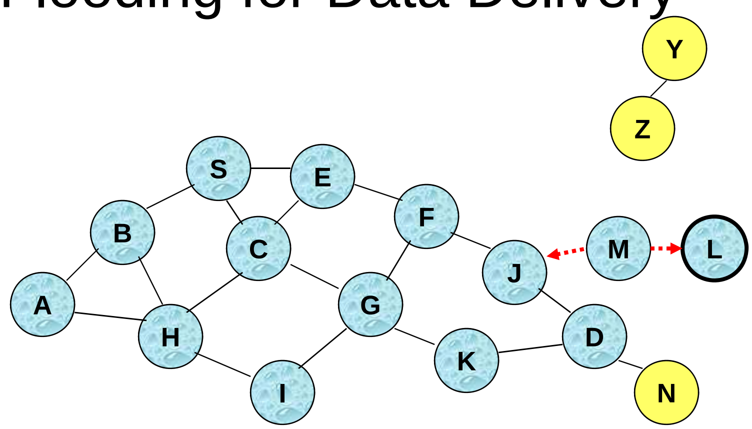
Flooding for Data Delivery



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

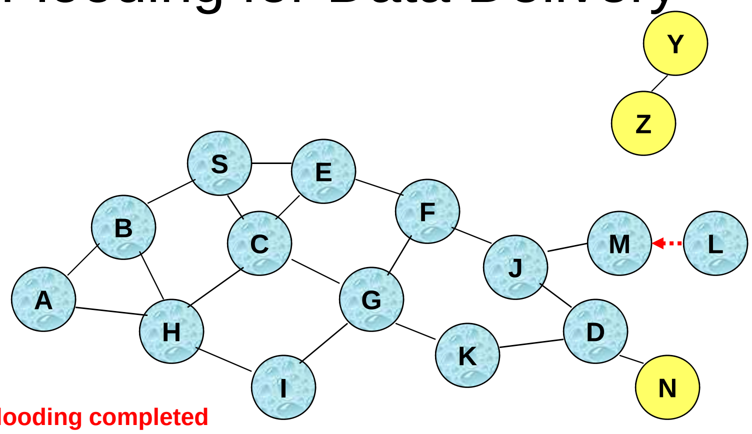
=> Packet P may not be delivered to node D at all, despite the use of flooding!!

Flooding for Data Delivery



- **Node D does not forward packet P, because node D is the intended destination of packet P**

Flooding for Data Delivery

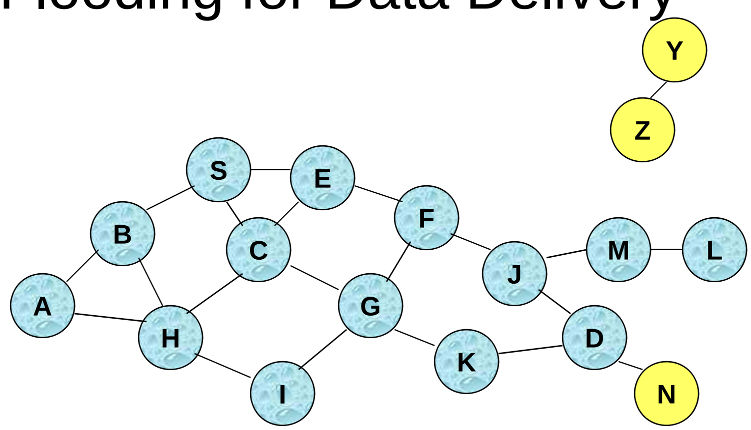


Flooding completed

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 for Data Delivery



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

Flooding for Data Delivery: Advantages

- Simplicity
- More efficient than other protocols when the rate of information transmission is low enough that the overhead of explicit route discovery/maintenance incurred by other protocols is relatively higher
  - 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
- **For high mobility patterns, it may be the only reasonable choice**

Flooding for Data Delivery: Disadvantages

- Potentially, very high overhead
  - Data packets may be delivered to too many nodes that 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, destination would not receive the packet at all

Flooding of Control Packets

- Many protocols perform (potentially *limited*) flooding of control packets, instead of data packets
- The control packets are used to discover routes
- Discovered routes are subsequently used to send data packets without flooding
- Overhead of control packet flooding is amortized over data packets transmitted between consecutive control packet floods

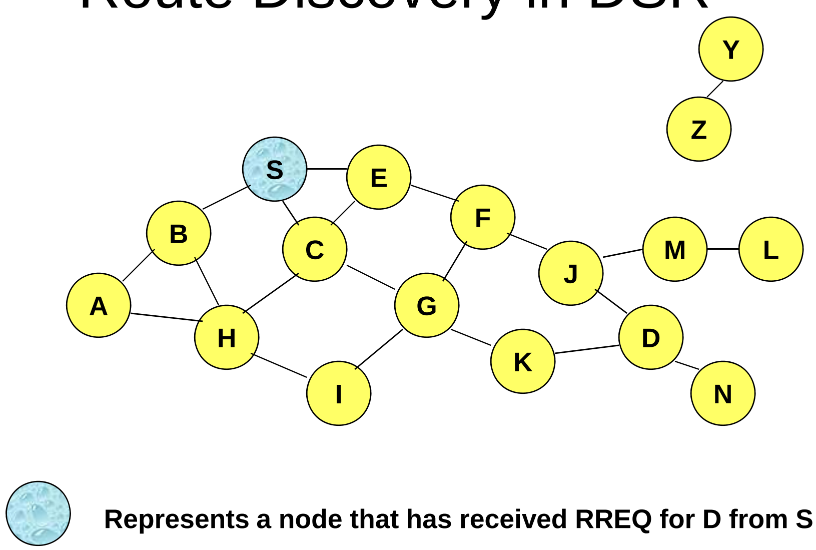
Metrics for Ad Hoc Routing

- Want to optimize
  - Number of hops
  - Distance
  - Latency
  - Load balancing for congested links
  - Cost ($$$)
  - …
- Many existing ad hoc routing descriptions use # of hops
- More work recently on latency, load balancing, etc.

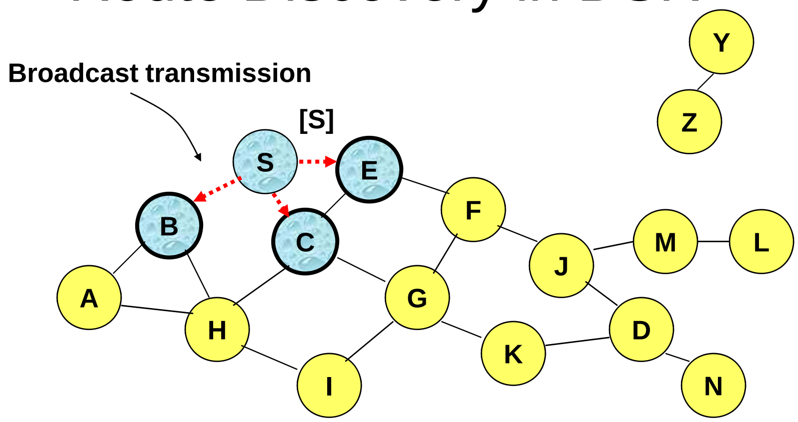
Dynamic Source Routing – DSR (Ref [9])

- When node S wants to send a packet to node D, but does not know a route to D, node S initiates a route discovery by flooding a Route Request (RREQ) packet
- Each node appends own identifier when forwarding RREQ
- A route if discovered will return from D to S
- 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
- Reactive: Routes are discovered only when a node wants to send data and route to destination is unavailable

Route Discovery in DSR



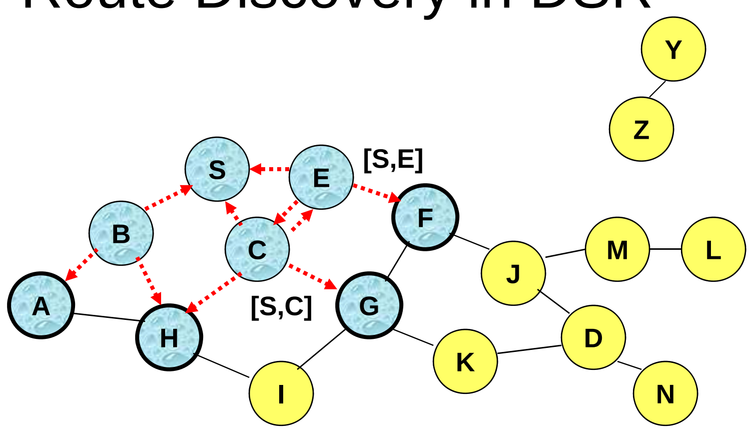
Route Discovery in DSR



Represents transmission of RREQ

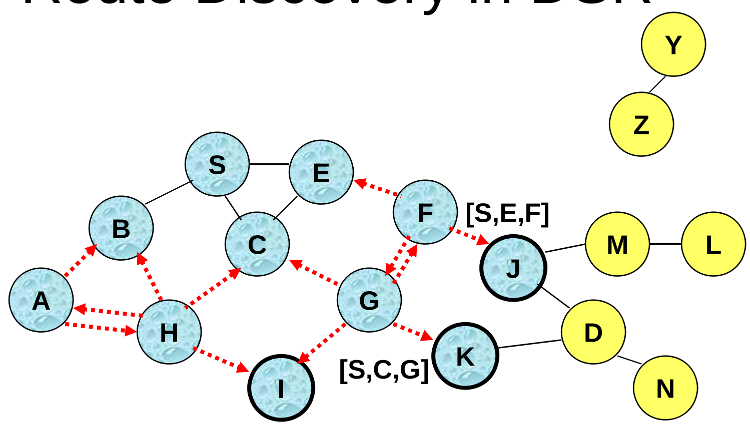
[X,Y] Represents list of identifiers appended to RREQ

Route Discovery in DSR



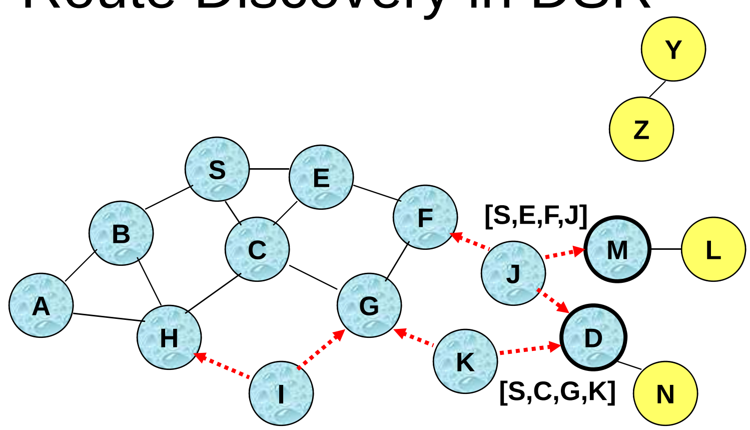
Node H receives packet RREQ from two neighbors:
potential for collision

Route Discovery in DSR



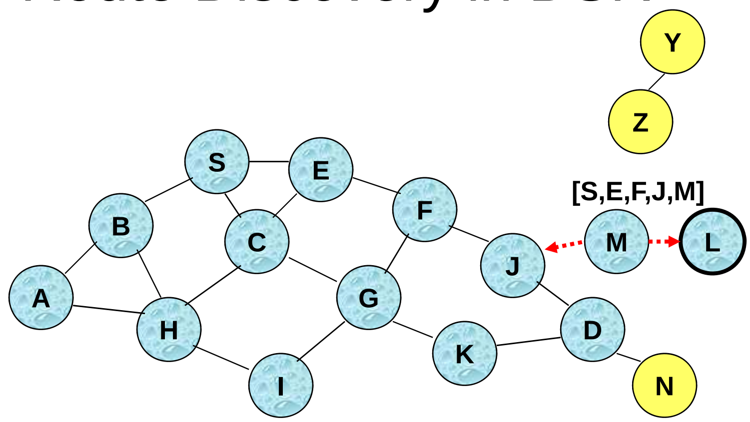
Node C receives RREQ from G and H, but does not forward it again, because node C has already forwarded RREQ once

Route Discovery in DSR



Nodes J and K both broadcast RREQ to node D
Since nodes J and K are hidden from each other, their transmissions may collide

Route Discovery in DSR

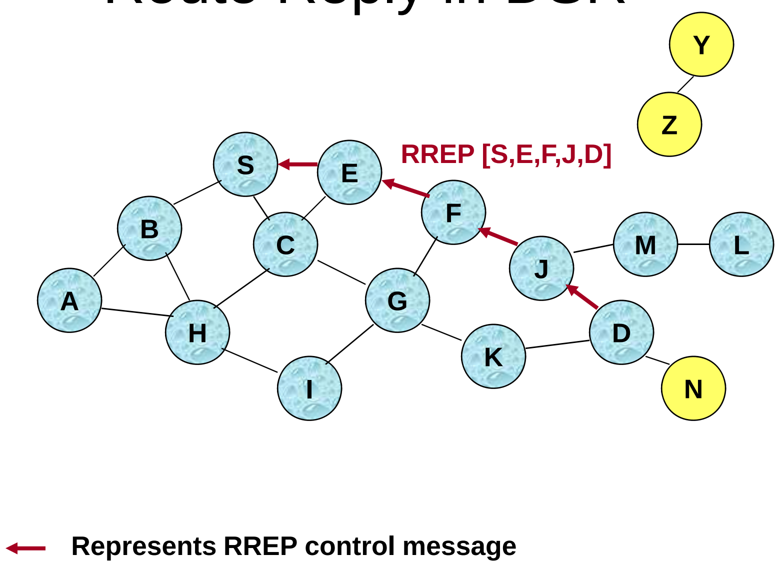


Node D does not forward RREQ, because node D is the intended target of the route discovery

Route Discovery in DSR: Part 2

- 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 (and from D to S) on which RREQ was received by node D

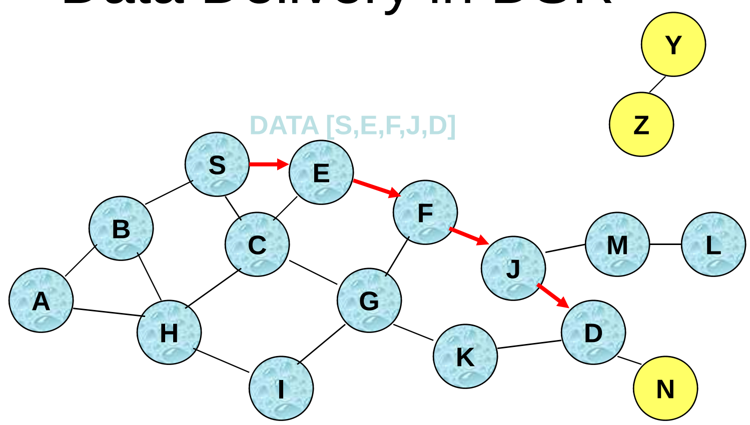
Route Reply in DSR



Route Reply in DSR

- Route Reply can be sent by reversing the route in Route Request (RREQ) only if links are <u>guaranteed to be bi-directional</u>
  - To ensure this, RREQ should be forwarded only if it is received on a link that is known to be bi-directional
- If unidirectional (asymmetric) links are allowed, then RREP may need a route discovery for S from node D
  - Unless node D already knows a route to node S
  - **If a route discovery is initiated by D for a route to S, then the Route Reply is piggybacked on the Route Request from D.**
- Node S on receiving RREP, caches the route included in the RREP

Data Delivery in DSR



Packet header size grows with route length

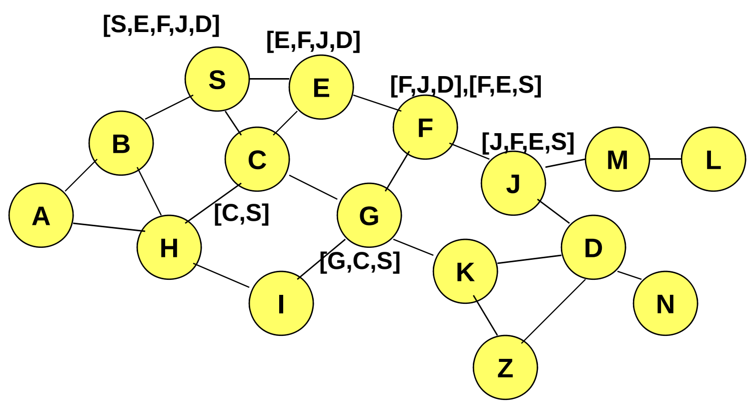
DSR Optimization: Route Caching

- Each node caches a new route it learns by *any means*
  - e.g., When node S finds route [S,E,F,J,D] to node D, node S also learns route [S,E,F] to node F
  - When node K receives Route Request RREQ [S,C,G] destined for node D, node K learns of reverse route [K,G,C,S] to node S
  - When node F forwards Route Reply RREP [S,E,F,J,D] to S, node F learns route [F,J,D] to node D
  - When node E forwards data through route [S,E,F,J,D] it learns route [E,F,J,D] to node D
- A node may also learn a route when it overhears data packets, even though it is not directly involved in the transmission

Route Caching (2)

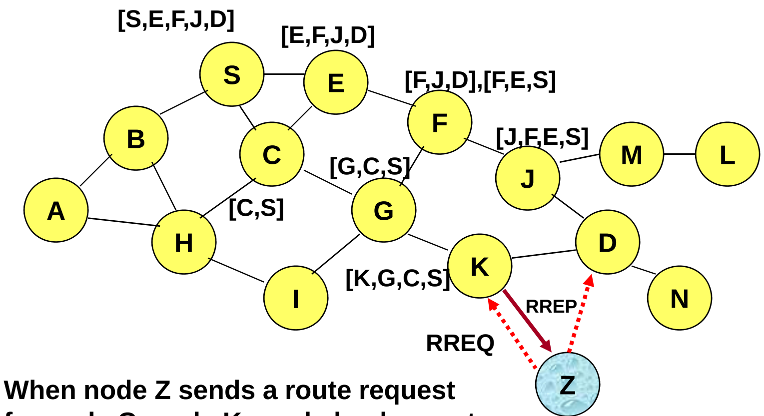
- When node S learns that a route to node D is broken, it uses another route from its local cache, if such a route to D exists in its cache.
- Otherwise, node S initiates route discovery by sending a route request
- Node X, on receiving a Route Request for some node D, can send a Route Reply directly if node X knows a route to node D
- Use of route cache
  - can speed up route discovery
  - can reduce propagation of route requests

Route Caching (3)



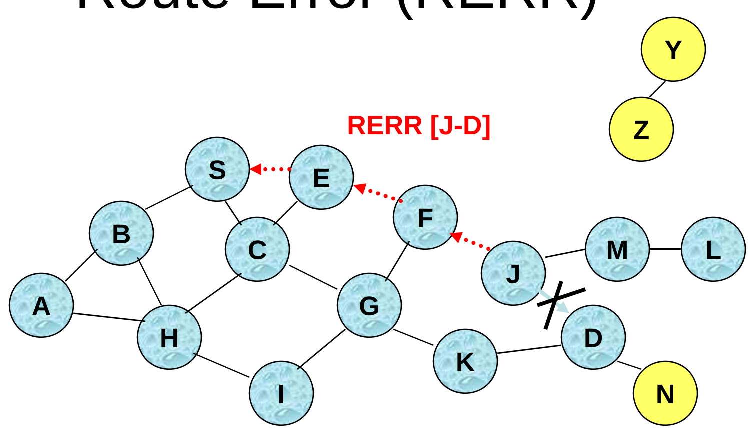
[P,Q,R] Represents cached route at a node
(DSR maintains the cached routes in a tree format)

Route Caching (4)



When node Z sends a route request for node C, node K sends back a route reply [Z,K,G,C] to node Z using a locally cached route

Route Error (RERR)



when J attempt to forward the data packet (with route SEFJD) to S but J-D fails, J sends a route error packet to S along route J-F-E-S

Nodes hearing RERR update their route cache to remove link J-D

Route Caching: Beware!

- Stale caches can adversely affect performance
- With passage of time and host mobility, cached routes may become invalid
- A sender host may try several stale routes (obtained from local cache, or replied from cache by other nodes), before finding a good route
- It may be <u>more expensive</u> to try several broken routes than to simply discover a new one!
- RERR messages are unreliable, so news of broken routes may not even propagate completely!

DSR: Advantages

- Routes maintained only between nodes who need to communicate
  - reduces overhead of route maintenance
- Route caching can further reduce route discovery overhead
- A single route discovery may yield many routes to the destination, due to intermediate nodes replying from local caches

DSR: Disadvantages

- Packet header size grows with route length due to source routing
- Flood of route requests may potentially reach all nodes in the network
- Care must be taken to avoid collisions between route requests propagated by neighboring nodes
  - insertion of random delays before forwarding RREQ
- Increased contention if too many route replies come back due to nodes replying using their local cache
  - Route Reply Storm problem
  - Reply storm may be eased by preventing a node from sending RREP if it hears another RREP with a shorter route

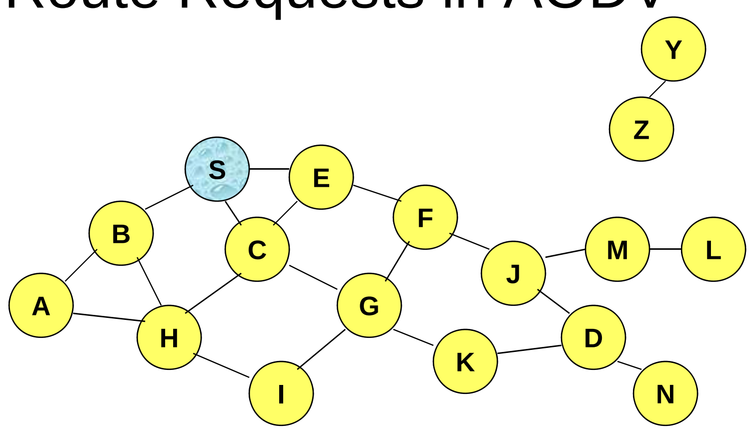
DSR: Disadvantages (2)

- An intermediate node may send Route Reply using a **<u>stale</u>** cached route, thus polluting other caches
- This problem can be eased if some mechanism to purge (potentially) invalid cached routes is incorporated.
  - Static timeouts
  - Adaptive timeouts based on
    - expected rate of mobility (mobility prediction is useful here)
    - number of changes, or number of routes that get expired

Ah-Hoc On-Demand Distance Vector (AODV)

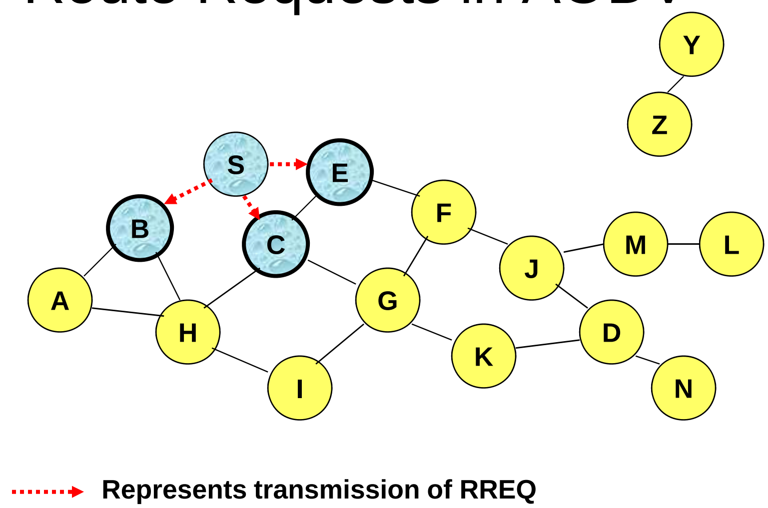
- Distance vector-based routing for ad hoc networks
- Significantly more complicated protocol than DSR, because avoiding routing loops is much more difficult
  - Loop elimination easy in DSR because entire route is available!
- The following pictorial does <u>not</u> expose the complexity of AODV—just to give a basic idea

Route Requests in AODV

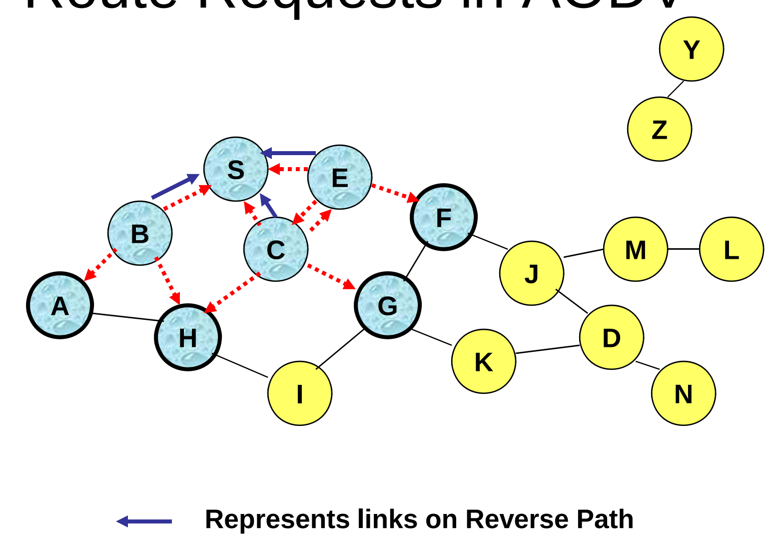


Represents a node that has received RREQ from S for D

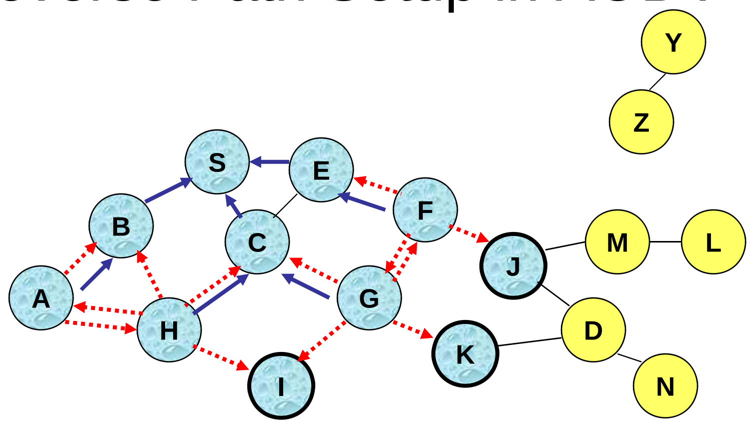
Route Requests in AODV



Route Requests in AODV

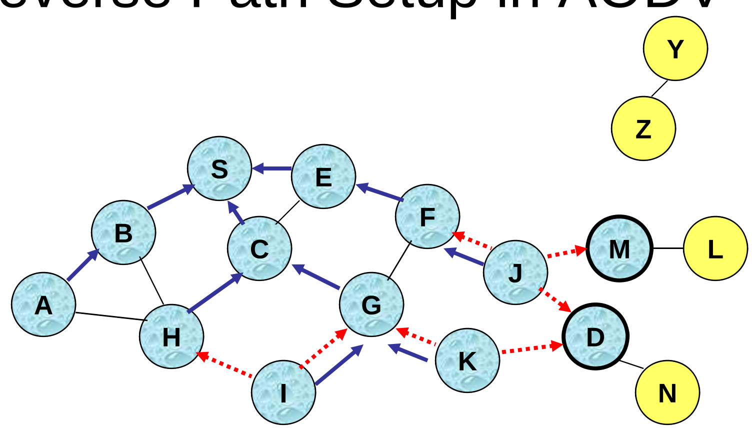


Reverse Path Setup in AODV

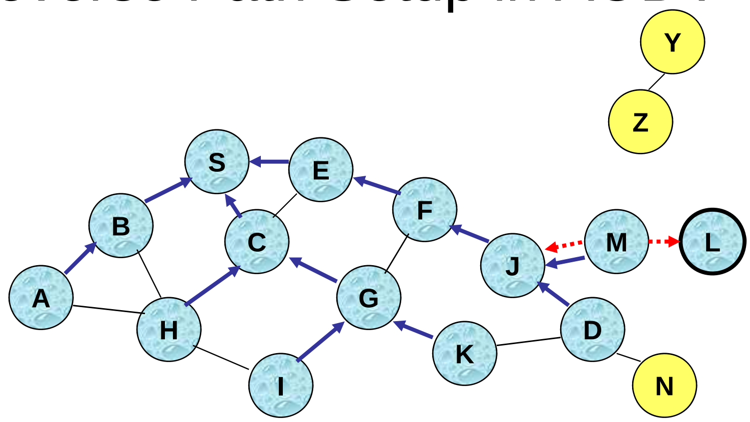


Node C receives RREQ from G and H, but does not forward it again, because node C has already forwarded RREQ once

Reverse Path Setup in AODV

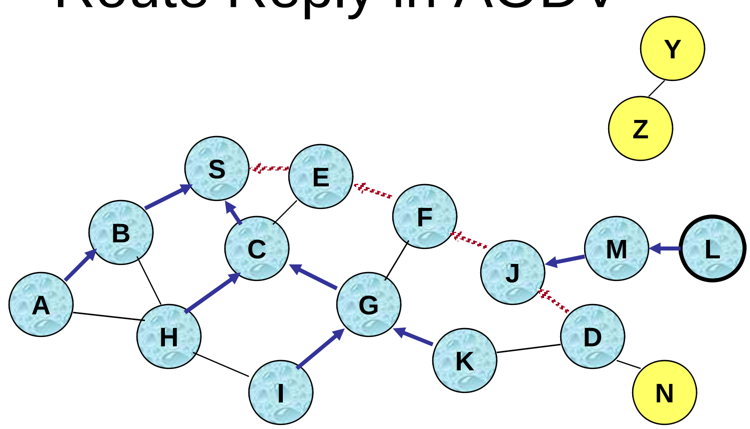


Reverse Path Setup in AODV



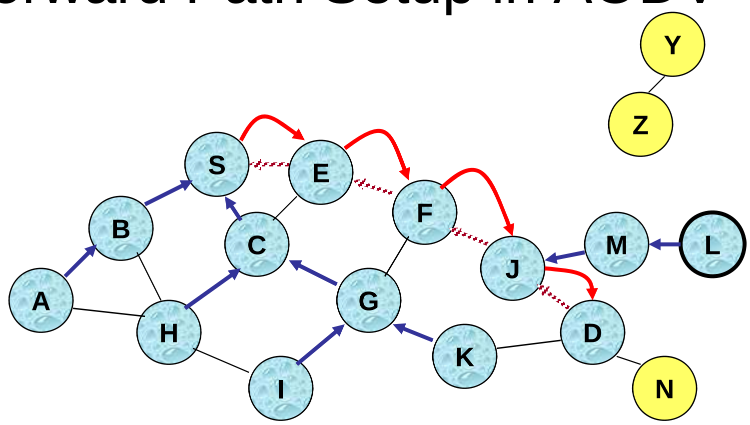
- Node D unitcasts RREP to S
- Since each node receiving the request caches a route back to S, the RREP can be unicast back from the destination to the source

Route Reply in AODV



Represents links on path taken by RREP

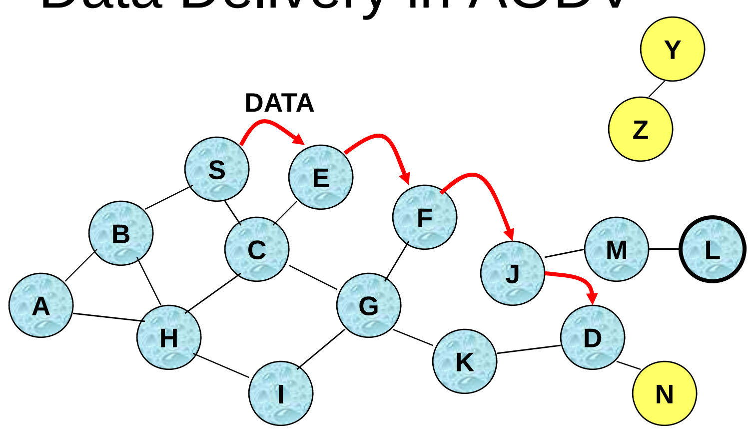
Forward Path Setup in AODV



Forward links are setup when RREP travels along the reverse path

 **Represents a link on the forward path**

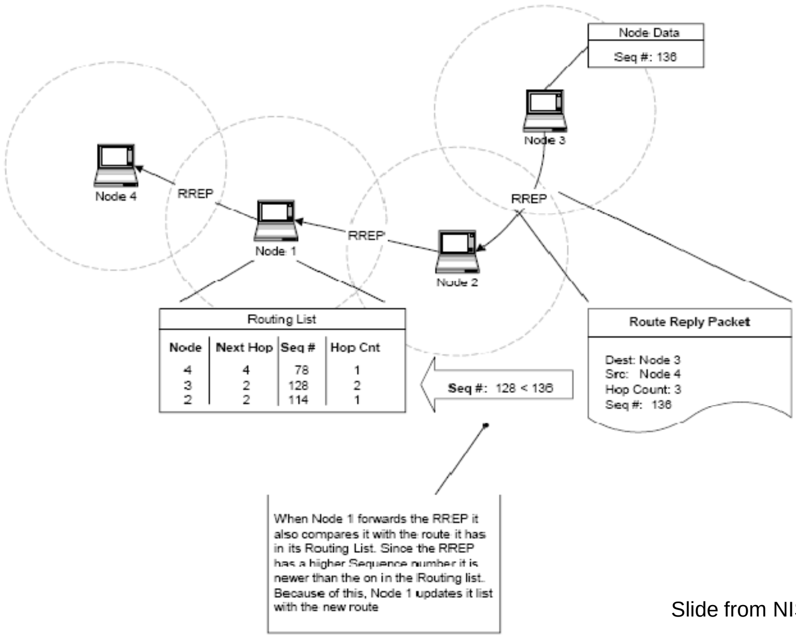
Data Delivery in AODV



Routing table entries used to forward data packet.

Route is *not* included in packet header.

Routing Table Format in AODV



Slide from NIST

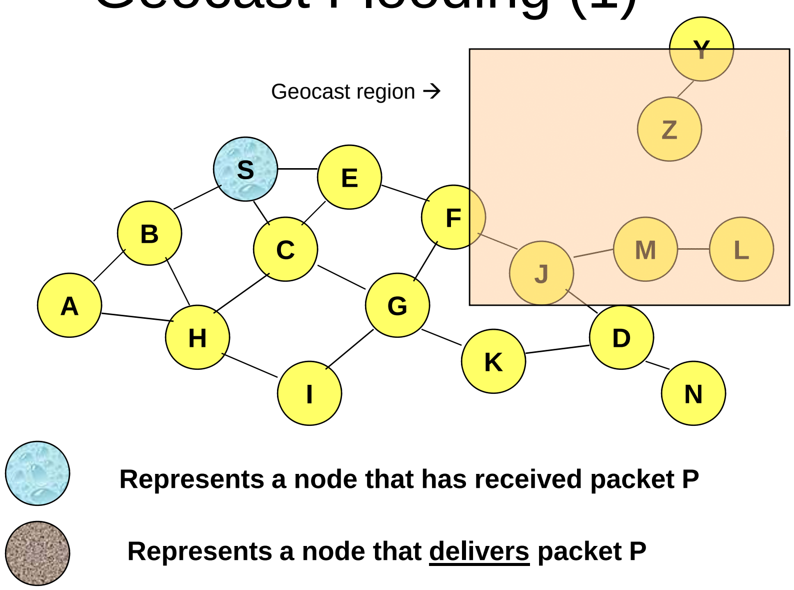
Geocasting (Ref [10])

- Geocast group is defined as the set of nodes that reside in a specified geographical region
- Unlike multicast, where nodes explicitly join and leave a group, membership in a geocast group is a function of "standing in the right place"
- Geocasts are useful to deliver location-dependent information
  - Only the people standing or walking near a building
  - "Attack!!" for units in a particular region
- "Geocast region" defines the delivery area

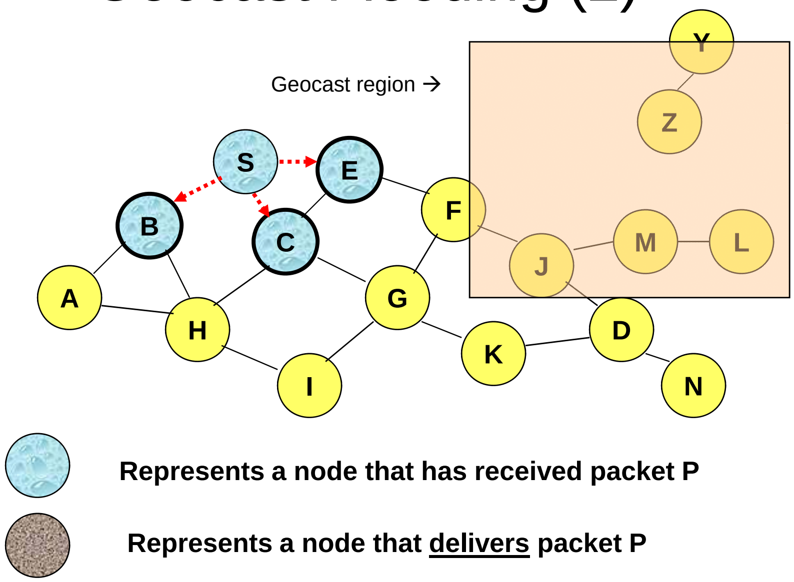
Geocasting by Flooding

- Use the basic flooding algorithm, where a packet sent by a geocast sender is flooded to all reachable nodes in the network
- The geocast region is tagged onto the geocast message
- Regions are generally circular or rectangular, but can (in theory) be any shape
- When a node receives a geocast packet by the basic flooding protocol, the packet is delivered to the application only if the node's location is within the geocast region
- GPS (or similar) is used to know location

Geocast Flooding (1)



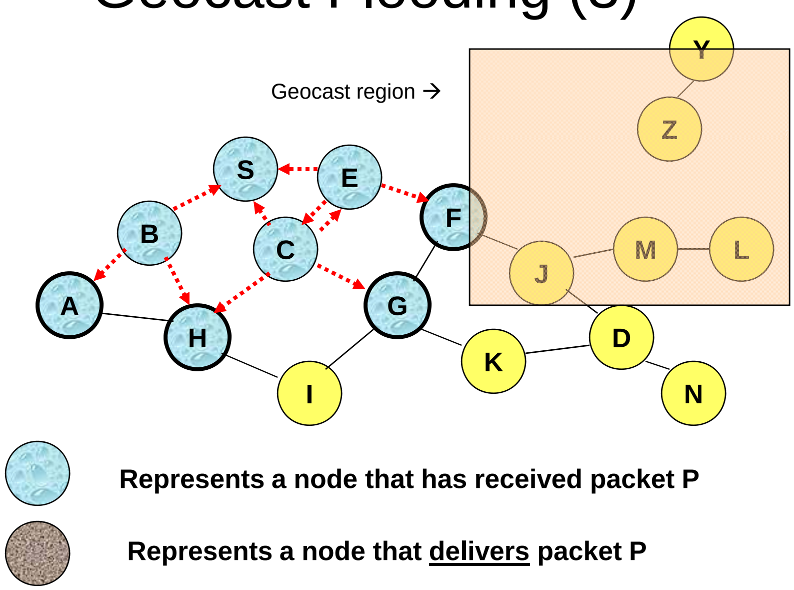
Geocast Flooding (2)



Represents a node that has received packet P

Represents a node that **delivers** packet P

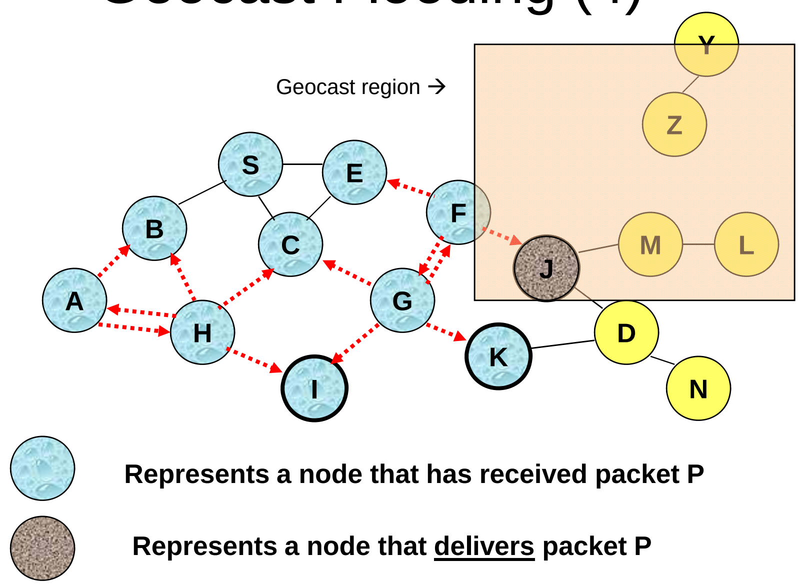
Geocast Flooding (3)



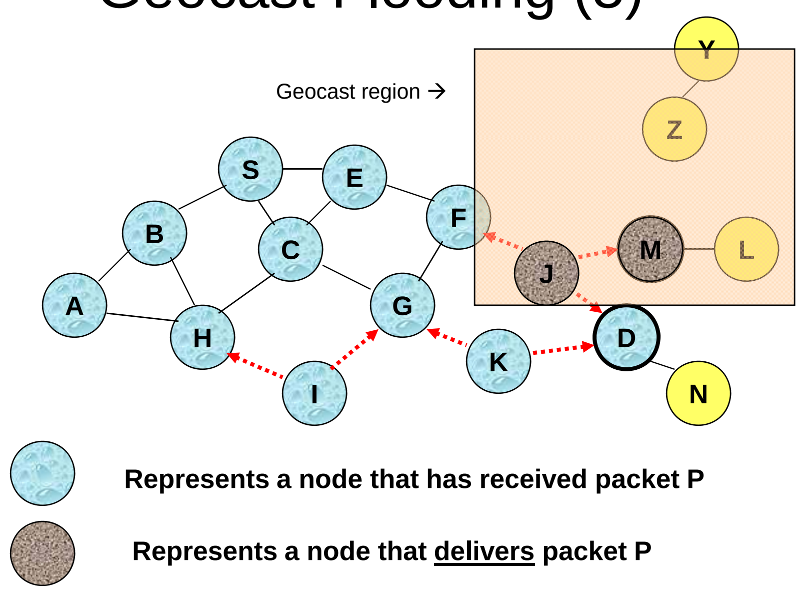
Represents a node that has received packet P

Represents a node that **delivers** packet P

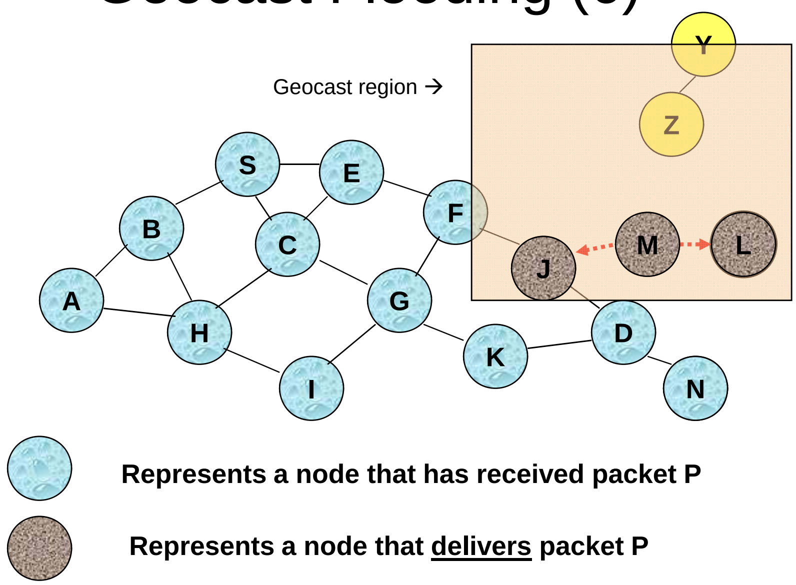
Geocast Flooding (4)



Geocast Flooding (5)



Geocast Flooding (6)



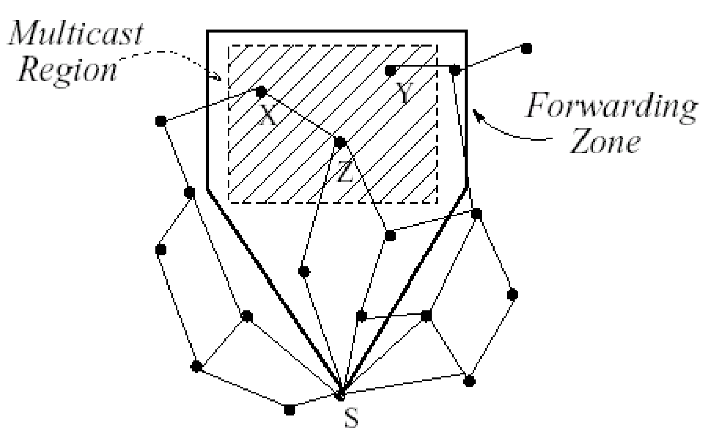
Geocast Flooding: Evaluation

- Advantages:
  - Usual advantages of flooding
  - Simple
  - About as accurate as possible—really gives each node a chance to receive/not receive based on location
- Disadvantages
  - Usual disadvantages of flooding
  - High overhead
    - Nodes must process messages they aren't interested in
    - Potential network congestion
  - Packet reaches all nodes reachable from the source, even nodes far from geocast region

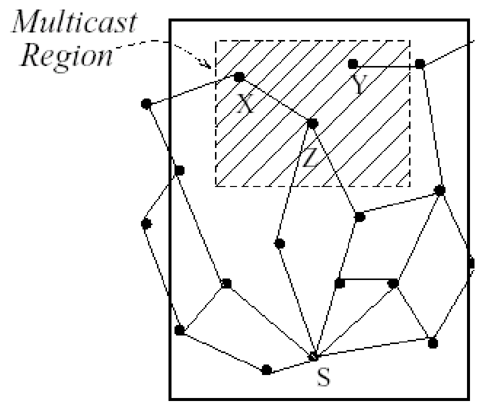
Optimization for Geocast Flooding

- Uses a forwarding zone to reduce flooding
- Only nodes in the forwarding zone continue the flooding operation
- Nodes outside the multicast region may be included in the forwarding zone if the source of the geocast isn't in the multicast region.

Polygonal Forwarding Zone

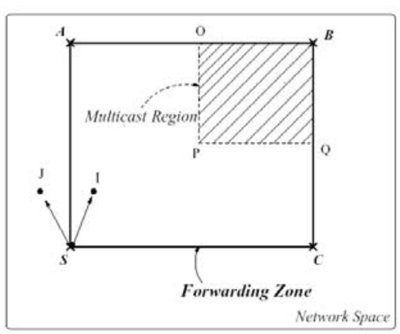


Rectangular Forwarding Zone



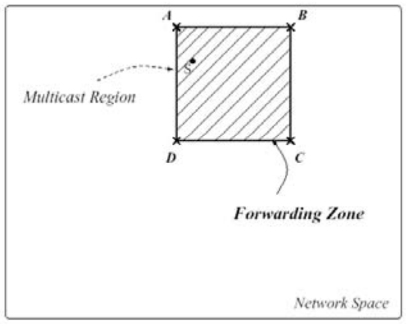
How to Determine Forwarding Zone?

- If source is outside the multicast region, the forwarding zone is the largest rectangle including both multicast region and source

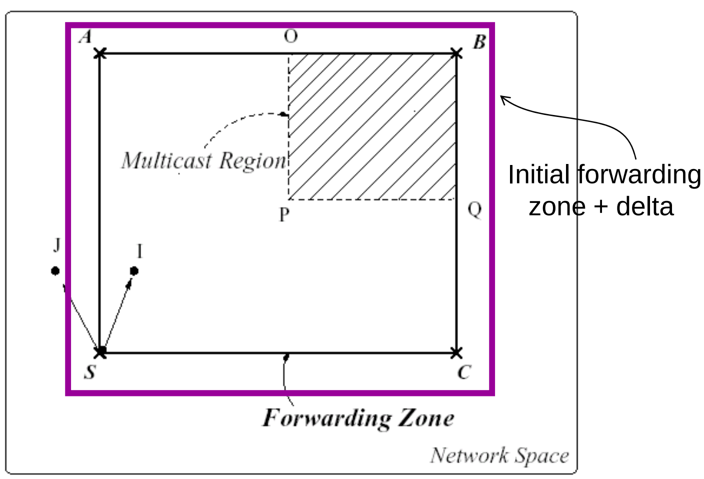


How to (2)

- If source is inside multicast region, can make forwarding zone == multicast region



Increasing Accuracy



Sensor Networks

- Special case of the general ad hoc networking problem
- Much more resource constrained than a network of PDAs or laptops
- Generally, special-purpose
- May have special restrictions, such as:
  - Re-deployment, movement impossible
  - Recharge impossible
  - Likelihood of many nodes being destroyed

Typical Sensor Node

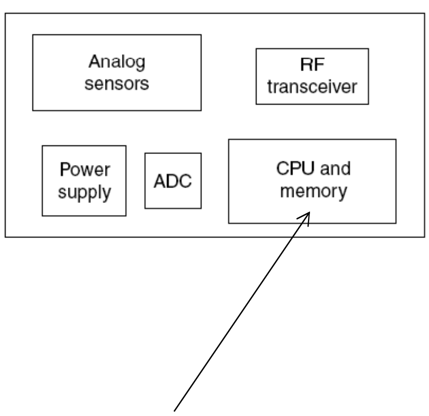


Figure 8.1 Generic wireless sensor node.

~4MHz processor, < 512KB of RAM to hold OS and applications

Typical Sensor Node Features

- A sensor node has:
  - Sensing Material
    - **Physical** – Magnetic, Light, Sound
    - **Chemical** – CO, Chemical Weapons
    - **Biological** – Bacteria, Viruses, Proteins
  - Integrated Circuitry (VLSI)
    - A-to-D converter from analog sensor to circuitry
  - Packaging for environmental safety
  - Power Supply
    - **Passive** – Solar, Vibration
    - **Active** – Battery power, RF Inductance

Advances in Wireless Sensor Nodes

Consider Multiple Generations of Berkeley Motes

Model	Rene	Mica	Mica-2	Mica-Z
Date	1999	2002	2003	2004
CPU	4 MHz	4 MHz	4 MHz	4 MHz
Flash Memory	8 KB	128 KB	128 KB	128 KB
RAM	512 B	4 KB	4 KB	4 KB
Radio	10 Kbps	40 Kbps	76 Kbps	250 Kbps

Historical Comparison

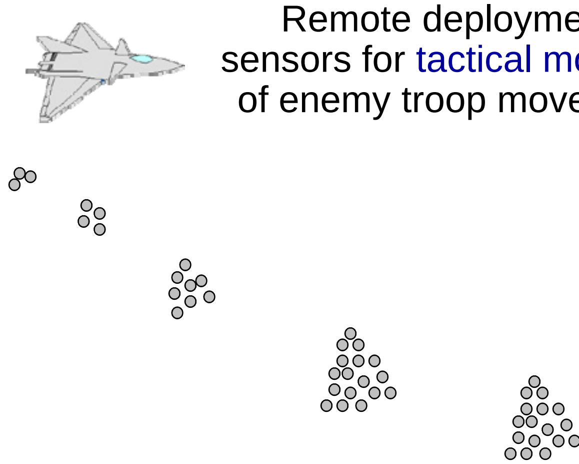
Consider a 40 Year Old Computer

Model	Honeywell H-300	Mica 2
Date	6/1964	7/2003
CPU	2 MHz	4 MHz
Flash Memory	None	128 KB
RAM	32 KB	4 KB

Smart Home / Smart Office

- Sensors controlling appliances and electrical devices in the house.
- Better lighting and heating in office buildings.
- The Pentagon building has used sensors extensively.

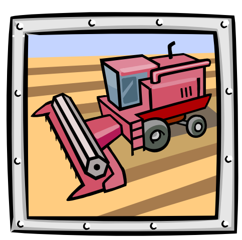
Military



Remote deployment of sensors for tactical monitoring of enemy troop movements.

Industrial & Commercial

- Numerous industrial and commercial applications:
  - Agricultural Crop Conditions
  - Inventory Tracking
  - In-Process Parts Tracking
  - Automated Problem Reporting
  - RFID – Theft Deterrent and Customer Tracing
  - Plant Equipment Maintenance Monitoring



Traffic Management & Monitoring

- Future cars could use wireless sensors to:
  - Handle Accidents
  - Handle Thefts

✓Sensors embedded in the roads to:
- Monitor traffic flows
- Provide real-time route updates

Typical Sensor Network (SN)

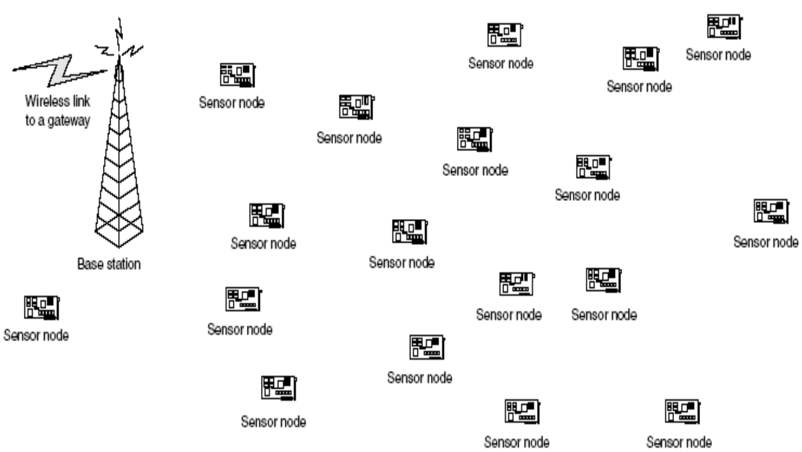


Figure 8.2 Sample wireless sensor network.

Event-driven Responses from SN

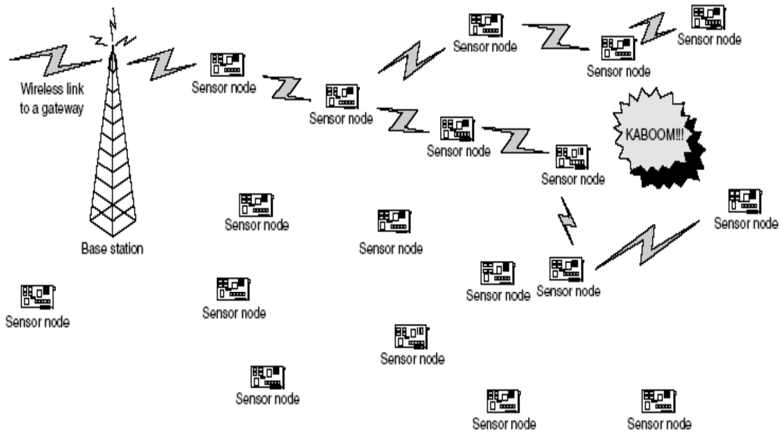


Figure 8.3 (a) Example of an event-driven sensor response.

Periodic Responses from SN

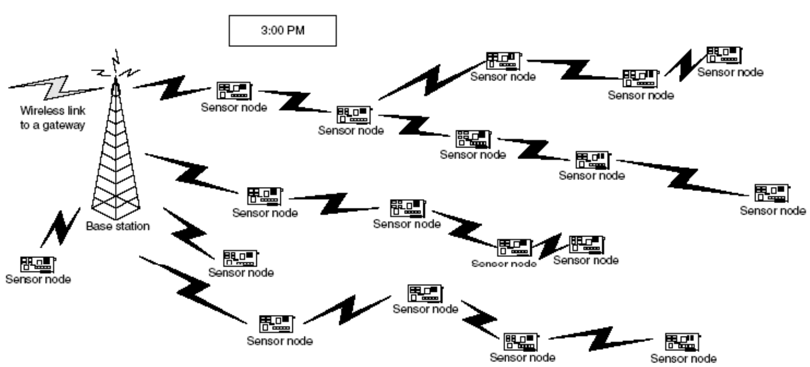


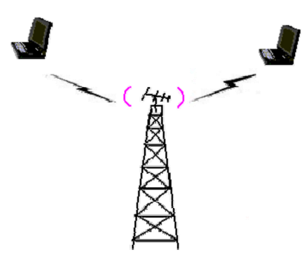
Figure 8.3 (b) Example of a periodic sensor response.

Sensor Network Tasks

- Neighbor discovery
- Self configuration
- Sensing, sensor data processing
- Data aggregation, storage, and caching
- Target detection, target tracking, and target monitoring
- Topology control for energy savings
- Localization
- Time synchronization
- Routing
- Medium access control

Wireless Channel Conditions

- Limitations of wireless channels
  - Noise
  - Interference
  - Link Contention
  - Unidirectional Links



- But inherently a broadcast medium

Constrained Resources

- No centralized authority
- Limited power – prolong life is of primary concern
- Wireless communication: more energy consumed and less reliable
- Limited computation and storage – lack of computation power/space affects the way security protocol is designed and caching/buffering can be performed.
- Limited input and output options – light/speaker only makes diagnosis and performance evaluation difficult

Auto-Configuration

- Autoconfiguration protocols allow sensor nodes to adapt automatically to their environment
- When nodes die or are replaced, manual configuration could be extremely tedious
- Naming…
  - Generation of unique names
- Location determination
  - Direct use of GPS
  - Probes to other GPS-equipped sensor nodes
- Discovery of nearby nodes…
  - e.g., Probe/ACK
- Service discovery…
  - Need lighter-weight protocols
  - Currently, an area for research

Need a Standardized Interface

- Automated interaction between sensors implies some standard mechanism for communication!
  - Requires compatible wireless technology
  - Standardization a common theme
    - TCP/IP for the Internet
    - Java for Internet programming
    - Jini, SLP, etc. for 802.11 wireless devices
- Need a service discovery protocol
  - Enables standard interface among sensors

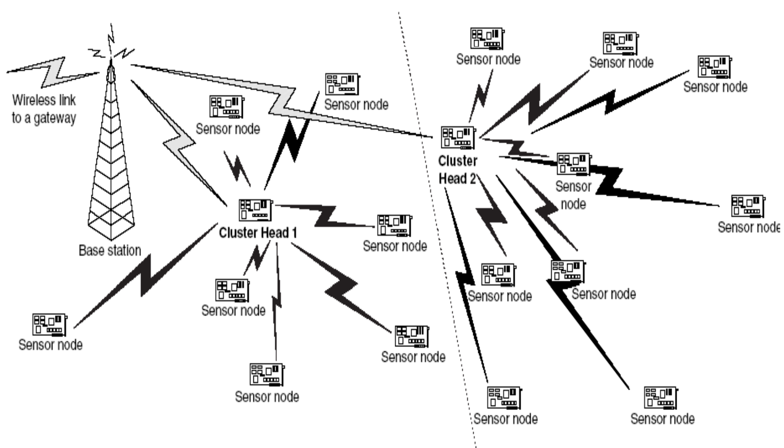
Security Issues

- Concerns about misuse and privacy
  - Privacy issues may slow consumer adoption of technology
    - User tracking – RFID concerns
  - Authentication and privacy are not always complementary objectives
  - Do not want your medical sensor hacked!!
  - Data tampering and computer viruses could be a nightmare!

Security Issues

- Storing large keys is not practical but smaller keys reduce the security
- More complicated algorithms increase security but drain energy
- Sharing security keys between neighbors with changing membership (due to node failure or addition) needs a scaleable key distribution and key management scheme that is resilient to adversary attacks
- Challenge is to provide security that meets the application security requirements while conserve energy

Clustering to Save Resources



Clustering

- Divide the network into a number of equal clusters each ideally containing the same # of nodes
- Cluster heads form a routing backbone
- Clustering is NP-complete
- Mobility may make a good clustering become bad later
- Data aggregation: Combining cluster data readings into a single packet can save energy

Multihop Routing vs. Energy

- Multihop routing often reduces energy consumption (because energy used is roughly proportional to square of distance) but introduces delay
- Energy consumption in transmitting a packet:
  - A constant cost for powering up the transmitter circuitry
  - Proportional to packet size
  - Proportional to square of distance
- How long should per-hop distance be?
  - If per-hop distance is too short, then
    - the constant cost of powering up the transmitter circuitry dominates
  - If per-hop distance is too long, then
    - Cost of packet transmission dominates
    - spatial reuse of bandwidth reduces
    - the number of neighbors within a hop increases for increased overhead for state information maintenance and scheduling overhead

LEACH Clustering (1)

- LEACH rotates cluster heads to balance energy consumption
- Each cluster head performs its duty for a period of time
- Each sensor makes an independent decision (e.g., 5% of becoming the cluster head) on whether to become a cluster head and if yes broadcasts advertisement packets
- Every node generates a random number (***R***) and computes a threshold T = P/(1-P*(r mod(1/P))) if it has not been a cluster head in the last 1/P rounds
  - P: desired percentage of cluster heads (e.g. 5%)
  - r: the current round
  - It elects itself as a cluster head if ***R < T***

LEACH Clustering (2)

- Each sensor that is not a cluster head listens to advertisements and selects the closest cluster head
- Once a cluster head knows the membership, a schedule is created for the transmission from sensors in the cluster to the cluster head to avoid collision (e.g., based on TDMA)
- The cluster head can send a single packet to the base station (directly) over long distance to save energy consumption
- No assurance of optimal cluster distributions

HEED Clustering

- HEED uses the residual energy info for cluster head election to prolong sensor network lifetime
- Probability of a sensor becoming a cluster head is:

$$CH_{prob} = C_{prob} \times \frac{E_{residual}}{E_{max}},$$

e.g., 5%

- Clusters are elected in iterations:
  - A sensor announces its intention to become a cluster head, along with a cost measure indicating communication cost if it were elected a cluster head
  - A non-CH sensor picks a candidate with the lowest cost
  - A non-CH sensor not covered doubles its CH_{prob} in iterations until CH_{prob} is 1, in which case the sensor elects itself to the cluster head

HEED Clustering - Protocol

```
I. Initialize
S_nbr ← {v: v lies within my cluster range}
Compute and broadcast cost to ∈ S_nbr
CH_prob ← max(C_prob × E_residual/E_max, p_min)
is_final_CH ← FALSE

II. Main Processing
Repeat
If ((S_CH ← {v: v is a cluster head}) ≠ φ)
  my_cluster_head ← least_cost(S_CH)
  If (my_cluster_head = NodeID)
    If (CH_prob = 1)
      Cluster_head_msg(NodeID,final_CH,cost)
      is_final_CH ← TRUE
    Else
      Cluster_head_msg(NodeID, tentative_CH,cost)
ElseIf (CH_prob = 1)
  Cluster_head_msg(NodeID,final_CH,cost)
  is_final_CH ← TRUE
ElseIf Random(0,1) ≤ CH_prob
  Cluster_head_msg(NodeID,tentative_CH,cost)
CH_previous ← CH_prob
CH_prob ← min(CH_prob × 2, 1)
Until CH_previous = 1

III. Finalize
If (is_final_CH = FALSE)
  If ((S_CH ← {v: v is a final cluster head}) ≠ φ)
    my_cluster_head ← least_cost(S_CH)
    join_cluster(cluster_head_ID, NodeID)
  Else Cluster_head_msg(NodeID, final_CH, cost)
Else Cluster_head_msg(NodeID, final_CH, cost)
```

PEGASIS

- A chain of sensors is formed for data transmission (could be formulated by base station)
- Finding the optimal chain is NP-complete
- Sensor readings are aggregated hop by hop until a single packet is delivered to the base station: effectively when aggregation is possible
- Advantages: No long-distance data transmission; no overhead of maintaining cluster heads
- Disadvantages:
  - Significant delay: Can use tree instead
  - Disproportionate energy depletion (for sensors near the base station): Can rotate parent nodes in the tree

Aggregation/Duplicate Suppression

- Another attempt to save resources
- Sensor nodes whose values match those of other sensor nodes, on forwarding messages, can simply annotate the message
- Or just remain silent, on overhearing identical (or “similar enough”) values

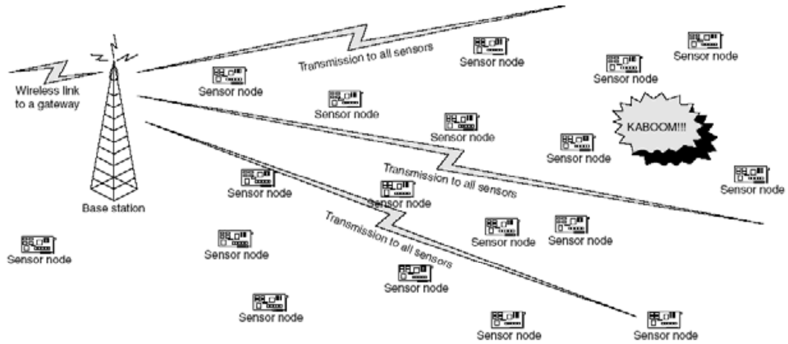
Asking a Sensor Network a Question (Querying)

- Can have sensor nodes periodically transmit sensor readings
- More likely: Ask the sensor network a question and receive an answer
- Issue: Getting the request out to the nodes
- Issue: Getting responses back from sensor nodes who have answers
- Routing:
  - Directed Diffusion Routing
  - Geographic Forwarding (related to geocasting)

Query-Oriented Routing

- For query-oriented routing: Queries are disseminated from the base station to the sensor nodes
- Sensor readings are sent by sensors to the base station in a reverse flooding order
- Sensor nodes that receive multiple copies of the same message suppress forwarding

Query: Asking a Question



Response to Base Station: Initial

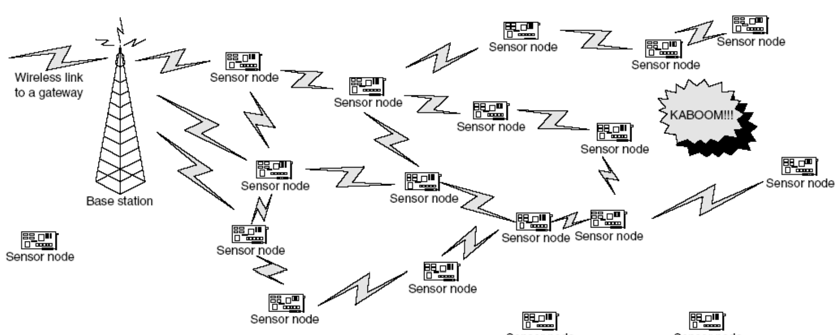


Figure 11.4 Initial processing of an event-driven query.

Directed Diffusion Routing

- Direction: From source (sensors) to sink (base station)
- Positive/negative feedback is used to encourage/discourage sensor nodes for forwarding messages toward the base station
  - Feedback can be based on delay in receiving data
  - Positive is sent to the first and negative is sent to others
- A node sends with low frequency unless it receives positive feedback
- This feedback propagates throughout the sensor network to suppress multiple transmissions
- Eventually message forwarding converges to the use of a single path with data aggregation (for energy saving) from the source to the base station

Responses, After Some Guidance

Neighboring nodes, upon receiving duplicate messages, can provide some guidance to allow responses to be more efficiently delivered in the future…

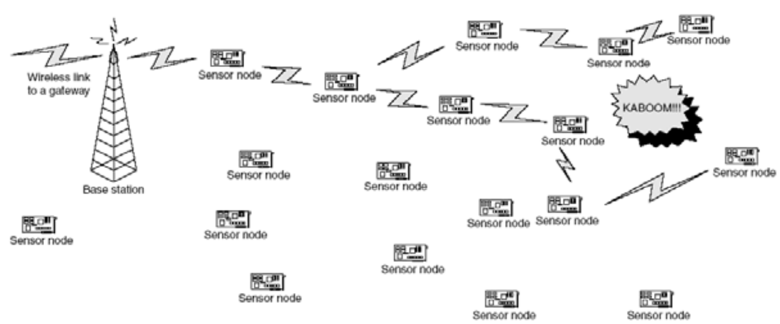


Figure 11.5 Directed diffusion routing paths after redundant path suppression.

Directional Routing (Geographical Forwarding)

- For dense sensor networks such that a sensor is available in the direction of routing
- Location of destination is sufficient to determine the routing orientation
- Research issue:
  - selecting paths with a long lifetime for delivering messages between sensors, and from sensors to a base station
  - Determining paths that avoid “holes” – determining the boundary or perimeter of a hole through local information exchanges periodically to trade energy consumption (for hole detection) vs. routing efficiency

Geographic Forwarding

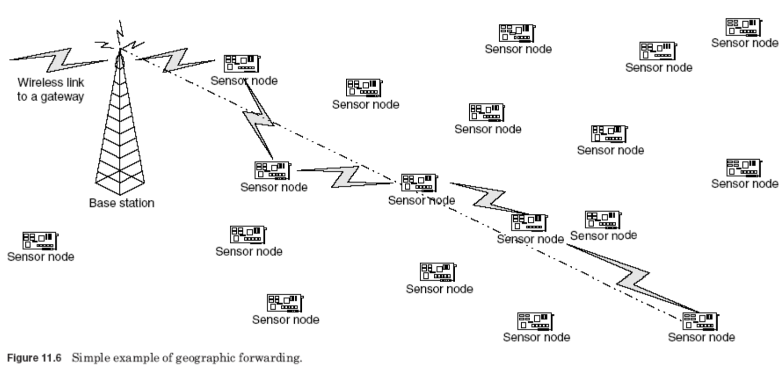


Figure 11.6 Simple example of geographic forwarding.

References

Chapters 8-11, F. Adelstein, S.K.S. Gupta, G.G. Richard III and L. Schwiebert, *Fundamentals of Mobile and Pervasive Computing*, McGraw Hill, 2005.

Other References:

9. **Y.C. Hu and D.B. Johnson, "Implicit source routes for on-demand ad hoc network routing," *2nd ACM International Symposium on Mobile Ad Hoc Networking & Computing*, Long Beach, CA, USA, 2001.**
10. **Y. Ko and N. Vaidya, "Geocasting in Mobile Ad hoc Networks: Location-Based Multicast Algorithms," *Second IEEE Workshop on Mobile Computer Systems and Applications, New Orleans,* Louisiana, USA, February 1999.**