Mobile Ad Hoc Networking

Carlos Cordeiro & Dharma Agrawal
OBR Research Center for Distributed and Mobile Computing
University of Cincinnati – USA

http://www.ececs.uc.edu/~cordeicm
cordeicm@ececs.uc.edu

Acknowledgments

- Some figures and slides were taken from Nitin Vaidya's MobiCom'2000 tutorial

Course Outline

- Introduction
- Unicast routing
- Multicast routing
- Medium Access Control
- Sensor Networks
- Standards activities
- Open problems

3

Notes

- Only most important features of various schemes are typically discussed
  - The concepts covered here enable you to understand any protocol
- Most schemes include many more details, and optimizations
  - Course handout has most details and references

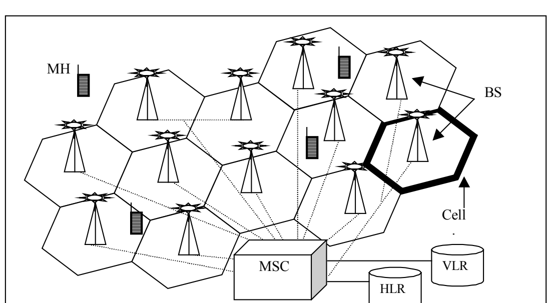
4

Mobile Ad Hoc Networks (MANET)

Introduction and Generalities

Traditional Cellular Network

- Single hop wireless connectivity to the wired world
  - Space divided into cells, where a base station is responsible to communicate with hosts in its cell
  - Mobile hosts can change cells while communicating
  - Hand-off occurs when a mobile host starts communicating via a new base station



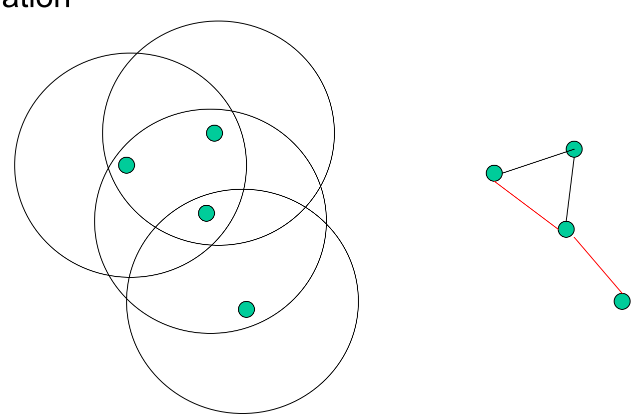
Mobile Ad hoc NETworks (MANET)

- Formed by wireless hosts which may be mobile
- Without (necessarily) using a pre-existing infrastructure
- Routes between nodes may potentially contain multiple hops

7

Mobile Ad hoc NETworks (MANET)

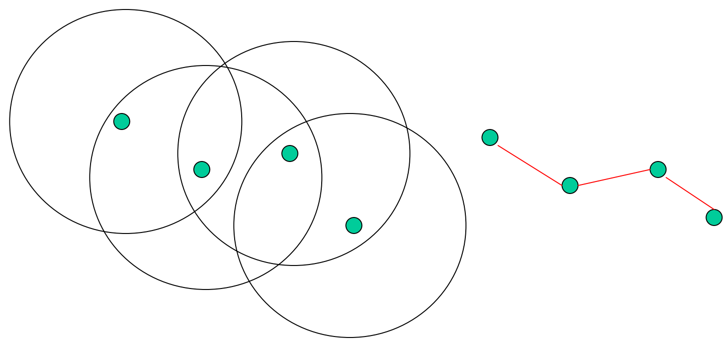
- May need to traverse multiple links to reach a destination



8

Mobile Ad hoc NETworks (MANET)

- Mobility causes route changes



9

Why Ad Hoc Networks ?

- Setting up of fixed access points and backbone infrastructure is not always viable
  - Infrastructure may not be present in a disaster area or war zone
  - Infrastructure may not be practical for short-range radios; Bluetooth (range ~ 10m)

- Ad hoc networks:
  - Do not need backbone infrastructure support
  - Are easy to deploy
  - Useful when infrastructure is absent, destroyed or impractical

10

Many Applications

- Personal area networking (PAN)
  - cell phone, laptop, ear phone, wrist watch
- Military environments
  - soldiers, tanks, planes
- Civilian environments
  - taxi cab network
  - meeting rooms
  - sports stadiums
  - boats, small aircraft
- Emergency operations
  - search-and-rescue
  - policing and fire fighting

Challenges in Mobile Environments

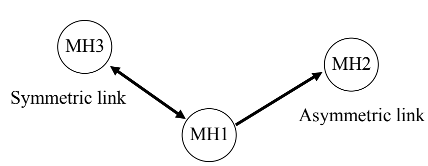
- Limitations of the Wireless Network
  - packet loss due to transmission errors
  - variable capacity links
  - frequent disconnections/partitions
  - limited communication bandwidth
  - broadcast nature of the communications
- Limitations Imposed by Mobility
  - dynamically changing topologies/routes
  - lack of mobility awareness by system/applications
- Limitations of the Mobile Computer
  - short battery lifetime
  - limited capacities

Effect of Mobility on the Protocol Stack

- Application
  - new applications and adaptations
- Transport
  - congestion and flow control
- Network
  - addressing and routing
- Link
  - media access and handoff
- Physical
  - transmission errors and interference

Assumption

- Unless stated otherwise, fully symmetric (bi-directional) environment is assumed implicitly



Routing in MANET

Routing Protocols

- Proactive (Table-driven) protocols
  - Traditional distributed shortest-path protocols
  - Maintain routes between every host pair at all times
  - Based on periodic updates; High routing overhead
  - Example: DSDV (destination sequenced distance vector)
- Reactive (On-Demand) protocols
  - Determine route if and when needed
  - Source initiates route discovery
  - Example: DSR (dynamic source routing)
- Hybrid protocols
  - Adaptive; Combination of proactive and reactive
  - Example : ZRP (zone routing protocol)

Protocol Trade-offs

- Proactive protocols
  - Always maintain routes
  - Little or no delay for route determination
  - Consume bandwidth to keep routes up-to-date
  - Maintain routes which may never be used
- Reactive protocols
  - Lower overhead since routes are determined on demand
  - Significant delay in route determination
  - Employ flooding (global search)
  - Control traffic may be bursty
- Which approach achieves a better trade-off depends on the traffic and mobility patterns

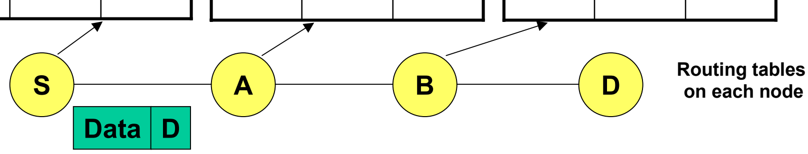
17

Hop-by-Hop Routing

Dest.	Next Hop	#Hops
D	A	3

Dest.	Next Hop	#Hops
D	B	2

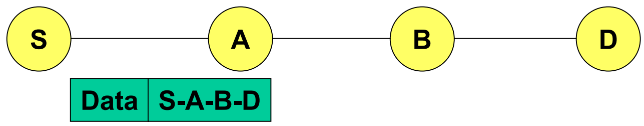
Dest.	Next Hop	#Hops
D	D	1



- Routing table on each node = Hop-by-hop routing
- Data packet has only the destination address

18

Source Routing



- In source routing, the data packet has the complete route (called source route) in the header
- Typically, the source node builds the whole route
- The data packet routes itself

19

Unicast Routing

in

Mobile Ad Hoc Networks

20

Reactive (On-Demand) Routing Protocols

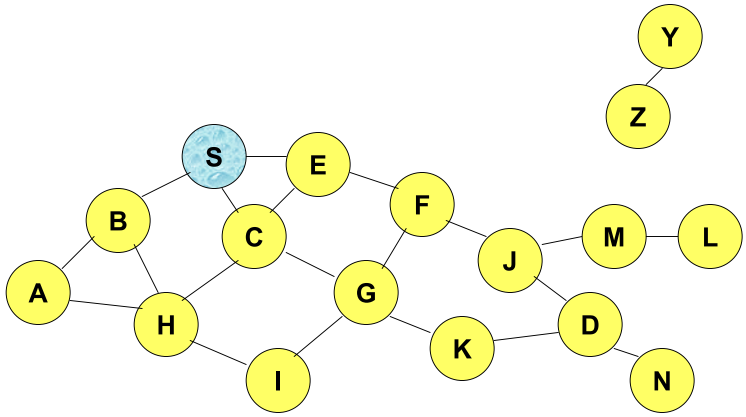
21

Dynamic Source Routing (DSR) [Johnson96]

- 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
- Source node S floods Route Request (RREQ)
- Each node *appends own identifier* when forwarding RREQ

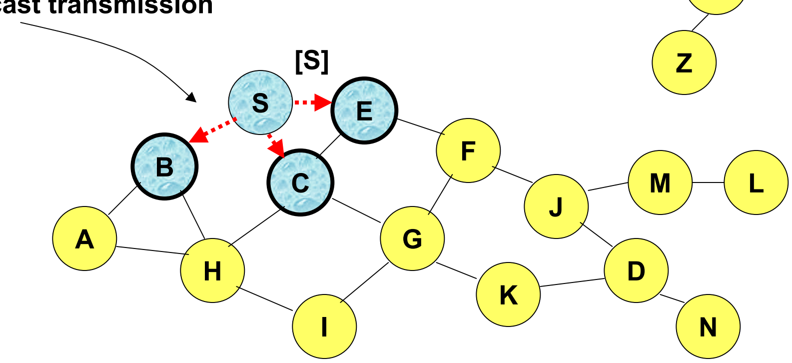
22

Route Discovery in DSR



Represents a node that has received RREQ for D from S

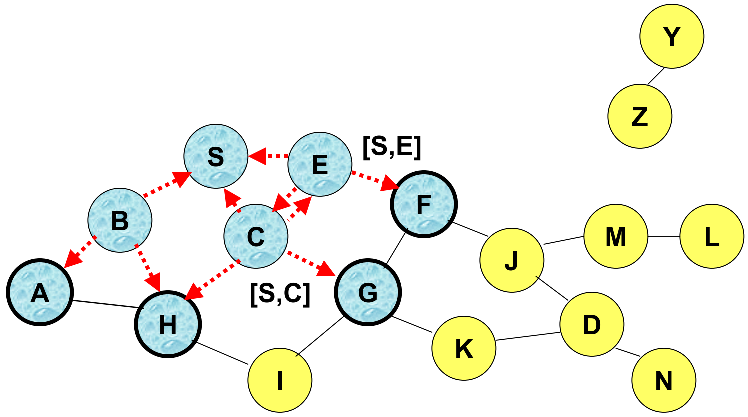
Route Discovery in DSR



Represents transmission of RREQ

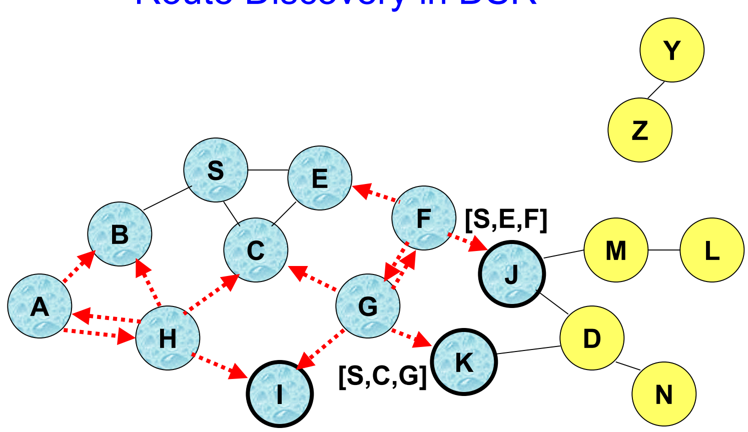
[X,Y] Represents list of identifiers appended to RREQ

Route Discovery in DSR



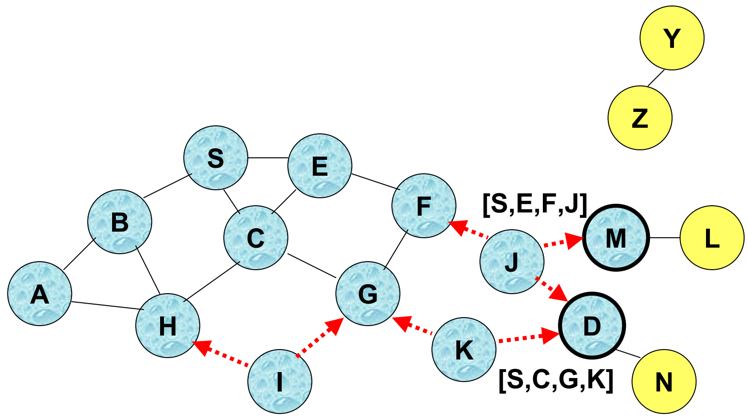
• Node H receives packet RREQ from two neighbors: **potential for collision**

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

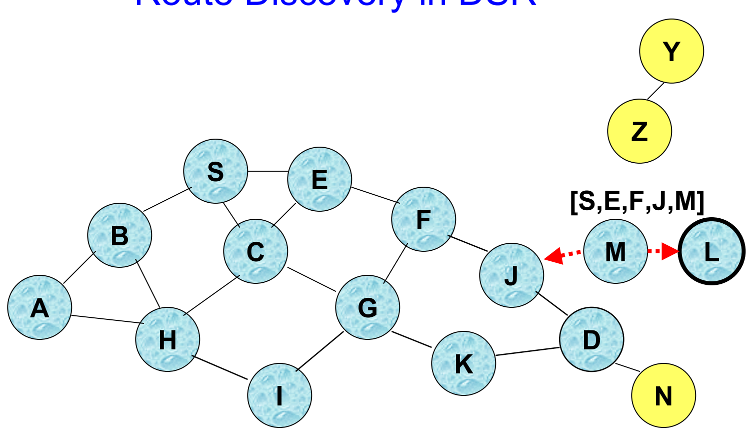
Route Discovery in DSR



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

27

Route Discovery in DSR



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

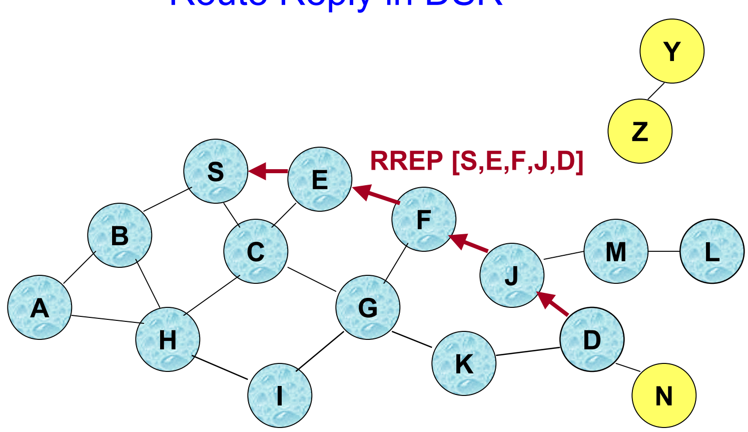
28

Route Discovery 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

29

Route Reply in DSR



Represents RREP control message

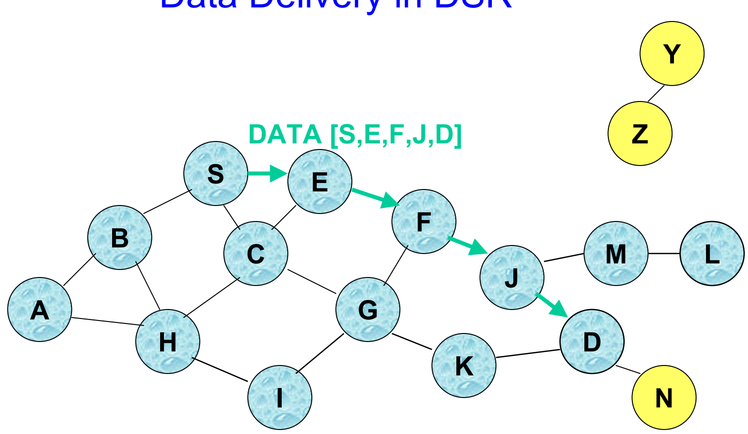
30

Dynamic Source Routing (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

31

Data Delivery in DSR



Packet header size grows with route length

32

DSR Optimization: Route Caching

- Each node caches a new route it learns by *any means*
- 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 [S,C,G] destined for node D, node K learns route [K,G,C,S] to node S
- When node F forwards Route Reply RREP [S,E,F,J,D], node F learns route [F,J,D] to node D
- When node E forwards Data [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
- Problem: Stale caches may increase overheads

Dynamic Source Routing: 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

UNIVERSITY OF Cincinnati

Dynamic Source Routing: Disadvantages

DMC

- Packet header size grows with route length due to source routing
- Flood of route requests may potentially reach all nodes in the network
- Potential 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
- Stale caches will lead to increased overhead

35

UNIVERSITY OF Cincinnati

Ad Hoc On-Demand Distance Vector Routing (AODV) [Perkins99Wmcsa]

DMC

- DSR includes source routes in packet headers
- Resulting large headers can sometimes degrade performance
  - particularly when data contents of a packet are small
- AODV attempts to improve on DSR by maintaining routing tables at the nodes, so that data packets do not have to contain routes
- AODV retains the desirable feature of DSR that routes are maintained only between nodes which need to communicate

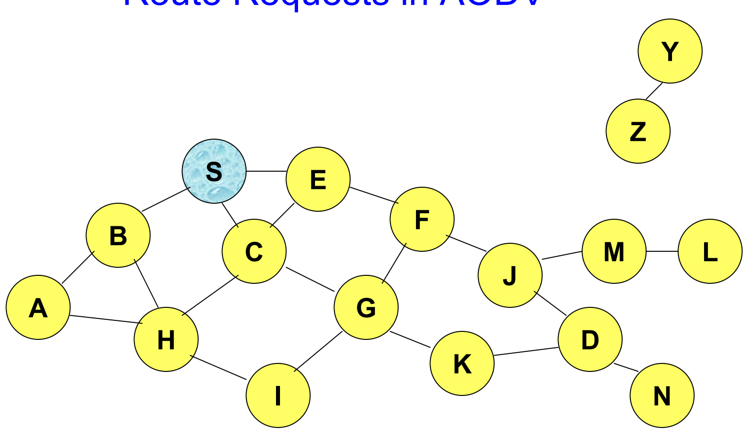
36

AODV

- Route Requests (RREQ) are forwarded in a manner similar to DSR
- When a node re-broadcasts a Route Request, it sets up a reverse path pointing towards the source
  - AODV assumes symmetric (bi-directional) links
- When the intended destination receives a Route Request, it replies by sending a Route Reply
- Route Reply travels along the reverse path set-up when Route Request is forwarded

37

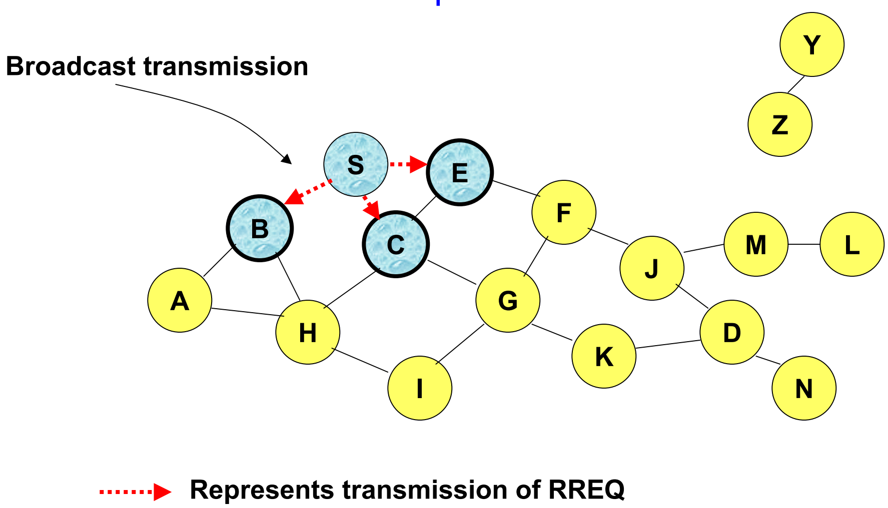
Route Requests in AODV



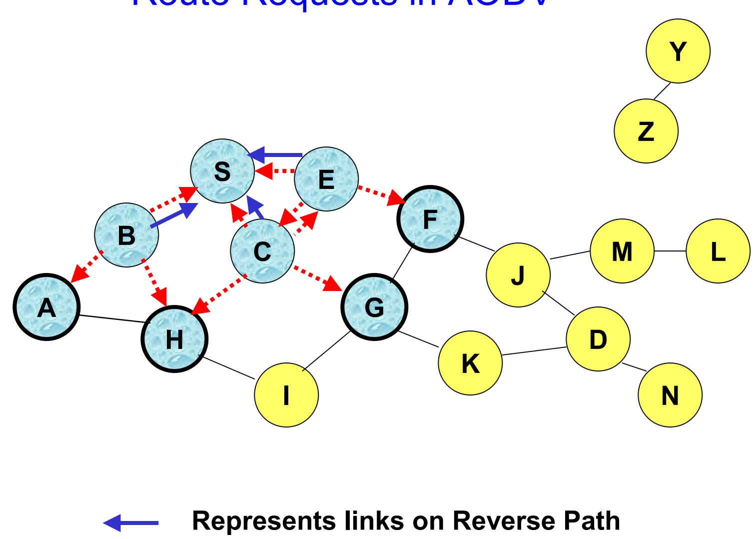
Represents a node that has received RREQ for D from S

38

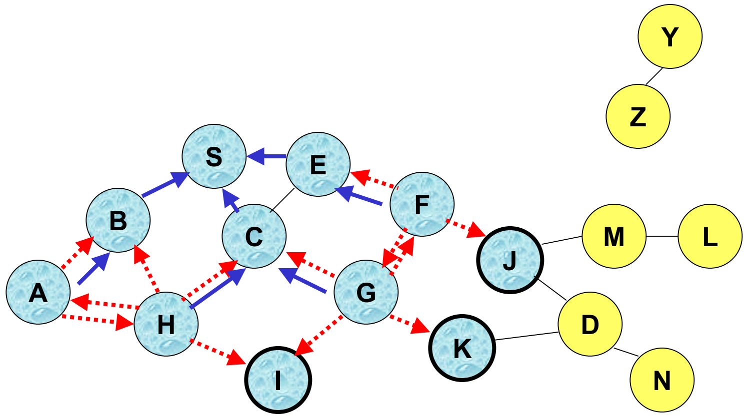
Route Requests in AODV



Route Requests in AODV

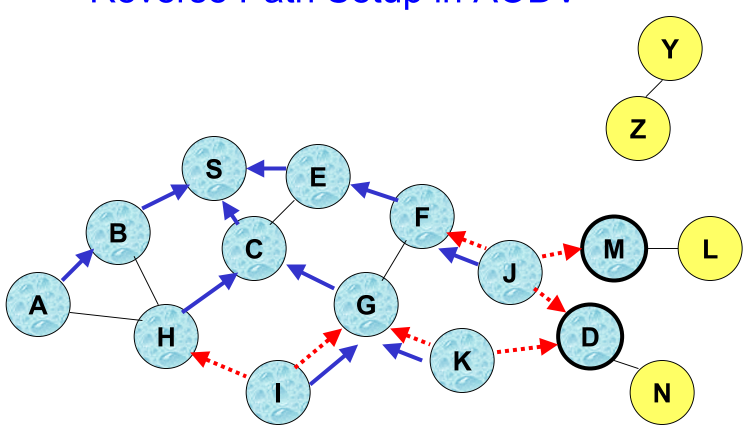


Reverse Path Setup in AODV

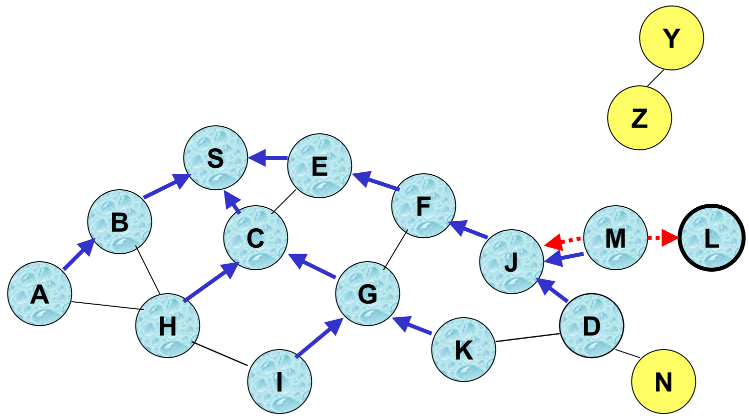


- Node C receives RREQ from G and H, but does not forward it again, because node C has already forwarded RREQ once

Reverse Path Setup in AODV

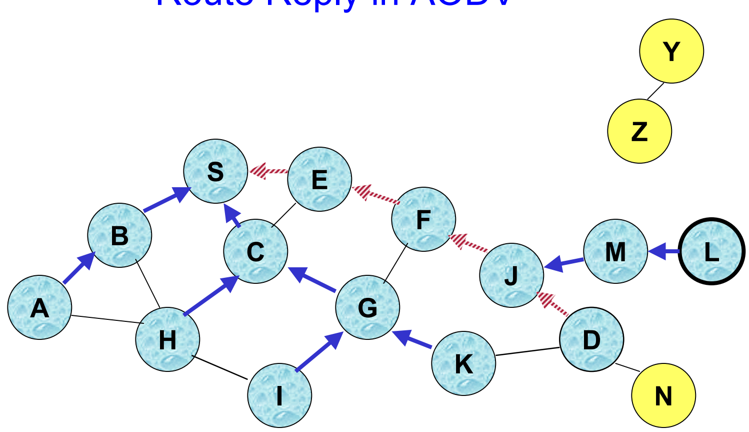


Reverse Path Setup in AODV



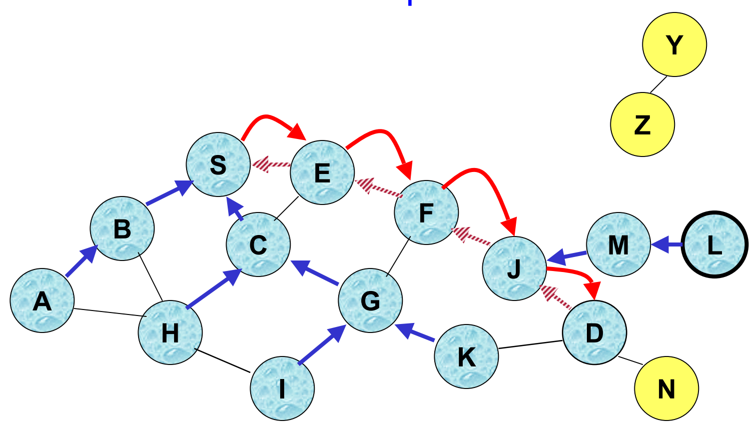
- Node D does not forward RREQ, because node D is the intended target of the RREQ

Route Reply in AODV



Represents links on path taken by RREP

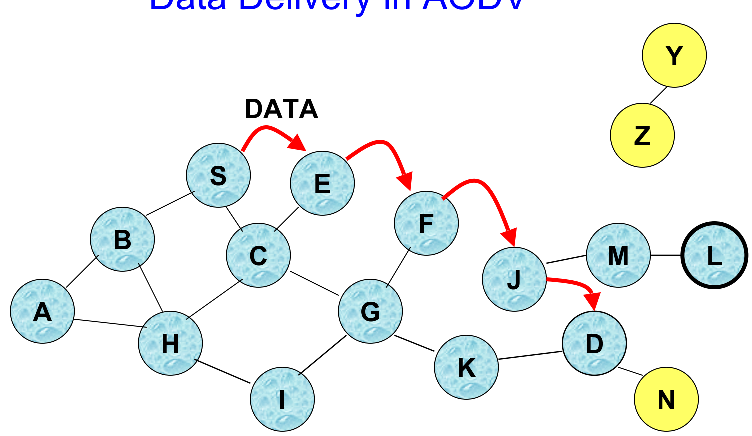
Forward Path Setup in AODV



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.

Timeouts

- A routing table entry maintaining a reverse path is purged after a timeout interval
  - timeout should be long enough to allow RREP to come back
- A routing table entry maintaining a forward path is purged if *not used* for a *active_route_timeout* interval
  - if no is data being sent using a particular routing table entry, that entry will be deleted from the routing table (even if the route may actually still be valid)

47

Link Failure Detection

- *Hello* messages: Neighboring nodes periodically exchange hello message
- Absence of hello message is used as an indication of link failure
  - When node X is unable to forward packet P (from node S to node D) on link (X,Y), it generates a RERR message
- Alternatively, failure to receive several MAC-level acknowledgement may be used as an indication of link failure

48

Summary: AODV

- Routes need not be included in packet headers
- Nodes maintain routing tables containing entries only for routes that are in active use
- At most one next-hop per destination maintained at each node
  - DSR may maintain several routes for a single destination

Flooding of Control Packets

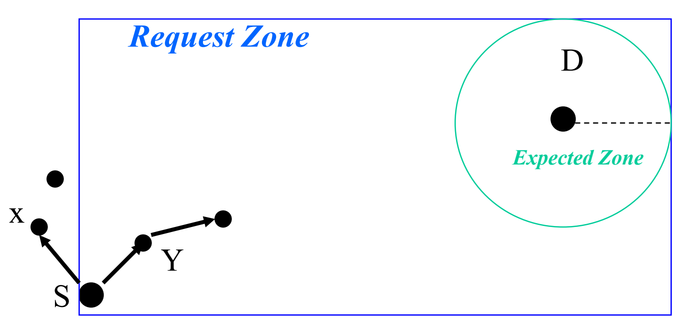
- How to reduce the scope of the route request flood ?
  - LAR [Ko98Mobicom]
  - Query localization [Castaneda99Mobicom]
- How to reduce redundant broadcasts ?
  - The Broadcast Storm Problem [Ni99Mobicom]
  - More to come in subsequent slides …

Location-Aided Routing (LAR) [Ko98Mobicom]

- 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

Request Zone

- Define a Request Zone
- LAR is same as flooding, except that only nodes in request zone forward route request
- Smallest rectangle including S and expected zone for D



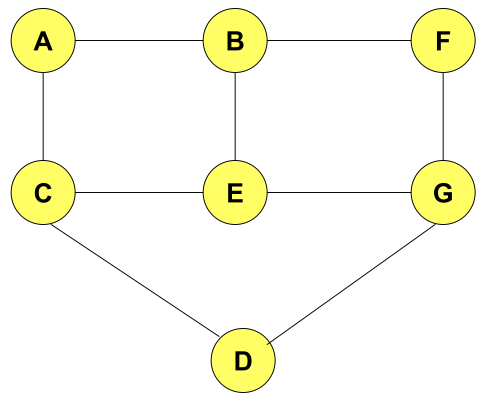
Location Aided Routing (LAR)

- Advantages
  - reduces the scope of route request flood
  - reduces overhead of route discovery
- Disadvantages
  - Nodes need to know their physical locations
  - Does not take into account possible existence of obstructions for radio transmissions

So far ...

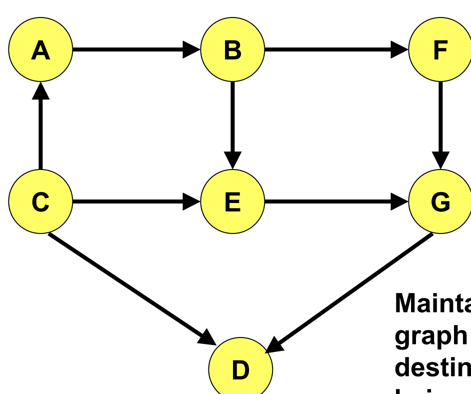
- All protocols discussed so far perform some form of flooding
- Now we will consider protocols which try to reduce/avoid such behavior

Link Reversal Algorithm [Gafni81]



55

Link Reversal Algorithm



Links are bi-directional

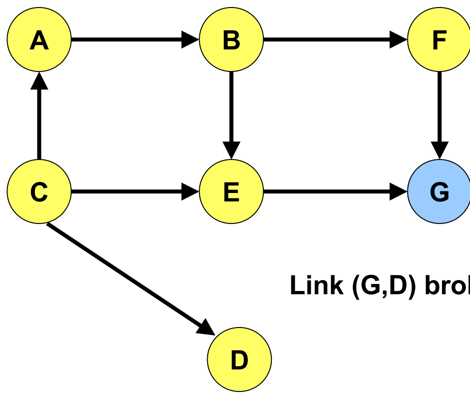
But algorithm imposes logical directions on them

Maintain a directed acyclic graph (DAG) for each destination, with the destination being the *only sink*

This DAG is for *destination node D*

56

Link Reversal Algorithm

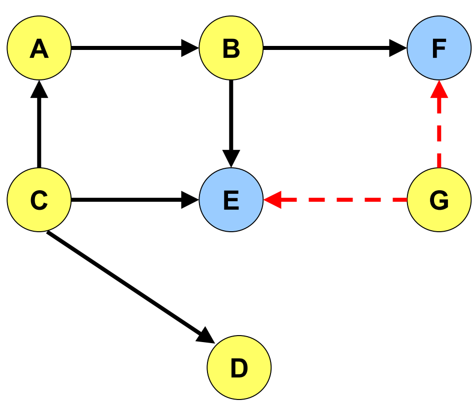


Link (G,D) broke

Any node, other than the destination, that has no outgoing links reverses all its incoming links.

Node G has no outgoing links

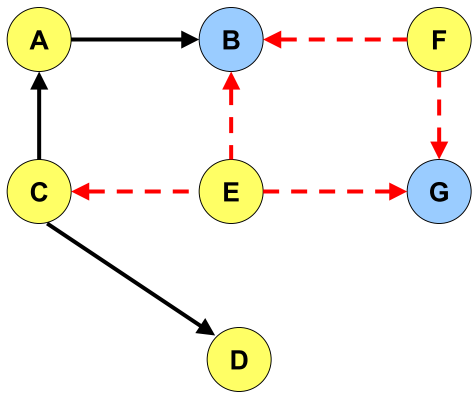
Link Reversal Algorithm



Represents a link that was reversed recently

Now nodes E and F have no outgoing links

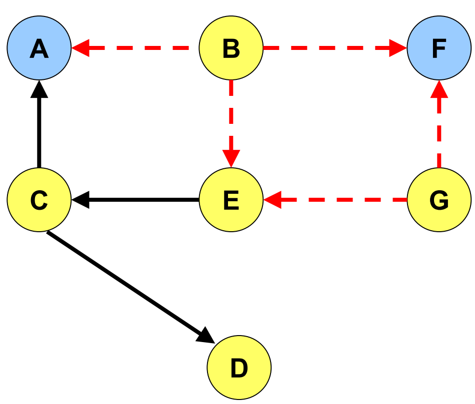
Link Reversal Algorithm



Represents a link that was reversed recently

Now nodes B and G have no outgoing links

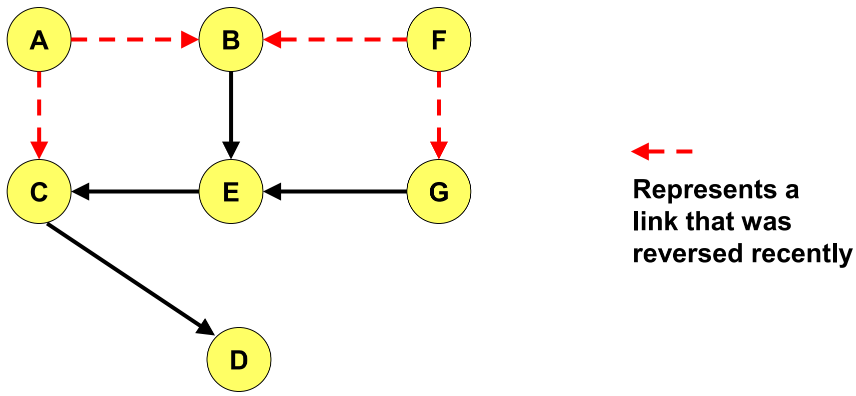
Link Reversal Algorithm



Represents a link that was reversed recently

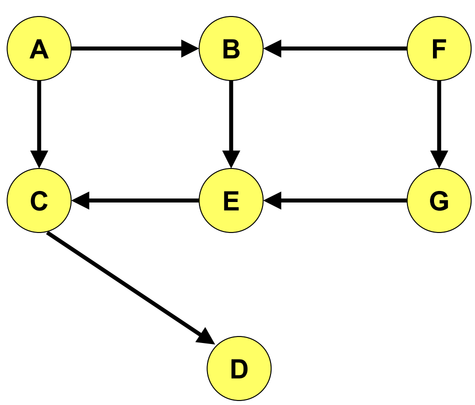
Now nodes A and F have no outgoing links

Link Reversal Algorithm



Now all nodes (other than destination D) have an outgoing link

Link Reversal Algorithm



DAG has been restored with only the destination as a sink

Link Reversal Algorithm

- Attempts to keep link reversals local to where the failure occurred
  - But this is not guaranteed
- When the first packet is sent to a destination, the destination oriented DAG is constructed
- The initial construction does result in flooding of control packets

63

Link Reversal Algorithm

- The previous algorithm is called a full reversal method since when a node reverses links, it reverses *all* its incoming links
- Partial reversal method [Gafni81]: A node reverses incoming links from only those neighbors who have not themselves reversed links "previously"
  - If all neighbors have reversed links, then the node reverses all its incoming links
  - "Previously" at node X means *since the last link reversal done by node X*

64

Link Reversal Methods

- Advantages
  - Link reversal methods attempt to limit updates to routing tables at nodes in the vicinity of a broken link
    - Partial reversal method tends to be better than full reversal method
  - Each node may potentially have multiple routes to a destination (multipath)

- Disadvantages
  - Need a mechanism to detect link failure
    - hello messages may be used
  - If network is partitioned, link reversals continue indefinitely

Temporally-Ordered Routing Algorithm (TORA) [Park97Infocom]

- Route optimality is considered of secondary importance; longer routes may be used

- At each node, a logically separate copy of TORA is run for each destination, that computes the height of the node with respect to the destination
  - Height captures number of hops and next hop
- Route discovery is by using query and update packets

- TORA modifies the partial link reversal method to be able to detect partitions
- When a partition is detected, all nodes in the partition are informed, and link reversals in that partition cease

Other Protocols

- Many variations of using control packet flooding for route discovery
- Power-Aware Routing [Singh98Mobicom]
  - Assign a weight to each link: function of energy consumed when transmitting a packet on that link, as well as the residual energy level
  - Modify DSR to incorporate weights and prefer a route with the smallest aggregate weight
- Associativity-Based Routing (ABR) [Toh97]
  - Only links that have been stable for some minimum duration are utilized
  - Nodes increment the associativity ticks of neighbors by using periodic beacons
- Signal Stability Based Adaptive Routing (SSA) [Dube97]
  - A node X re-broadcasts a Route Request received from Y only if the (X,Y) link has a *strong signal stability*
  - Signal stability is evaluated as a moving average of the signal strength of packets received on the link in recent past

Proactive (Table-driven) Routing Protocols

Broad Classification of Proactive Protocols

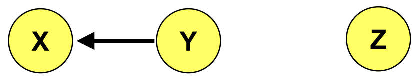
- Distance-Vector based
  - DSDV (Destination-Sequenced Distance-Vector)
- Link-State based
  - TBRPF (Topology Broadcast with Reverse Path Forwarding)
  - OLSR (Optimized Link-State Routing)

Destination-Sequenced Distance-Vector (DSDV) [Perkins94Sigcomm]

- 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 (indicate freshness of routes)
- 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

Destination-Sequenced Distance-Vector (DSDV)

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

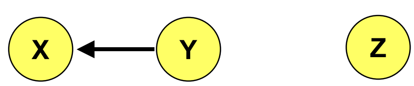


- Let S(X) and S(Y) denote the destination sequence number for node Z as stored at node X, and as sent by node Y with its routing table to node X, respectively

71

Destination-Sequenced Distance-Vector (DSDV)

- Node X takes the following steps:

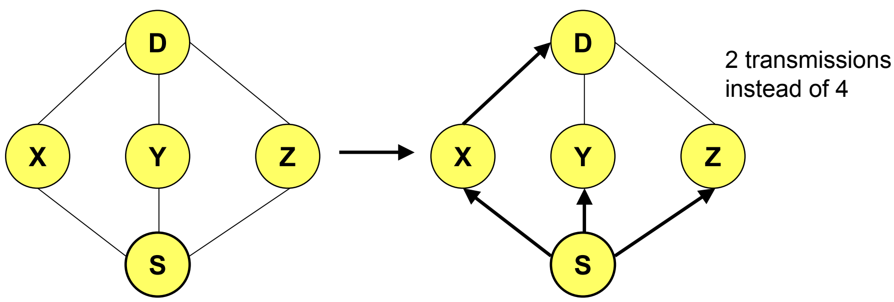


  - If S(X) > S(Y), then X ignores the routing information received from Y
  - If S(X) = S(Y), and cost of going through Y is smaller than the route known to X, then X sets Y as the next hop to Z
  - If S(X) < S(Y), then X sets Y as the next hop to Z, and S(X) is updated to equal S(Y)

72

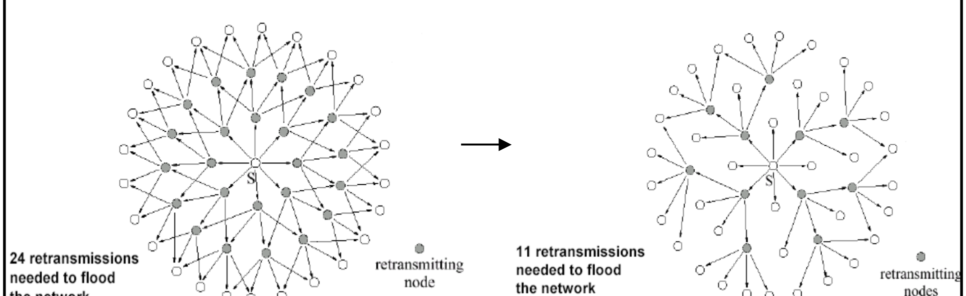
TBRPF (Topology Broadcast with Reverse Path Forwarding) [Bellur99Infocom]

- Send link-state updates only via the minimum-hop spanning tree rooted at the source of the update
- Little cost in maintaining the spanning tree
  - The network connectivity information is available



OLSR (Optimized Link-State Routing) [Clausen01Inmic]

- Only multipoint relays (MPR) participate in the routing
- Each node maintains information about its MPR
- OLSR floods link-state information only through MPRs



Hybrid Routing Protocols

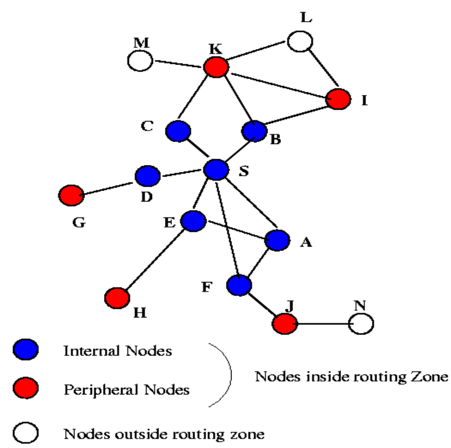
75

Zone Routing Protocol (ZRP) [Haas98]

- ZRP combines proactive and reactive approaches
  - More like a framework
- 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
- Intra-zone routing: Proactively maintain routes to all nodes within the source node's own zone.
- Inter-zone routing: Use an on-demand protocol (similar to DSR or AODV) to determine routes to outside zone.

76

Zone Routing Protocol (ZRP)



Radius of routing zone = 2

77

Routing Summary

- Protocols
  - Typically divided into proactive, reactive and hybrid
  - Geographic forwarding (does not really perform routing)
- Performance Studies
  - Typically studied by simulations using NS, discrete event simulator
  - Nodes (10-200) remains stationary for pause time seconds (0-900s) and then move to a random destination (1500m X 300m space) at a uniform speed (0-20m/s). CBR traffic sources (4-30 packets/sec, 64-1024 bytes/packet)
  - Attempt to estimate latency of route discovery, routing overhead …
- Actual trade-off depends a lot on traffic and mobility patterns
  - Higher traffic diversity (more source-destination pairs) increases overhead in on-demand protocols
  - Higher mobility will always increase overhead in all protocols

78

Other Routing Protocols

- Plenty of other routing protocols
- Discussion here is far from exhaustive
- Course handout contains descriptions (references) of some other protocols

Multicast Routing
in
Mobile Ad Hoc Networks

Multicasting

- A multicast group is defined with a unique *group identifier*
- Nodes may join or leave the multicast group anytime
- In traditional networks, the physical network topology does not change often
- In MANET, the physical topology can change often

Multicasting in MANET

- Need to take topology change into account when designing a multicast protocol
- Several new protocols have been proposed for multicasting in MANET
  - AODV Multicast
  - ODMRP
  - Flooding, AMRoute, CAMP, AMRIS, …

AODV Multicasting [Royer00Mobicom]

- Each multicast group has a group leader
- Group leader is responsible for maintaining group sequence number (which is used to ensure freshness of routing information)
  - Similar to sequence numbers for AODV unicast
- First node joining a group becomes *group leader*
- A node on becoming a group leader, broadcasts a *Group Hello* message

83

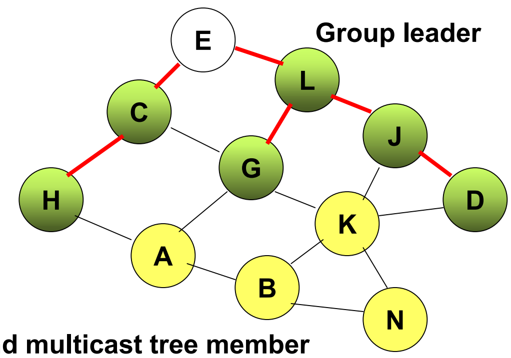
AODV Group Sequence Number

- In our illustrations, we will ignore the group sequence numbers
- However, note that a node makes use of information received only with *recent enough* sequence number

84

AODV Multicast Tree

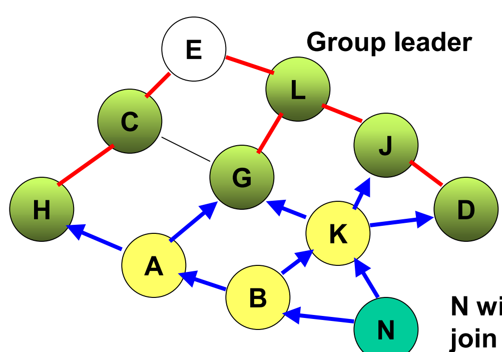
Multicast tree links



Group and multicast tree member

Tree (but not group) member

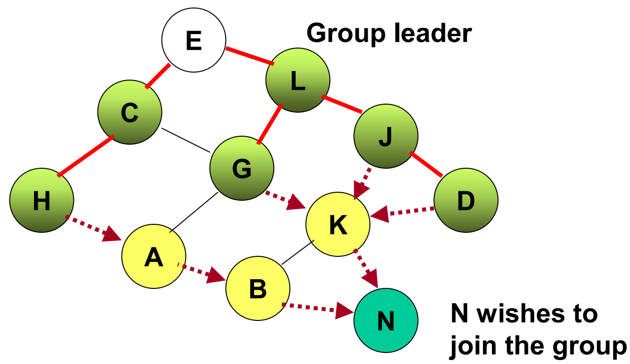
Joining the Multicast Tree: AODV



N wishes to join the group: it floods RREQ

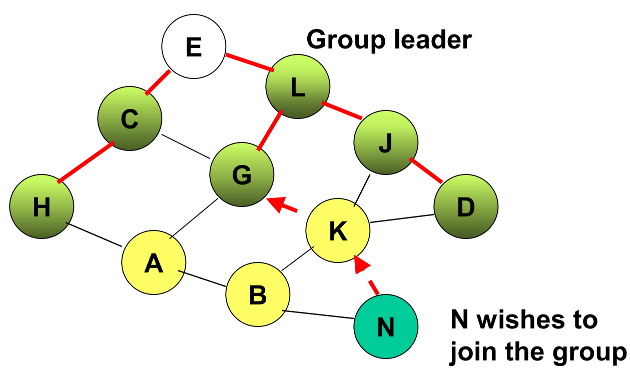
Route Request (RREQ)

Joining the Multicast Tree: AODV



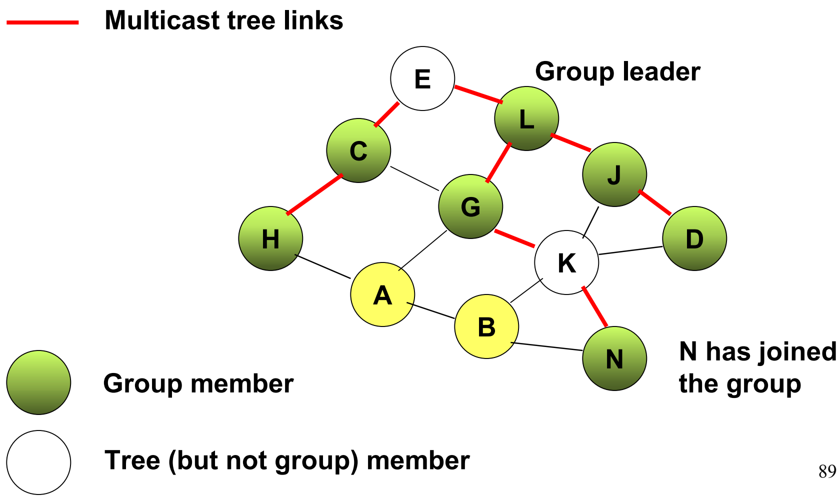
Route Reply (RREP)

Joining the Multicast Tree: AODV



Multicast Activation (MACT)

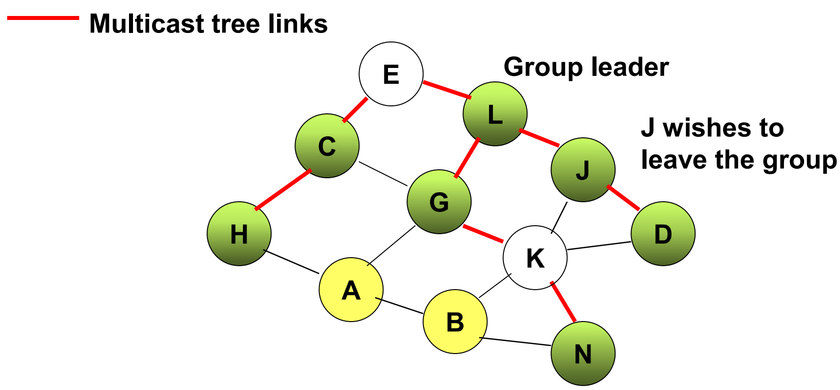
Joining the Multicast Tree: AODV



Sending Data on the Multicast Tree

- Data is delivered along the tree edges maintained by the Multicast AODV algorithm
- If a node which does not belong to the multicast group wishes to multicast a packet
  - It sends a *non-join* RREQ which is treated similar in many ways to RREQ for joining the group
  - As a result, the sender finds a route to a multicast group member
  - Once data is delivered to this group member, the data is delivered to remaining members along multicast tree edges

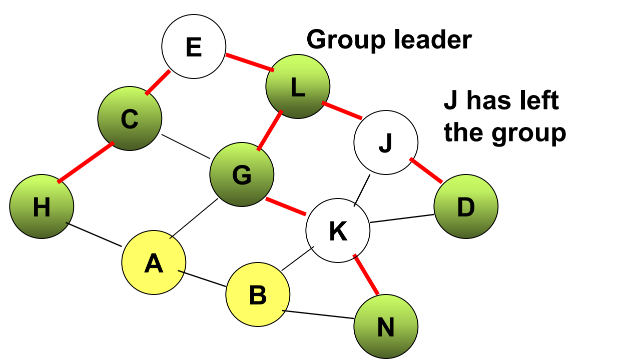
Leaving a Multicast Tree: AODV



91

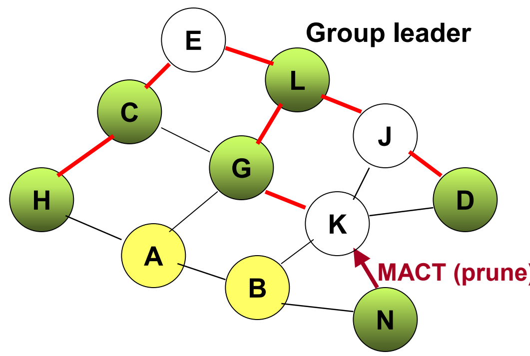
Leaving a Multicast Tree: AODV

Since J is not a leaf node, it must remain a tree member



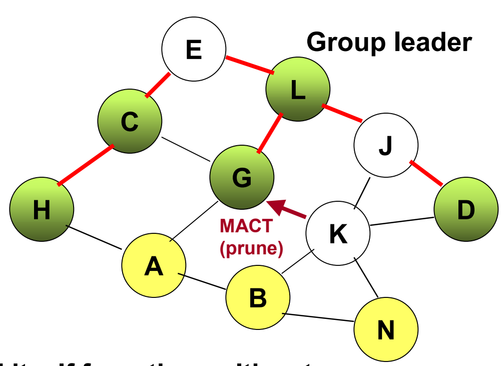
92

Leaving a Multicast Tree: AODV



N wishes to leave
the multicast group

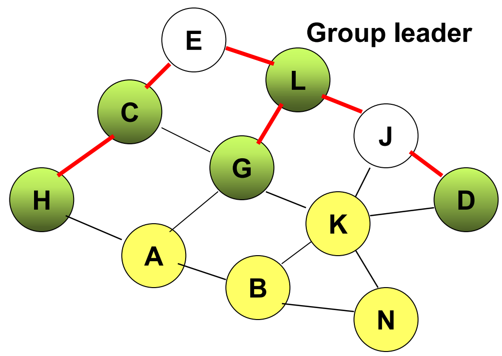
Leaving a Multicast Tree: AODV



Node N has removed itself from the multicast group.

Now node K has become a leaf, and K is not in the group.
So node K removes itself from the tree as well.

Leaving a Multicast Tree: AODV



Nodes N and K are no more in the multicast tree.

95

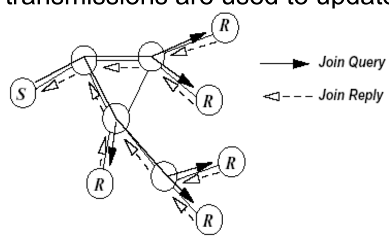
Summary: Multicast AODV

- Similar to unicast AODV
- Uses leaders to maintain group sequence numbers, and to help in tree maintenance
- Provisions for handling network partitions are also included

96

On-Demand Multicast Routing Protocol (ODMRP)

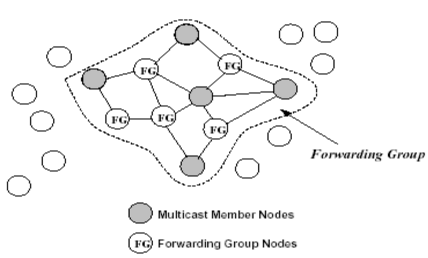
- ODMRP requires cooperation of nodes wishing to send data to the multicast group
  - To construct the multicast *mesh*
- A sender node wishing to send multicast packets *periodically* floods a Join Query packet throughout the network
  - Periodic transmissions are used to update the routes

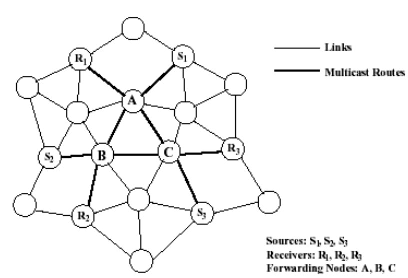


97

On-Demand Multicast Routing Protocol (ODMRP)

- Each multicast group member on receiving a Join Query, broadcasts a Join Reply to all its neighbors
- When node N receives the above broadcast, N becomes member of the *forwarding group*





98

Other Multicasting Protocols

- Several other multicasting protocols have been proposed
- For a comparison study, see [Lee00Infocom]

99

Medium Access Control Protocols

100

Motivation

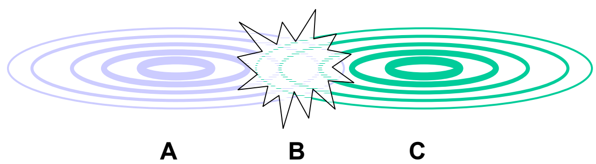
- Can we apply media access methods from fixed networks?
- Example CSMA/CD
  - **C**arrier **S**ense **M**ultiple **A**ccess with **C**ollision **D**etection
  - send as soon as the medium is free, listen into the medium if a collision occurs (original method in IEEE 802.3)
- MAC problems in wireless networks
  - signal strength decreases proportional to the distance
  - sender would apply CS and CD, but the collisions happen at the receiver
  - sender may not “hear” the collision, i.e., CD does not work
  - CS might not work, e.g. if a terminal is “hidden”

MAC Protocols: Issues

- Hidden and Exposed Terminal Problems
- Reliability
- Collision avoidance
- Congestion control
- Energy efficiency

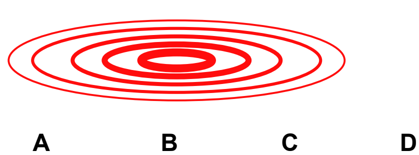
Hidden Terminal Problem

- Hidden terminals
  - A sends to B, C cannot detect A's transmission
  - C wants to send to B, C senses a "free" medium (CS fails)
  - collision at B, A cannot detect the collision (CD fails)
  - A is "hidden" for C



Exposed Terminal Problem

- Exposed terminals
  - B sends to A, C wants to send to D
  - C senses carrier, finds medium in use and has to wait
  - A is outside the radio range of C, therefore waiting is not necessary
  - C is "exposed" to B



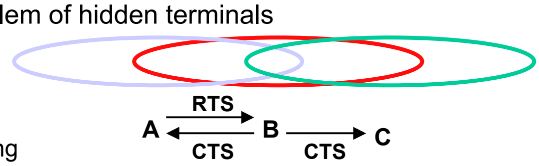
Multiple Access with Collision Avoidance (MACA) [Karn90]

- MACA uses signaling packets for collision avoidance
  - RTS (request to send)
    - sender request the right to send from a receiver with a short RTS packet before it sends a data packet
  - CTS (clear to send)
    - receiver grants the right to send as soon as it is ready to receive
- Signaling packets contain
  - sender address
  - receiver address
  - Duration
- Variants of this method are used in IEEE 802.11

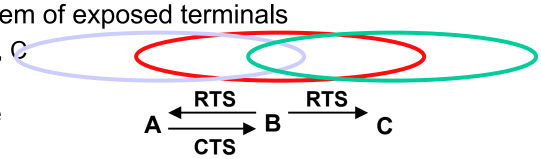
105

MACA Solutions [Karn90]

- MACA avoids the problem of hidden terminals
  - A and C want to send to B
  - A sends RTS first
  - C waits after receiving CTS from B



- MACA avoids the problem of exposed terminals
  - B wants to send to A, C to another terminal
  - now C does not have to wait, as it cannot receive CTS from A



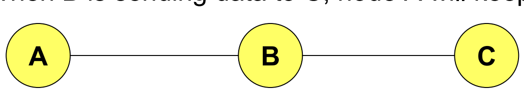
106

MAC: Reliability

- Wireless links are prone to errors. High packet loss rate is detrimental to transport-layer performance.
- Solution: Use of acknowledgements
  - When node B receives a data packet from node A, node B sends an Acknowledgement (Ack).
  - If node A fails to receive an Ack, it will retransmit the packet
  - This approach adopted in many protocols [Bharghavan94, IEEE 802.11]
- IEEE 802.11 Wireless MAC
  - Distributed and centralized MAC components
    - Distributed Coordination Function (DCF)
    - Point Coordination Function (PCF)
  - PCF suitable for access point-based networking
  - DCF suitable for ad hoc networking

IEEE 802.11 DCF

- Uses RTS-CTS exchange to avoid hidden terminal problem
  - Any node overhearing a RTS or CTS cannot transmit for the duration of the transfer
  - Note that RTS/CTS can collide
- Uses ACK to achieve reliability
- Any node receiving the RTS cannot transmit for the duration of the transfer
  - To prevent collision with ACK when it arrives at the sender
  - When B is sending data to C, node A will keep quite



MAC: Collision Avoidance

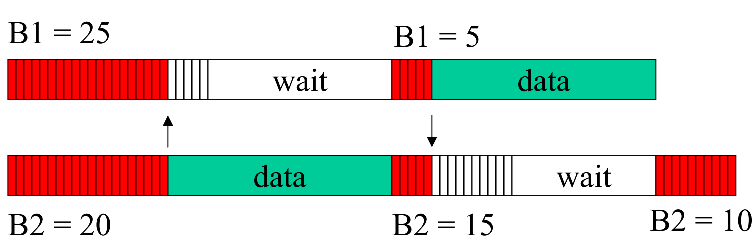
- With half-duplex radios, collision detection is not possible
- Collision avoidance: Once channel becomes idle, the node waits for a randomly chosen duration before attempting to transmit

- IEEE 802.11 DCF
  - When transmitting a packet, choose a backoff interval in the range [0,cw]; cw is contention window
  - Count down the backoff interval when medium is idle
  - Count-down is suspended if medium becomes busy
  - When backoff interval reaches 0, transmit RTS

- Time spent counting down backoff intervals is a part of MAC overhead
- *large cw* leads to larger backoff intervals
- *small cw* leads to larger number of collisions

109

DCF Example



cw = 31

B1 and B2 are backoff intervals at nodes 1 and 2

110

MAC Protocols: Issues

- Hidden and Exposed Terminal Problems
- Reliability
- Collision avoidance
- Congestion control
- Energy efficiency

MAC: Congestion Control

- IEEE 802.11 DCF: Congestion control achieved by dynamically choosing the contention window *cw*
- Binary Exponential Backoff in DCF:
  - When a node fails to receive CTS in response to its RTS, it increases the contention window
    - *cw* is doubled (up to an upper bound)
  - When a node successfully completes a data transfer, it restores *cw* to *CWmin*

MAC: Energy Conservation

- Proposals typically suggest turning the radio off when not needed
- Power Saving Mode in IEEE 802.11 (Infrastructure Mode)
  - An Access Point periodically transmits a beacon indicating which nodes have packets waiting for them
  - Each power saving (PS) node wakes up periodically to receive the beacon
  - If a node has a packet waiting, then it sends a PS-Poll
    - After waiting for a backoff interval in [0,CWmin]
  - Access Point sends the data in response to PS-poll

MAC Protocols: Summary

- Wireless medium is prone to hidden and exposed terminal problems
- Protocols are typically based on CSMA/CA
- RTS/CTS based signaling
- ACKs for reliability
- Contention window is used for congestion control
- IEEE 802.11 wireless LAN standard
- Fairness issues are still unclear

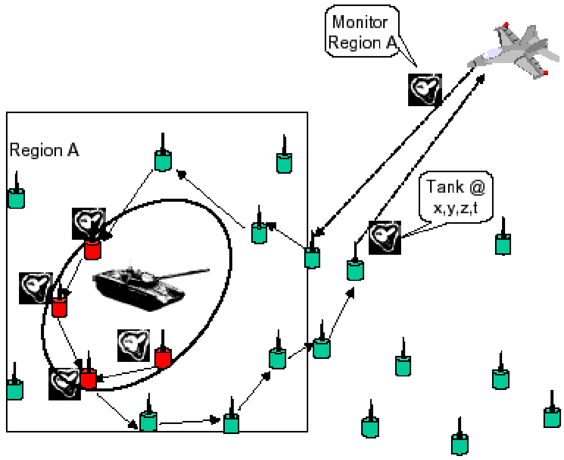
Other MAC Protocols

- **Lot** of other protocols !
- See past MobiCom, WCNC, MilCom, VTC, etc., conferences

Wireless Sensor Networks

Applications

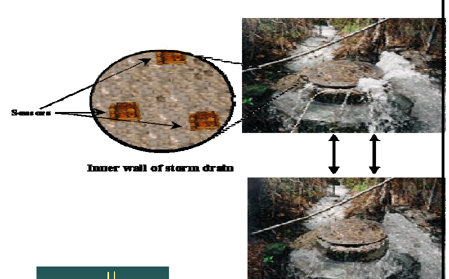
Military: battlefield surveillance



Applications

Scientific: eco-physiology, biocomplexity mapping

Infrastructure: contaminant flow monitoring



Engineering: monitoring structures

Wireless Sensor Networks

- Why not use proposed Ad Hoc protocols?
  - The number of sensor nodes in a sensor network can be several orders of magnitude higher than the nodes in an ad hoc network.
  - Sensor nodes are densely deployed.
  - Sensor nodes are prone to failures.
  - Sensor nodes mainly use broadcast communication paradigm whereas most ad hoc networks are based on point-to-point communications.
  - Sensor nodes are limited in power, computational capacities, and memory.
  - Sensor nodes may not have global *identication* (ID) because of the large amount of overhead and large number of sensors.
  - Data-Centric

119

Wireless Sensor Networks

- Characteristics of sensor networks
  - Application Specific Requirements
  - Data-Aggregation
  - "Data-Centric" Property
  - Location Awareness

120

A Sensor Node

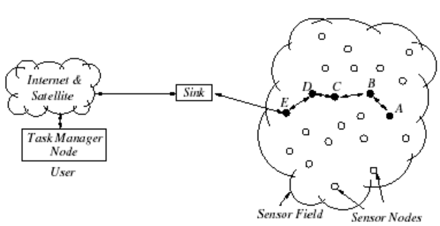
- May need to fit into a matchbox-sized module
- Smart dust mote
  - 4 MHz Atmel AVR 8535 micro-controller
  - 8 KB instruction flash memory
  - 512 bytes RAM
  - 512 bytes EEPROM
  - TinyOS – 3500 bytes of code
- Each sensor node are assumed to be equipped with a GPS unit
  - Or a limited number of nodes have GPS and help others to figure out their locations

121

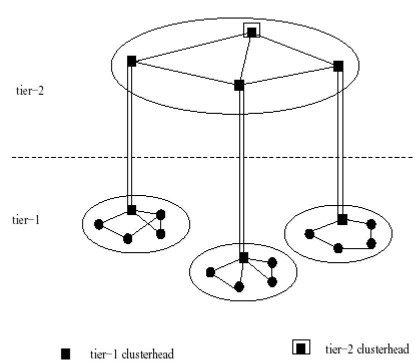
Communication Architecture

- Basically of two types

Flat



Hierarchical



122

Routing in Sensor Networks

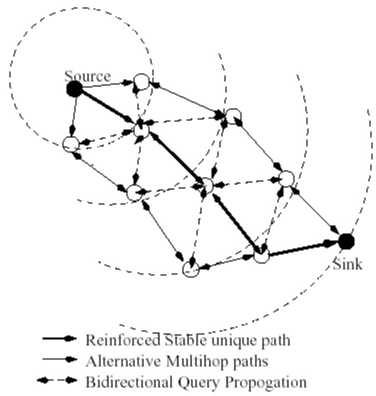
Classification of Sensor Networks

- Proactive Networks
  - The nodes in the network periodically switch on their sensors and transmitters, sense the environment and transmit the data of interest.
- Reactive Networks
  - In this scheme the nodes react immediately to sudden and drastic changes in the value of sensed attribute.
- Hybrid Networks

Routing in Sensor Networks

Directed Diffusion [Intanagonwiwat 2000]

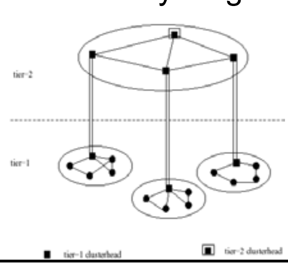
- The query is flooded throughout the network (Flat).



- Does not fully exploit the feature of sensor networks that adjacent nodes have similar data.

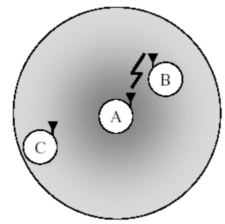
Hierarchical Sensor Network Model

- Each cluster has a cluster head (CH) which collects data form its cluster members.
- CH aggregates the data and sends it to the BS or an upper level cluster head.
- All the nodes transmit only to their immediate CH.
- CH at increasing levels in the hierarchy need to transmit data over relatively longer distances (energy consumption)

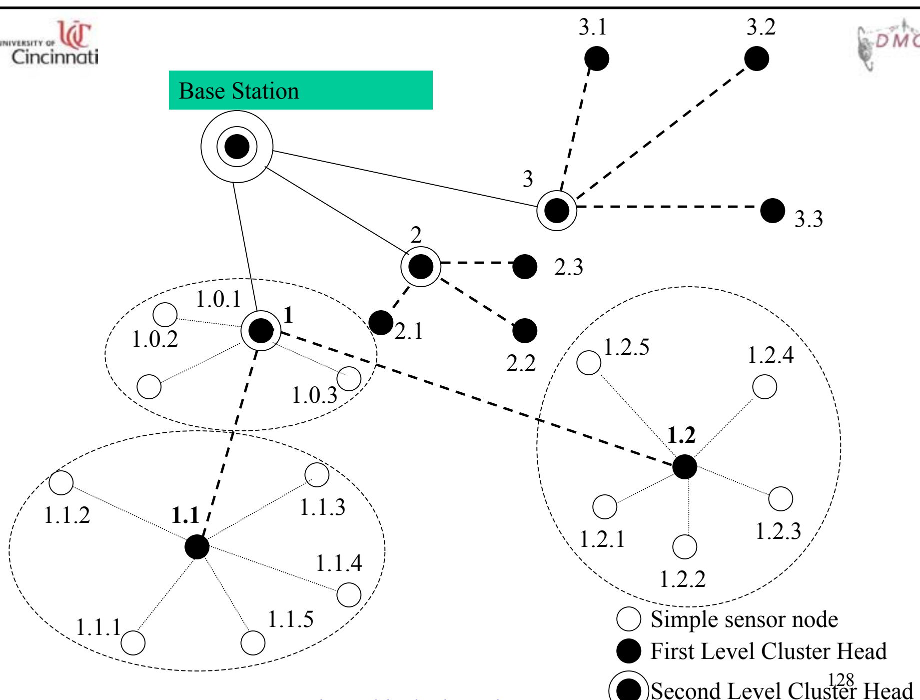


LEACH (Low-Energy Adaptive Clustering Hierarchy) [Heinzelman 2000b]

- Proactive network protocol (Hierarchical)
  - Cluster-based
- MAC: TDMA/CDMA
  - TDMA – Intra-Cluster (Fixed schedule)
  - CDMA – Inter-Cluster (Different codes)



- Utilizes randomized rotation of local cluster-heads to extend battery life
- Data collection is centralized and done periodically
  - Appropriate for constant monitoring of networks



Hierarchical Clustering

Reactive Network Protocol:TEEN

TEEN (Threshold sensitive Energy Efficient sensor Network protocol) [Manjeshwar 2001]

- Designed for reactive networks.
  - Nodes sense their environment continuously
- In this scheme at every cluster change time, the CH broadcasts the following to its members:
  - *Hard Threshold (HT):* This is a threshold value for the sensed attribute.
  - *Soft Threshold (ST):* This is a small change in the value of the sensed attribute which triggers the node to switch on its transmitter and transmit.

TEEN

- Advantages
  - Suited for time critical sensing applications.
  - Message transmission consumes more energy than data sensing. So the energy consumption in this scheme is less than the proactive networks.
  - The soft threshold can be varied.
  - At every cluster change time, the parameters are broadcast afresh and so, the user can change them as required.
- Disadvantage
  - If the thresholds are not reached, the nodes will never communicate.

Hybrid Networks

- Combining the best features of proactive and reactive networks while minimizing their limitations to create a new type of network is called a Hybrid Network

APTEEN (Adaptive TEEN) [Manjeshwar 2002]

Functioning:

- The cluster heads broadcasts the following parameters to sensors:
  - *Attributes (A):* This is a set of physical parameters which the user is interested in obtaining data about.
  - *Thresholds*: This parameter consists of a hard threshold (HT) and a soft threshold (ST).
  - *Schedule:* This is a TDMA schedule, assigning a slot to each node.
  - *Count Time (CT):* It is the maximum time period between two successive reports sent by a node.

APTEEN

- Proceeds exactly like TEEN plus
  - If a node does not send data for a time period equal to the count time (CT), it is forced to sense and retransmit the data.
- TDMA schedule is used and each node in the cluster is assigned a transmission slot.

APTEEN

- Advantages
  - It combines both proactive and reactive policies.
  - It offers a lot of flexibility by allowing the user to set the time interval (CT) and the threshold values for the attributes.
  - Energy consumption can be controlled by changing the count time as well as the threshold values.
- Disadvantages
  - The main drawback of the scheme is the additional complexity required to implement the threshold functions and the count time.
  - **Rate** of energy consumption is increased

UNIVERSITY OF Cincinnati

DMC

Wireless Sensor Networks
Hierarchical X Flat

Hierarchical	Flat
Reservation-based scheduling	Contention-based scheduling
Collisions avoided	Collision overhead present
Reduced duty cycle due to periodic sleeping	Variable duty cycle by controlling sleep time of nodes
Data aggregation by cluster head	Node on multi-hop path aggregates incoming data from neighbors
Simple but non-optimal routing	Routing is complex but optimal
Requires global and local synchronization	Links formed in the fly, without synchronization
Overhead of cluster formation throughout the network	Routes formed only in regions that have data for transmission
Lower latency as multi-hop network formed by cluster-heads is always available	Latency in waking up intermediate nodes and setting up the multi-hop path
Energy dissipation is uniform	Energy dissipation depends on traffic patterns
Energy dissipation cannot be controlled	Energy dissipation adapts to traffic pattern
Fair channel allocation	Fairness not guaranteed

135

UNIVERSITY OF Cincinnati

DMC

Current Research Projects

Project Name	Research Area	HTTP Location
SensoNet [3]	*-Transport, network, data link and physical layers. -Power control, mobility and task management planes.*	*http://www.ece.gatech.edu/research/labs/bwn/*
WINS [22, 69]	*-Distributed network and Internet access to sensors, controls, and processors.*	*http://www.janet.ucla.edu/WINS/*
SPIN [35]	*-Data dissemination protocols.*	*http://nms.lcs.mit.edu/projects/leach*
SPINS [66]	*-Security protocol.*	*http://paris.cs.berkeley.edu/~perrig/projects.html*
SINA [75, 84]	*-Information networking architecture.*	*http://www.eecis.udel.edu/~cshen/*
µAMPS [77]	*-Framework for implementing adaptive energy-aware distributed microsensors.*	*http://www-mtl.mit.edu/research/icsystems/uamps/*
LEACH [34]	*-Cluster formation protocol*	*http://nms.lcs.mit.edu/projects/leach*
Smart Dust [42]	*-Laser communication from a cubic millimeter -Mote delivery -Sub-microWatt electronics -Power sources -Macro Motes (COTS Dust)*	*http://robotics.eecs.berkeley.edu/~pister/SmartDust/*
SCADDS [22, 11, 33] [8, 20, 96, 39, 23, 27]	*-Scalable coordination architectures for deeply distributed and dynamic systems.*	*http://www.isi.edu/scadds/*
PicoRadio [71, 70]	*-Develop a "system-on-chip" implementation of a PicoNode.*	*http://bwrc.eecs.berkeley.edu/Research/Pico_Radio/PicoNode.htm*
PACMAN [79]	*-Mathematical framework that incorporates key features of computing nodes and networking elements.*	*http://pacman.usc.edu*
Dynamic Sensor Networks [19]	*-Routing and power aware sensor management -Network services API*	*http://www.east.isi.edu/DIV10/dsn/*
Aware Home [36]	*-Requisite technologies to create a home environment that can both perceive and assist its occupants.*	*http://www.cc.gatech.edu/fce/ahri*
COUGAR Device Database Project [7]	*-Distributed query processing.*	*http://www.cs.cornell.edu/database/cougar/index.htm*
DataSpace [38]	*-Distributed query processing.*	*http://www.cs.rutgers.edu/dataman/*

136

Related Standards Activities

Internet Engineering Task Force (IETF) Activities

- 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**

Related Standards Activities

- BlueTooth
  - http://www.bluetooth.com
- IEEE 802.15
  - http://grouper.ieee.org/groups/802/15/
- HomeRF [Lansford00ieee]
  - http://www.homerf.org
- IEEE 802.11
  - http://grouper.ieee.org/groups/802/11/
- HiperLan/2
  - http://www.etsi.org/technicalactiv/hiperlan2.htm

139

Bluetooth [Haartsen98]

- Features: Cheaper, smaller, low power, ubiquitous, unlicensed frequency band (2.4GHz)
- Current Spec version 1.1 (1600+ pages)
- Promoter group consisting of 9
  - Ericsson, IBM, Intel, Nokia, Toshiba, 3Com, Agere, Microsoft, Motorola
- 3000+ adopters

140

Bluetooth: Link Types

- Designed to support multimedia applications that mix voice and data
- Synchronous Connection-Oriented (SCO) link
  - Symmetrical, circuit-switched, point-to-point connections
  - Suitable for voice
  - Two consecutive slots (forward and return slots) reserved at fixed intervals
- Asynchronous Connectionless (ACL) link
  - Symmetrical or asymmetric, packet-switched, point-to-multipoint
  - Suitable for bursty data
  - Master units use a polling scheme to control ACL connections

141

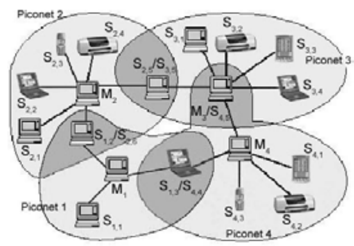
Bluetooth: Piconet

- A *channel* is characterized by a frequency-hopping pattern
- Two or more terminals sharing a channel form a *piconet*
  - Roughly 1 Mbps per Piconet
- One terminal in a piconet acts as a *master* and up to 7 *slaves*
- Other terminals are *slaves*
- Polling scheme: A slave may send in a slave-to-master slot when it has been addressed by its MAC address in the previous master-to-slave slot

142

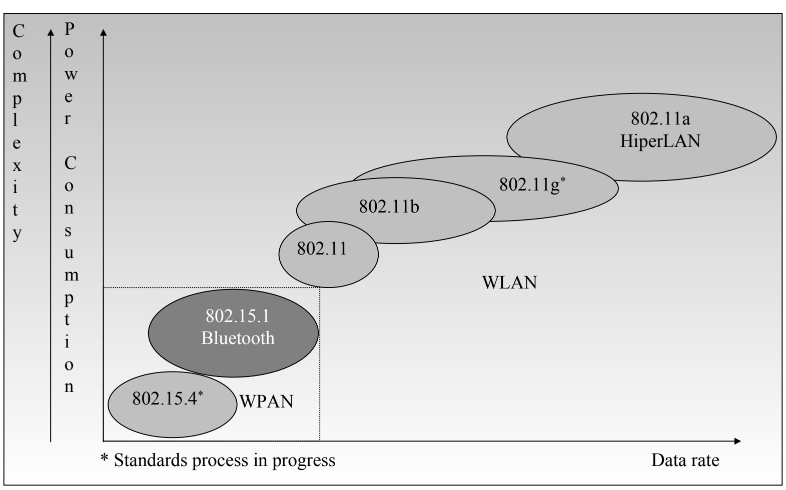
Bluetooth: Scatternet

- Several piconets may exist in the same area (such that units in different piconets are in each other's range)
  - A large number of piconets in the vicinity may eventually interfere with each other [Cordeiro01Globecom]
  - Interference mitigation schemes [Cordeiro02Sbrc]
- A group of piconets is called a *scatternet*
  - New routing issues [Bhagwat99Momuc]



143

The Scope of the Various WLAN and WPAN Standards



144

Open Issues
in
Mobile Ad Hoc Networking

Open Problems

- Issues other than routing have received much less attention so far

Other interesting problems:

- Address configuration (DHCP ???)
- MAC protocols
- Improving interaction between protocol layers
- QoS issues
- Applications for MANET

Thank you !!!

For more information, send e-mail to
Carlos Cordeiro at
cordeicm@ececs.uc.edu
or visit
http://www.ececs.uc.edu/~cordeicm

147