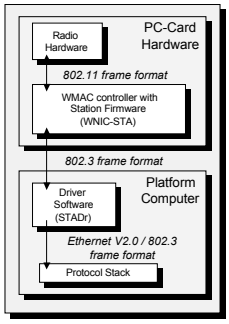
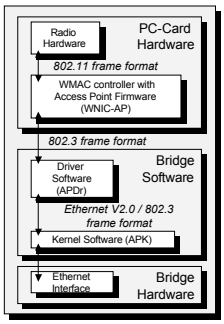
IEEE 802.11 Terminology - STA (Station)



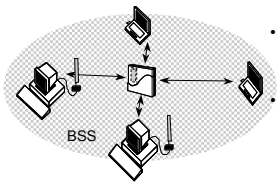
- Device that contains IEEE 802.11 conformant MAC and PHY interface to the wireless medium, but does not provide access to a distribution system
- Most often end-stations available in terminals (work-stations, laptops etc.)
- Implemented in Wireless IEEE 802.11 PC-Card
- Ethernet-like driver interface
  - supports virtually all protocol stacks
- Frame translation according to IEEE Std 802.1H
  - IEEE 802.3 frames: translated to 802.11
  - Maximum Data limited to 1500 octets
- Transparent bridging to Ethernet

IEEE 802.11 Terminology - AP (Access Point)



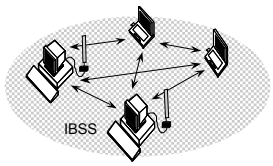
- Device that contains IEEE 802.11 conformant MAC and PHY interface to the wireless medium, providing access to a distribution system for associated stations
- Most often infra-structure products that connect to wired backbones
- Implemented in Wireless IEEE 802.11 PC-Card inserted in AP
- STAs select an AP and "associate" with it
- APs :
  - Support roaming
  - Provide time synchronization (beaconing)
  - Provide Power Management support

IEEE 802.11 Terminology - Basic Service Set (BSS)



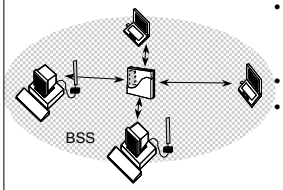
- A set of stations controlled by a single "Coordination Function" (=the logical function that determines when a station can transmit or receive)
- Similar to a "cell" in Cellular network terminology
- A BSS can have an Access-Point (both in standalone networks and in building-wide configurations), or can run without and Access-Point (in standalone networks only)
- Station-to-Station traffic is relayed by the Access Point

IEEE 802.11 Terminology - Independent Basic Service Set (IBSS)



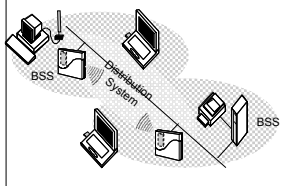
- A Basic Service Set (BSS) which forms a self-contained network in which no access to a Distribution System is available
- A BSS without an Access-Point
- Station-to-station traffic flows directly without any relay action
- All stations in the cell will be able to receive frames transmitted by another station in the cell (filtering of traffic for subsequent processing is based on MAC address of the receiver)

IEEE 802.11 Terminology - Extended Service Set (ESS)



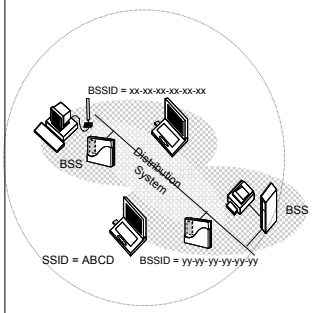
- A set of one or more Basic Service Sets interconnected by a Distribution System (DS)
- Traffic always flows via Access-Point
- Distribution System (DS):
- A system to interconnect a set of Basic Service Sets
  - Integrated; A single Access-Point in a standalone network
  - Wired; Using cable to interconnect the Access-Points
  - Wireless; Using wireless to interconnect the Access-Points

IEEE 802.11 Terminology - Extended Service Set (ESS)



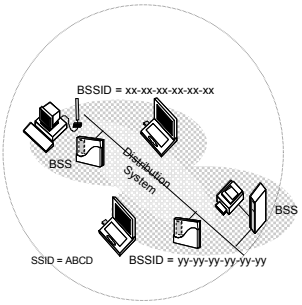
- A set of one or more Basic Service Sets interconnected by a Distribution System (DS)
- Traffic always flows via Access-Point
- Distribution System (DS):
- A system to interconnect a set of Basic Service Sets
  - Integrated; A single Access-Point in a standalone network
  - Wired; Using cable to interconnect the Access-Points
  - Wireless; Using wireless to interconnect the Access-Points

IEEE 802.11 Terminology SSID (Network name)



- Service Set Identifier (SSID): "Network name"
- One network (ESS or IBSS) has one SSID: 32 octets long string
- Needed to separate one network from the other
- Used during initial establishment of communication between STA and AP to allow STA to select the correct AP
- Can be viewed as Security Provision in combination with so-called "Closed Option" (not providing the correct SSID means no access to the network)

IEEE 802.11 Terminology BSSID (Cell Identifier)



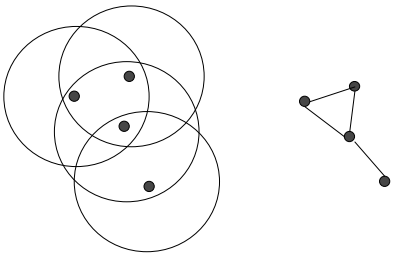
- Basic Service Set Identifier (BSSID) - "cell identifier"
- One BSS has one BSSID
- 6 octets long (MAC address format)
- In ESS is the same as the MAC address of the radio in the AP
- In IBSS the value of BSSID will be randomly generated, and with local-bit on
- Used as filter for multi-cast traffic and for traffic from other networks (in IBSS networks)
- Used during hand-over (roaming) to other AP, in identifying the "old" AP

Mobile Ad Hoc Networks

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

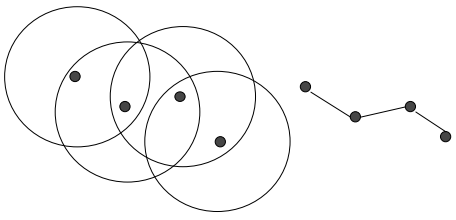
Mobile Ad Hoc Networks

- May need to traverse multiple links to reach a destination



Mobile Ad Hoc Networks (MANET)

- Mobility causes route changes



Why Ad Hoc Networks ?

- Ease of deployment
- Speed of deployment
- Decreased dependence on infrastructure

Many Applications

- Personal area networking
  - 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

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
- 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 in different ad hoc networks
  - bit rate
  - timeliness constraints
  - reliability requirements
  - unicast / multicast / geocast
  - host-based addressing / content-based addressing / capability-based addressing
- May co-exist (and co-operate) with an infrastructure-based network

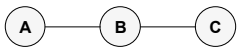
Many Variations

- Mobility patterns may be different
  - people sitting at an airport lounge
  - New York taxi cabs
  - kids playing
  - military movements
  - personal area network
- 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
  - Hidden terminal problem (see next slide)
- Packet losses due to transmission errors
- Mobility-induced route changes
- Mobility-induced packet losses
- Battery constraints
- Potentially frequent network partitions
- Ease of snooping on wireless transmissions (security hazard)

Hidden Terminal Problem



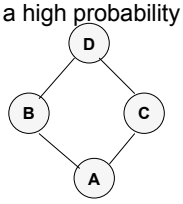
Nodes A and C cannot hear each other

Transmissions by nodes A and C can collide at node B

Nodes A and C are hidden from each other

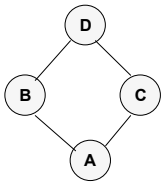
Broadcast Storm Problem

- When node A broadcasts a route query, nodes B and C both receive it
- B and C both forward to their neighbors
- B and C transmit at about the same time since they are reacting to receipt of the same message from A
- This results in a high probability of collisions



Broadcast Storm Problem

- Redundancy: A given node may receive the same route request from too many nodes, when one copy would have sufficed
- Node D may receive from nodes B and C both

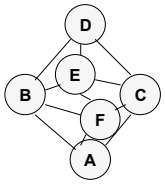


Solutions for Broadcast Storm

- Probabilistic scheme: On receiving a route request for the first time, a node will re-broadcast (forward) the request with probability p
- Also, re-broadcasts by different nodes should be staggered by using a collision avoidance technique (wait a random delay when channel is idle)
  - this would reduce the probability that nodes B and C would forward a packet simultaneously in the previous example

Solutions for Broadcast Storms

- Counter-Based Scheme: If node E hears more than *k* neighbors broadcasting a given route request, before it can itself forward it, then node E will not forward the request
- Intuition: *k* neighbors together have probably already forwarded the request to all of E's neighbors



Summary: Broadcast Storm Problem

- Flooding is used in many protocols, such as Dynamic Source Routing (DSR)
- Problems associated with flooding
  - collisions
  - redundancy
- Collisions may be reduced by "jittering" (waiting for a random interval before propagating the flood)
- Redundancy may be reduced by selectively re-broadcasting packets from only a subset of the nodes

Routing Protocols

- Proactive protocols
  - Determine routes independent of traffic pattern
  - Traditional link-state and distance-vector routing protocols are proactive
- Reactive protocols
  - Maintain routes only if needed
- Hybrid protocols

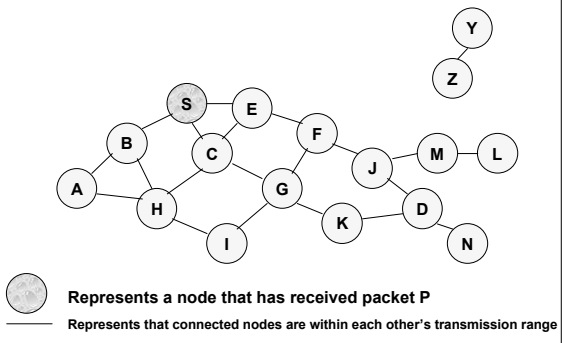
Trade-Off

- 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 trade-off depends on the traffic and mobility patterns

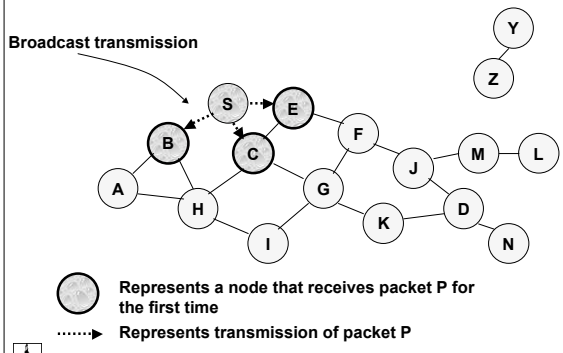
Flooding for Data Delivery

- Sender S broadcasts data packet P to all its neighbors
- Each node receiving P forwards P to its neighbors
- Sequence numbers 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

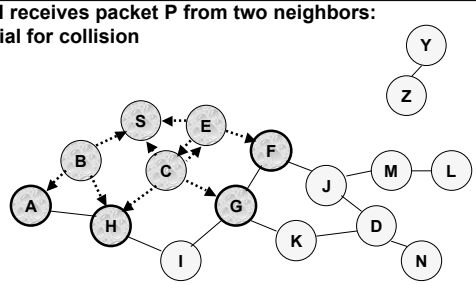


Flooding for Data Delivery



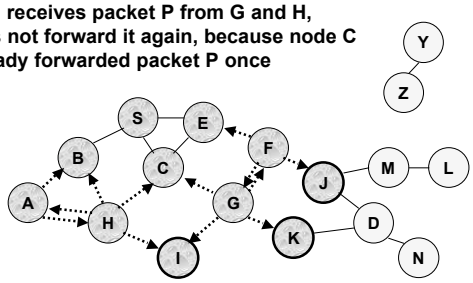
Flooding for Data Delivery

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



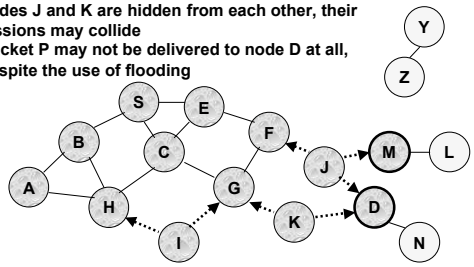
Flooding for Data Delivery

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



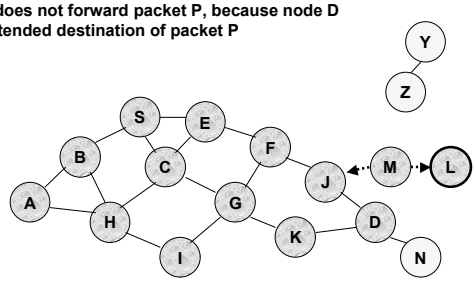
Flooding for Data Delivery

- 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



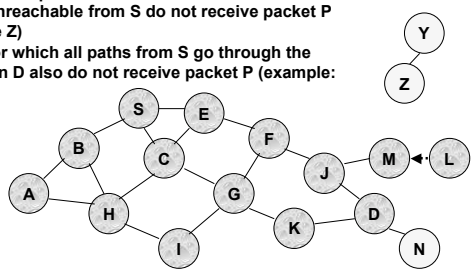
Flooding for Data Delivery

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



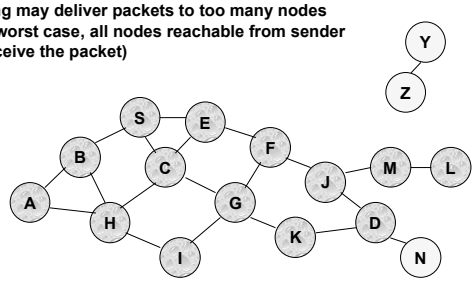
Flooding for Data Delivery

- 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
- May be more efficient than other protocols when 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

Flooding for Data Delivery: Disadvantages

- Potentially, very high overhead
  - Data packets may be delivered to too many nodes who 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 packet(s)
- Overhead of control packet flooding is amortized over data packets transmitted between consecutive control packet floods

CMU Implementation: Lessons Learned

- "Wireless propagation is not what you would expect" [Maltz99]
  - Straight flat areas with line-of-sight connectivity had worst error rates
- "Bystanders will think you are nuts" [Maltz99]
  - If you are planning experimental studies in the streets, it may be useful to let police and security guards know in advance what you are up to

Implementation Issues:

- Where to Implement Ad Hoc Routing
  - Link layer
  - Network layer
  - Application layer

Implementation Issues:

- Address Assignment
  - Restrict all nodes within a given ad hoc network to belong to the same subnet
    - Routing within the subnet using ad hoc routing protocol
    - Routing to/from outside the subnet using standard internet routing
  - Nodes may be given random addresses
    - Routing to/from outside world becomes difficult unless Mobile IP is used

Implementation Issues:

- Address Assignment
  - How to assign the addresses ?
- Non-random address assignment:
  - DHCP for ad hoc network ?
- Random assignment
  - What happens if two nodes get the same address ?
  - Duplicate address detection needed
  - One procedure for detecting duplicates within a connected component: When a node picks address A, it first performs a few route discoveries for destination A. If no route reply is received, then address A is assumed to be unique.

Implementation Issues:

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

Implementation Issues

- Can we make any guarantees on performance?
  - When using a non-licensed band, difficult to provide hard guarantees, since others may be using the same band
- Must use an licensed channel to attempt to make any guarantees
  - 802.11 (9xx MHz, cordless phones, baby monitors), 802.11b, 802.11g, 802.11e operate in 2.4 GHz (along with Microwaves, cordless phones), 802.11a (cordless phones)

Implementation Issues

- Only some issues have been addressed in existing implementations
- Security issues typically ignored
- Address assignment issue also has not received sufficient attention

Routing In Bluetooth

- Ad hoc routing protocols needed to route between multiple piconets
- Existing protocols may need to be adapted for Bluetooth
  - For instance, not all nodes within transmission range of node X will hear node X
    - Only nodes which belong to node X's current piconet can hear the transmission from X
  - Flooding-based schemes need to take this limitation into account