Wireless Mesh Networks

Prasant Mohapatra

Department of Computer Science

University of California, Davis

Email: prasant@cs.ucdavis.edu

Brief History

- The concept of wireless multihop networks dates back to 1970s
  - DARPA packet radio networks
- Development languished in 1980s
  - Partially due to the lack of low cost CPU and memory for ad hoc routing
- Rekindled since about 1995

Enabling Technologies

- Self organizing systems
- Software defined radio
- Miniaturization
- Battery technology
- Smart antennas
- User terminal evolution
- New frequency bands

Organization

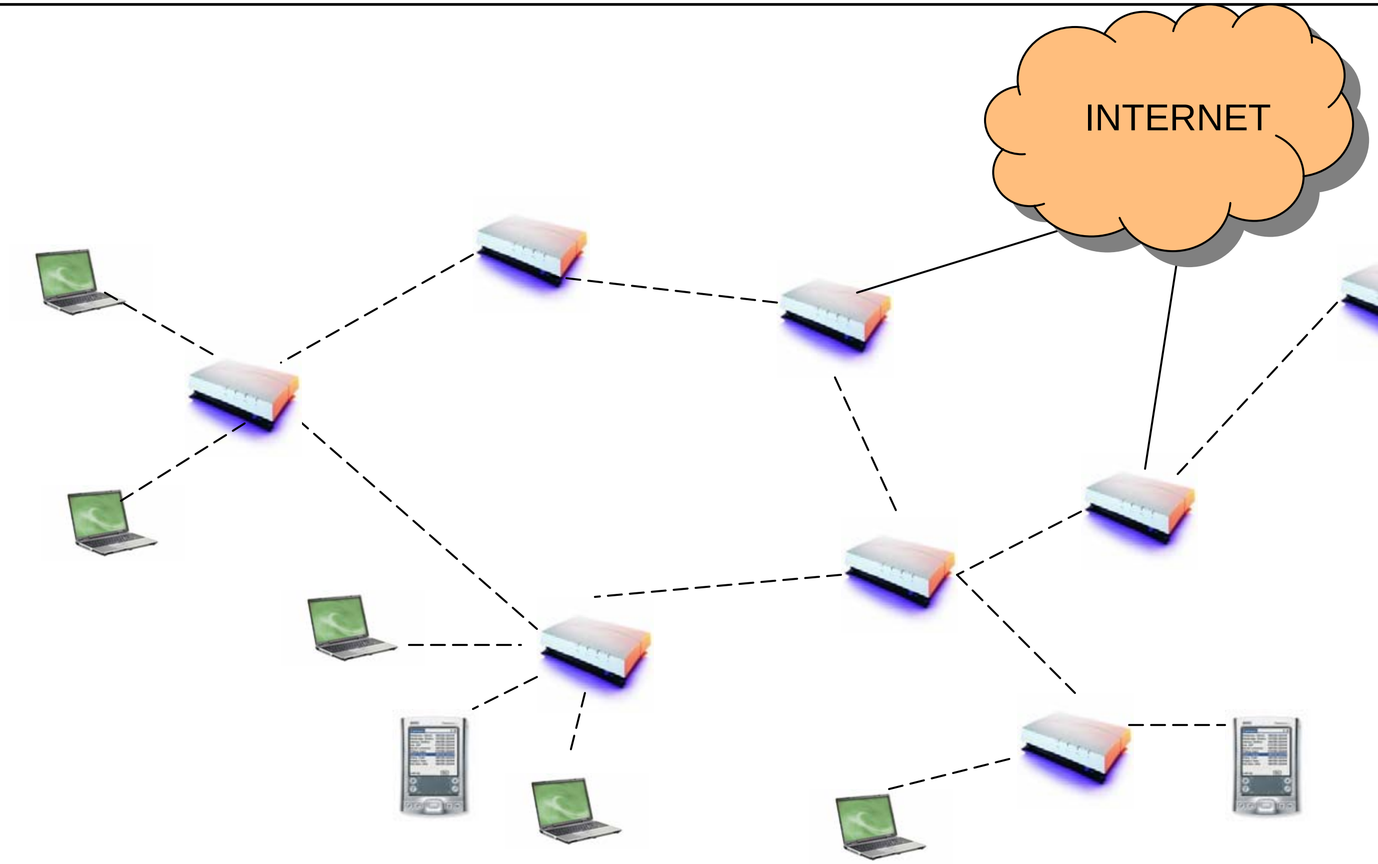
1. Mesh Architecture
2. Applications
3. Transport Layer
4. Routing
5. Medium Access Control
6. Capacity Enhancement
7. QoS Support
8. Security & Management
9. Standardization Efforts
10. Experimental and Commercial Systems
11. Concluding Remarks

1. Mesh Architecture

What are mesh networks?

- Wireless Mesh Networks are composed of wireless access points (routers) that facilitates the connectivity and intercommunication of wireless clients through multi-hop wireless paths
- The mesh may be connected to the Internet through gateway routers
- The access points are considered as the nodes of mesh; they may be heterogeneous and connected in a hierarchical fashion
- Unlike MANETs, end hosts and routing nodes are distinct. Routers are usually stationary.

Wireless Mesh Architecture

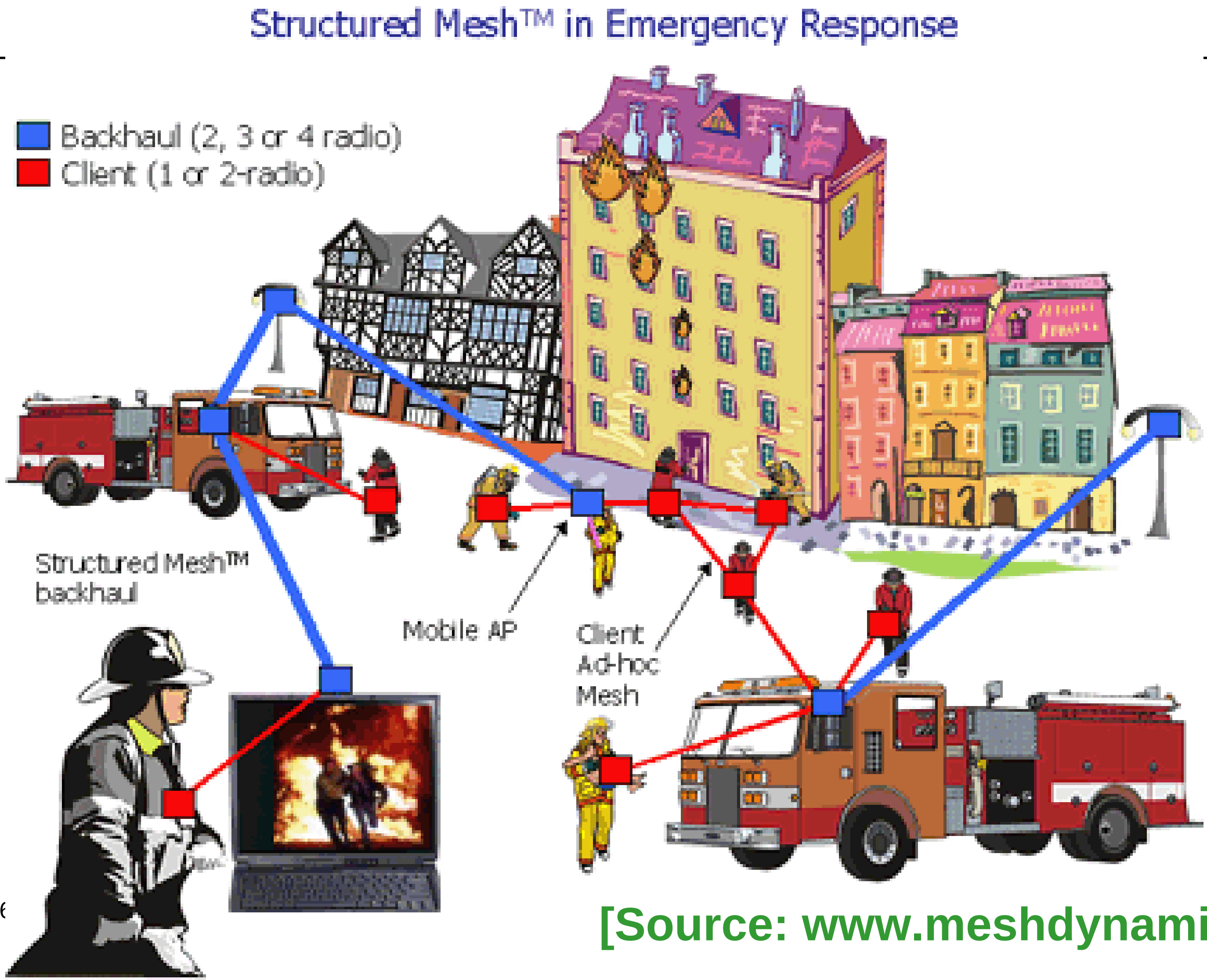


2. Applications

Applications

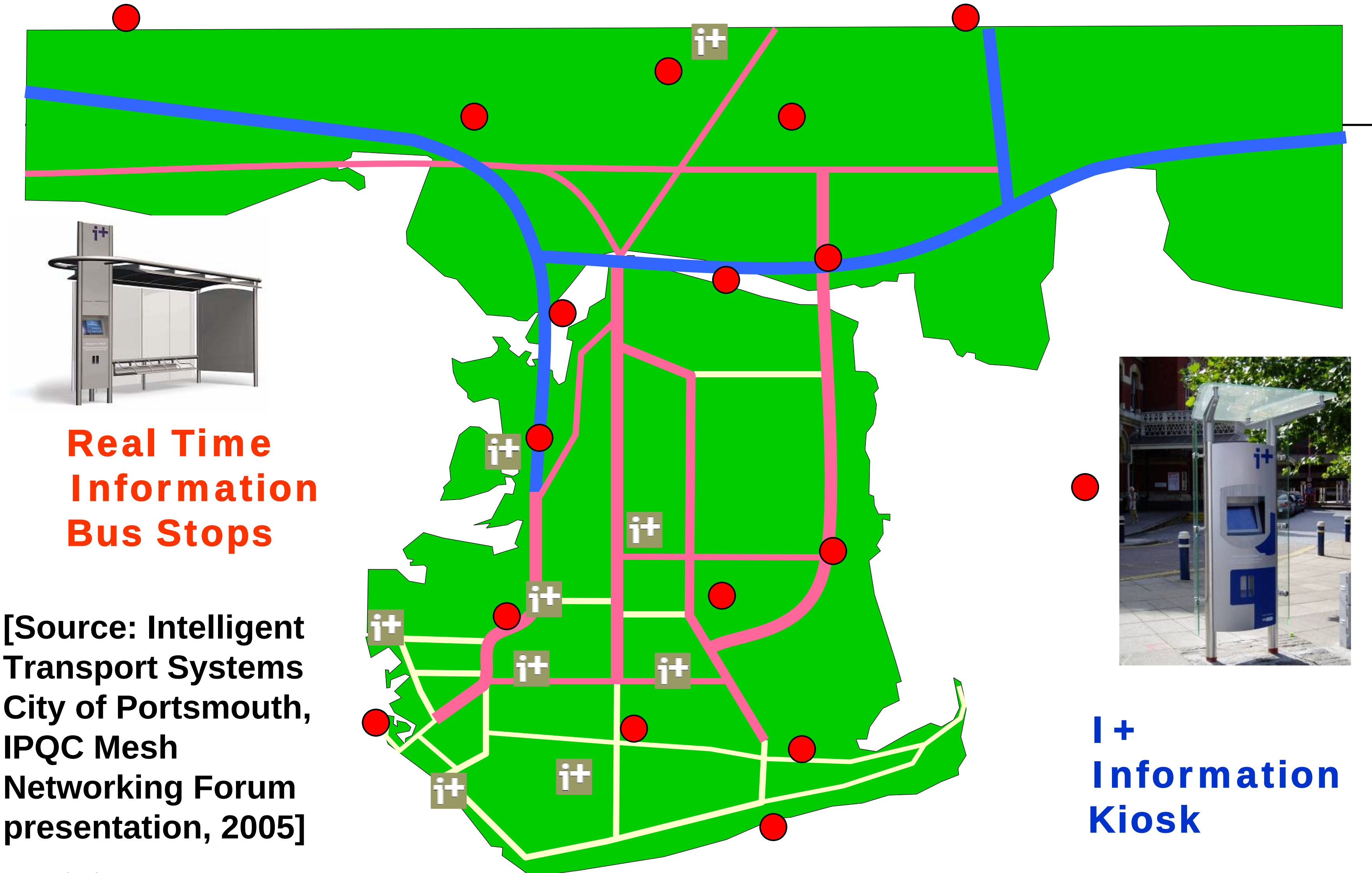
- Community Networks
- Enterprise Networks
- Home Networks
- Local Area Networks for Hotels, Malls, Parks, Trains, etc.
- Metropolitan Area Networks
- Ad hoc deployment of LAN
  - Public Safety, Rescue & Recovery Operation

Public Safety



[Source: www.meshdynamics.com]

Intelligent Transportation System



Real Time Information Bus Stops

I+ Information Kiosk

[Source: Intelligent Transport Systems City of Portsmouth, IPQC Mesh Networking Forum presentation, 2005]

Why Wireless Mesh?

- Low up-front costs
- Ease of incremental deployment
- Ease of maintenance
- Provide NLOS coverage
- Advantages of Wireless APs (over MANETs)
  - Wireless AP backbone provides connectivity and robustness which is not always achieved with selfish and roaming users in ad-hoc networks
  - Take load off of end-users
  - Stationary APs provide consistent coverage

3. Transport Layer

TCP Characteristics

- TCP Characteristics – impact on wireless mesh:
  - Window based transmissions
    - Varying RTT estimates due to bursty traffic
    - Short-term load increases
  - Slow-start
    - Underutilization of network resources
    - Unfairness
  - Linear increase multiplicative decrease
    - Multiplicative decrease is not appropriate
  - Dependence on ACKs
    - High overheads for WLANs

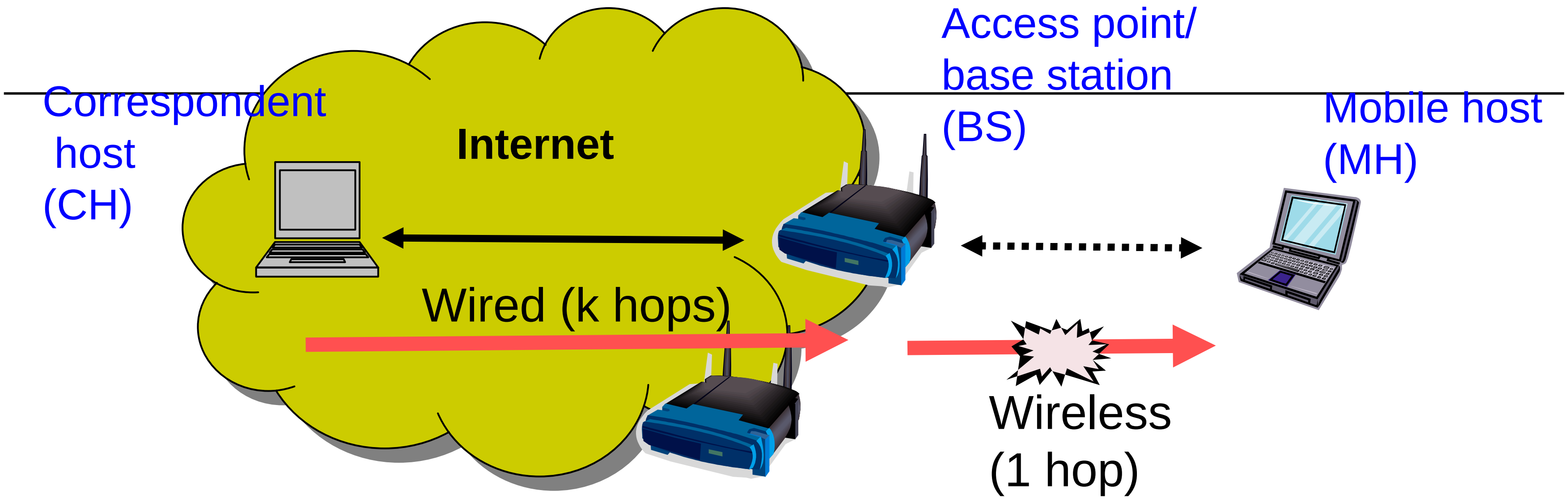
Characteristics – cont.

- TCP sender misinterprets losses as congestion
  - Retransmits unACKed segments
  - Invokes congestion control
  - Enters slow start recovery
  - Throughput is always low as a result of frequent slow start recovery
- Why use TCP at all in such cases?
  - For seamless portability to applications like file transfer, e-mail and browsers which use standard TCP

TCP Adaptations for Wireless Mesh

- Hide error losses from the sender
  - So the sender will not reduce congestion window
- Let the sender know, or determine, cause of packet loss
  - For losses due to errors, it will not reduce congestion window

Hiding Packet Losses



- Split-connection approaches:
  - Split the TCP connection into two independent connection at BS. Example: I-TCP
- Snoop TCP approach:
  - BS acks the CH. Copies packet. Retransmits locally on the wireless hop in case of loss.
- Need to maintain state on BS.

Adapted Transport Layer Protocols

- Ad Hoc Transport Protocol (ATP)
- Ad Hoc Transmission Control Protocol (ATCP)

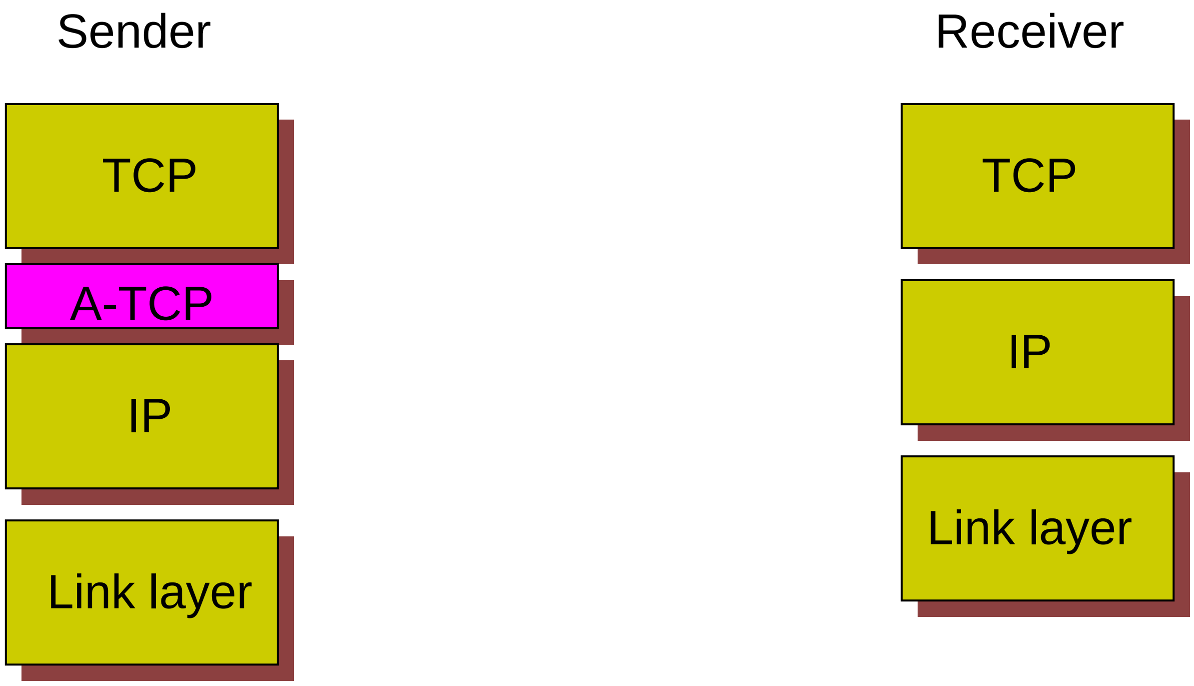
Ad Hoc Transport Protocol (ATP)

- Layer coordination
  - Uses feedback from network nodes for congestion detection, avoidance, and control
- Rate based transmissions
  - Avoids impact of bursty traffic
- Decoupling of congestion control and reliability
  - Congestion control uses feedback from the network; Reliability is ensured through receiver feedback and selective ACK
- Assisted congestion control
  - Adapts sending rate based on feedback from intermediate nodes
- TCP friendliness and fairness
  - Achieved through feedback from intermediate nodes

ATCP Approach

- ATCP utilizes network layer feedback (from the intermediate nodes) to take appropriate actions
- Network feedback is:
  - ICMP: The *Destination Unreachable* ICMP message indicates route disruption
  - ECN: Indicates network congestion
    - With ECN enabled, time out and 3 dup ACKs are assumed to no longer be due to congestion

ATCP in the TCP/IP Stack



TCP/ATCP Behavior

- RTO or 3rd dup ACK:
  - Retransmits unACKed segments
- ACK with ECN flag:
  - Invokes congestion control
- *Destination Unreachable* ICMP message:
  - Stops transmission; Enter Persist Mode
  - Wait until a new route is found
    - → resume transmission
- ATCP monitors TCP state and spoofs TCP in such a way to achieve the above behaviors

TCP Persist Mode

- Triggered by an ACK carrying zero advertised window size from TCP receiver
- Parameters are frozen
- Persist timer is started
- TCP sender sends a probe segment each time persist timer expire
- When TCP sender receives an ACK carrying non-zero advertised window size from TCP receiver

  ➔ TCP sender resumes transmission

Advantages of ATCP

- ATCP improves TCP performance
  - Maintains high throughput since TCP's unnecessary congestion control is avoided
  - Saves network resources by reducing number of unnecessary re-transmissions
- End-to-End TCP semantics are maintained
- ATCP is transparent
  - Nodes with and without ATCP can set up TCP connections normally

Transport Layer Challenges

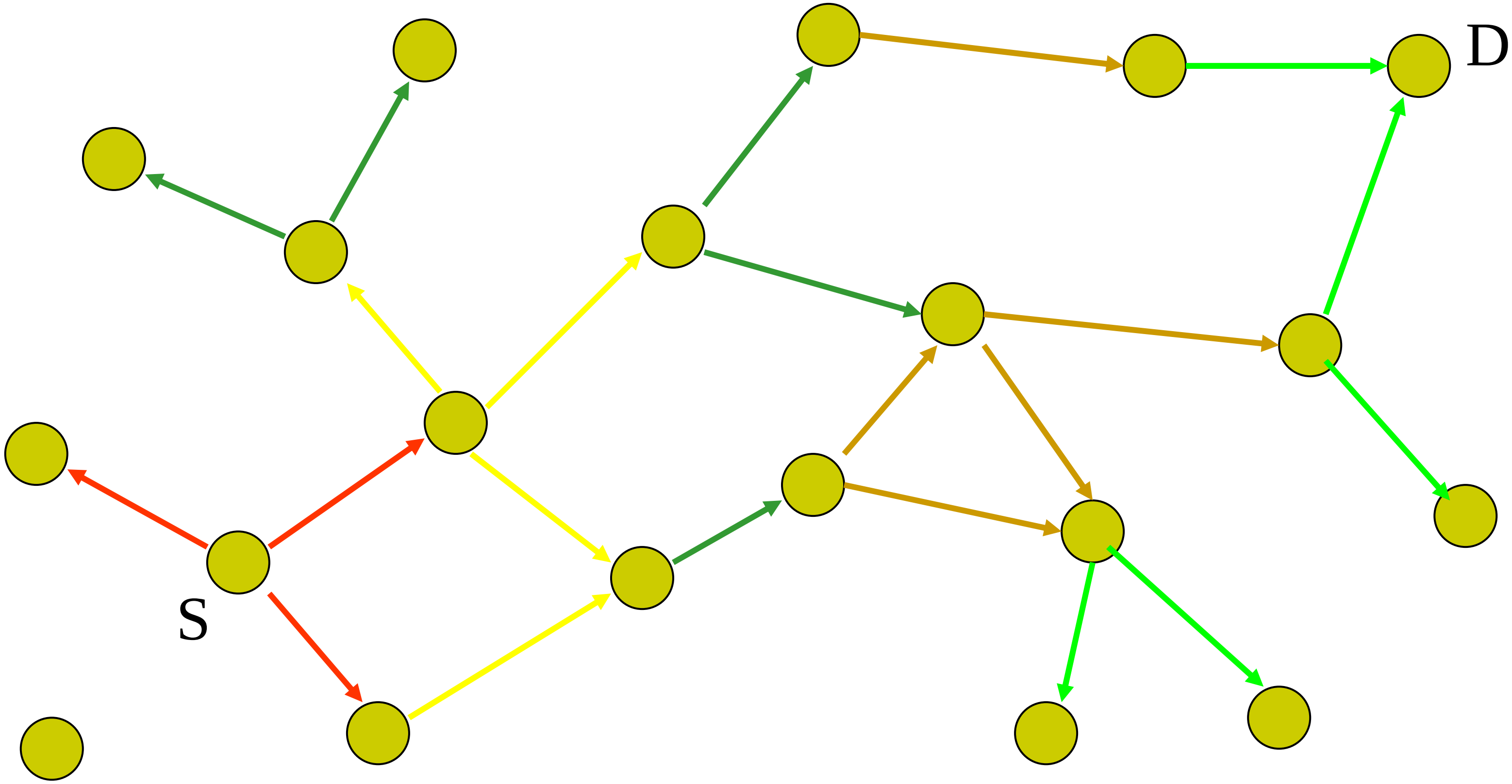
- New transport layer protocols need to be developed that avoids the shortcomings of TCP while being compatible with it
- Transport layer protocols for supporting real-time traffic in wireless meshes are desirable
- Integration of transport layer with other layers; or inferring and reacting with respect to the observations at other layers
- Impact of mobility on transport layer

4.Routing in Wireless Mesh

Multi-hop Routing Protocols

- Applying Ad-hoc network routing methods
- Special considerations
  - WMN routers differ from MANET routers
    - Power supply
    - Mobility
  - Separation of WMN routers and clients
- Routing Approaches
  - Flooding-based routing
  - Proactive routing
  - Reactive (on-demand) routing
  - Hierarchical routing

Flooding-Based Routing



Proactive Routing

- Nodes maintain global state information
- Consistent routing information are stored in tabular form at all the nodes
- Changes in network topology are propagated to all the nodes and the corresponding state information are updated
- Routing state maintenance could be flat or hierarchical

Examples of Proactive Routing

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

Destination Sequenced Distant Vector (DSDV) Routing

- Table-Driven algorithm based on Bellman-Ford routing mechanism
- Every node maintains a routing table that records the number of hops to every destination
- Each entry is marked with a sequence number to distinguish stale routes and avoiding routing loops
- Routes labeled with most recent sequence numbers is always used
- Routing updates can be incremental or full dumps

Optimized Link State Routing (OLSR)

- Uses the concept of multipoint relays (MPR).
  - Multipoint relays of node X are its neighbors such that *each two-hop neighbor of X is a one-hop neighbor of at least one multipoint relay of X.*
- Only MPRs participate in routing.
  - Only MPRs generate link state updates.
  - Only MPRs relay link state updates.

Routing Protocols for Wireless Mesh

- TBRPF
  - Topology broadcast based on reverse-path forwarding
  - PacketHop Inc. and Firetide Inc. WIMENET routers
- AODV
  - Ad hoc On-demand Distance Vector Routing
  - Kiyon Inc.'s Autonomous Network
- DSR
  - Dynamic Source Routing
  - MSR's WIMENET testbed
- ExOR
  - Extremely Opportunistic Routing
  - RoofNet project of MIT

TBRPF

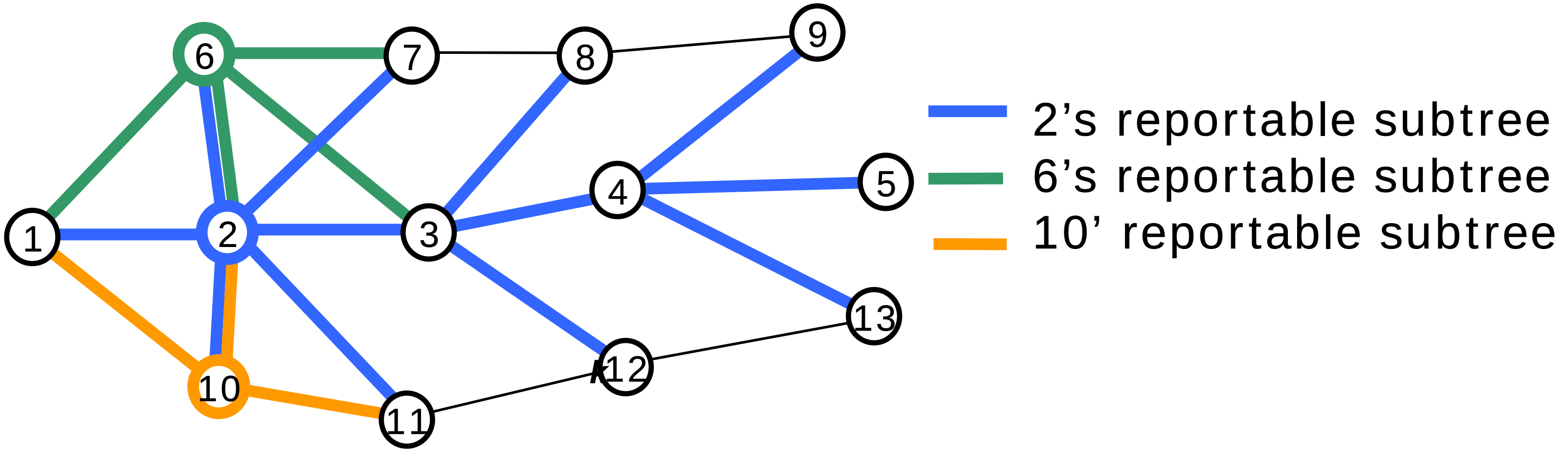
- Proactive link-state routing protocol
- Hop-by-hop routing
- Periodic and differential updates of link states are sent using the source-based spanning tree
- Consists of two modules
  - neighbor discovery module
  - routing module

TBRPF Neighbor Detection (TND)

- Detects neighbor nodes and broken links
- Key features are differential hello messages
  - only changes are reported
  - smaller messages than normal link-state routing protocols
  - messages can be sent more frequently
  - faster detection of changes
- TND runs on each interface of a node
- TND calls a procedure if changes occur to notify the routing module

TBRPF Routing

- By means of a reportable subtree
  - Links to all neighbors



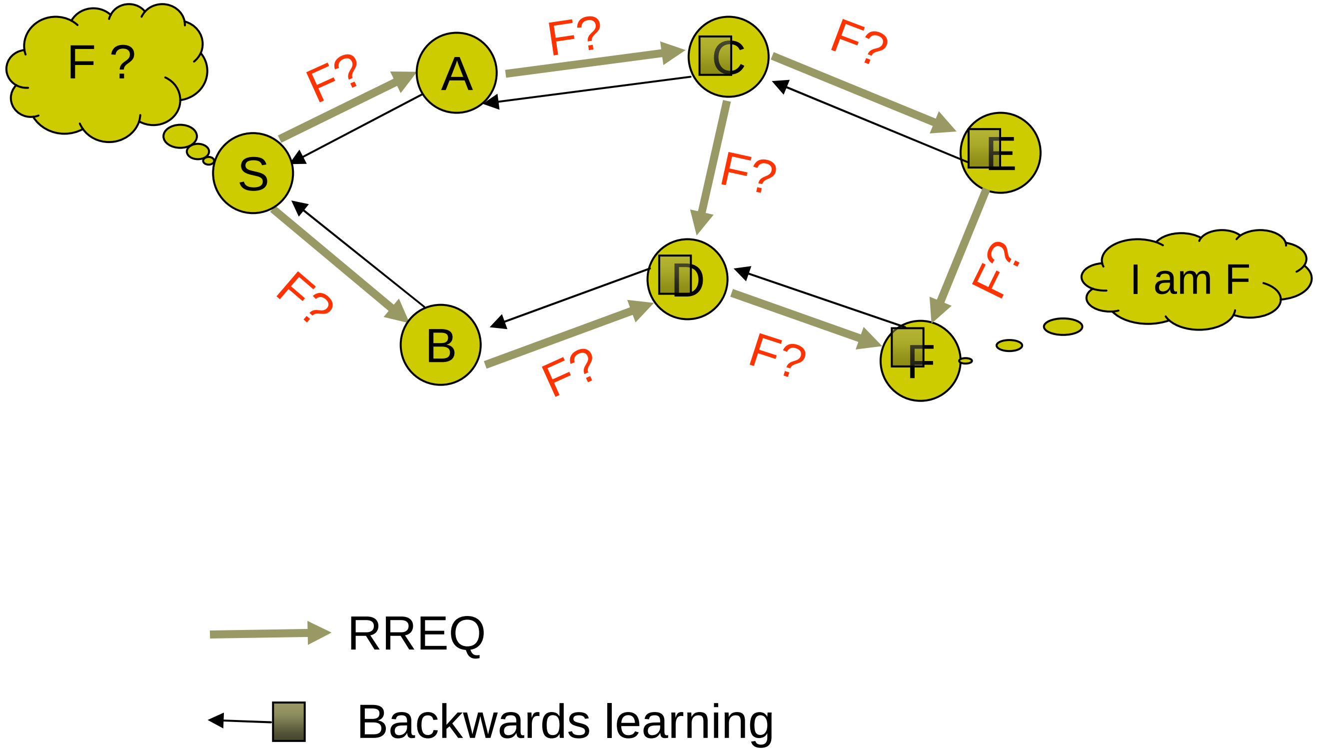
On-demand (Reactive) Routing

- A path is computed only when the source needs to communicate with a destination
- The source node initiates a *Route Discovery Process* in the network
- After a route is discovered, the path is established and maintained until it is broken or is no longer desired

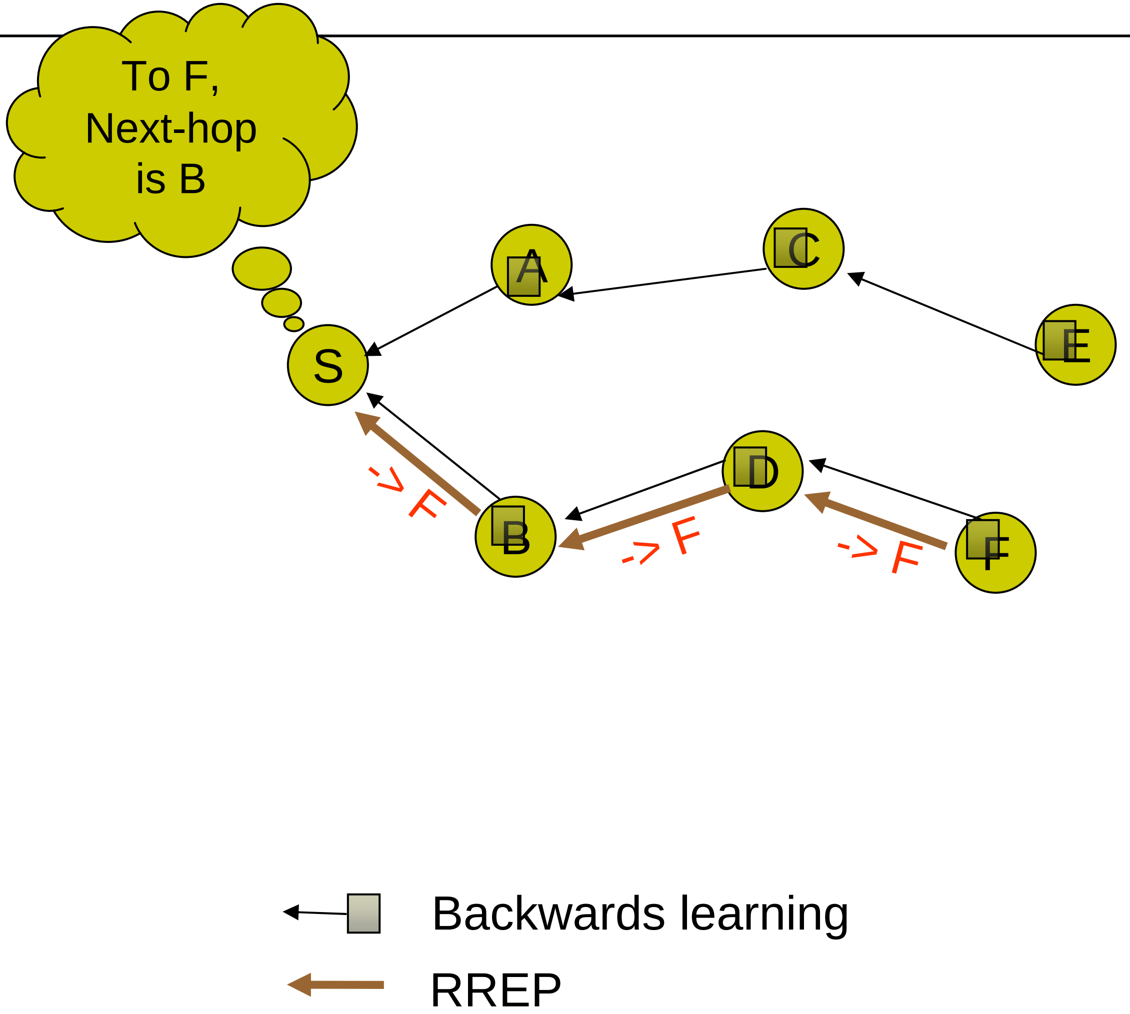
Ad-hoc On-demand Distance Vector Routing (AODV)-1

- When a source desires to send a message to any destination, and if the route table does not have a corresponding entry, it initiates a route discovery process.
- The source broadcasts a route request (RREQ) packet to its neighbors, which in turn, forward it to their neighbors, and so on, until either the destination node or an intermediate node with a valid route to the destination is located.
- The intermediate nodes set of a reverse route entry for the source node in their routing table.
- The reverse route entry is used for forwarding a route reply (RREP) message back to the source.
- An intermediate node while forwarding the RREP to the source, sets up a forward path to the destination

AODV -2



AODV -3



Dynamic Source Routing (DSR)

- On-demand source-based routing approach
- Packet routing is loop-free
- Avoids the need for up-to-date route information in intermediate nodes
- Nodes that are forwarding or overhearing cache routing information for future use
- Two phases: Route Discovery and Route Maintenance

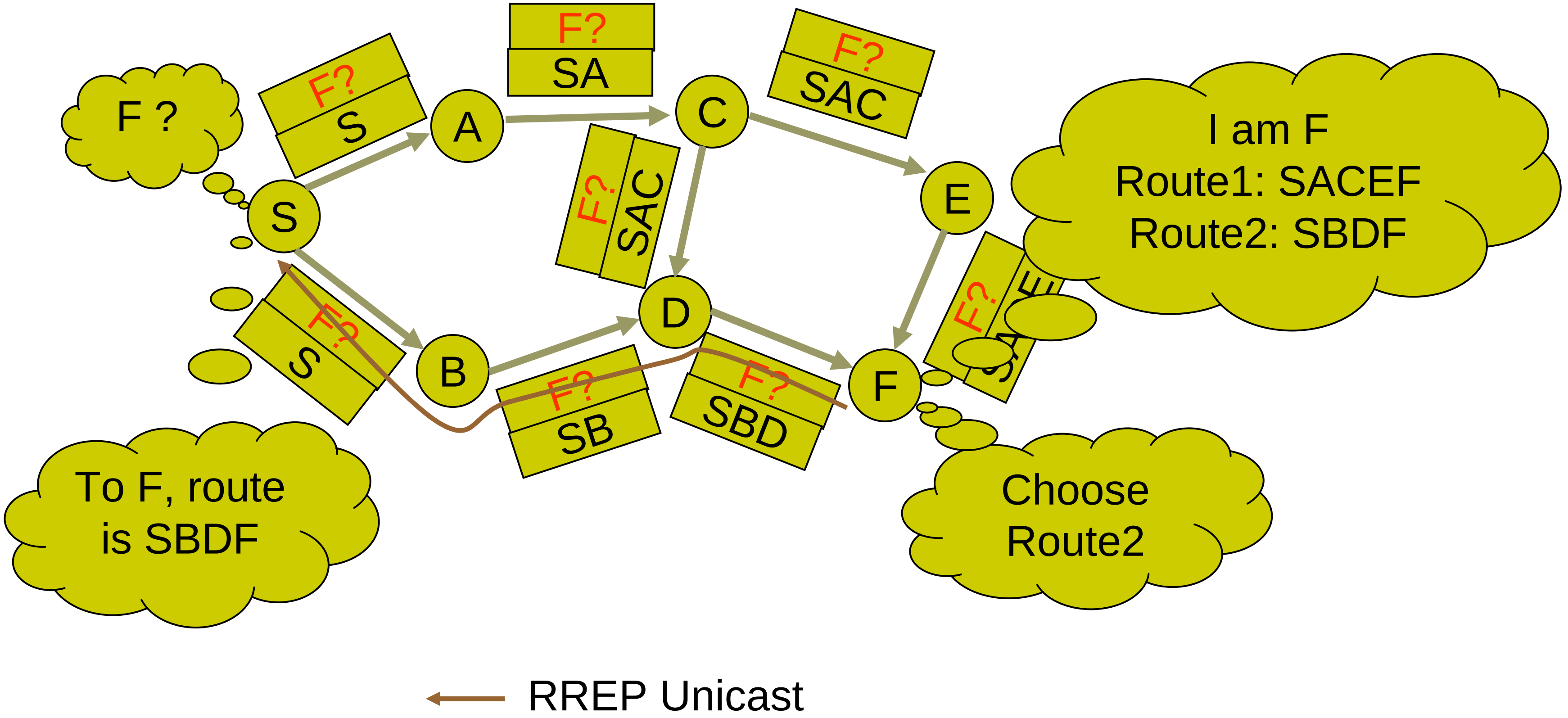
DSR: Route Discovery

- Route discovery is initiated if the source node does not have the routing information in its cache
- The source node broadcasts a route request packet that contains destination address, source address, and a unique ID
- Intermediate nodes that do not have a valid cached route, add their own address to the route record of the packet and forwards the packet along its outgoing links

DSR: Route Reply

- Route reply is generated by the destination or a node that has a valid cached route
- The route record obtained from the route request is included in the route reply
- The route is sent via the path in the route record, or from a cached entry, or is discovered through a route request
- Route maintenance is accomplished through route error packets and acknowledgments

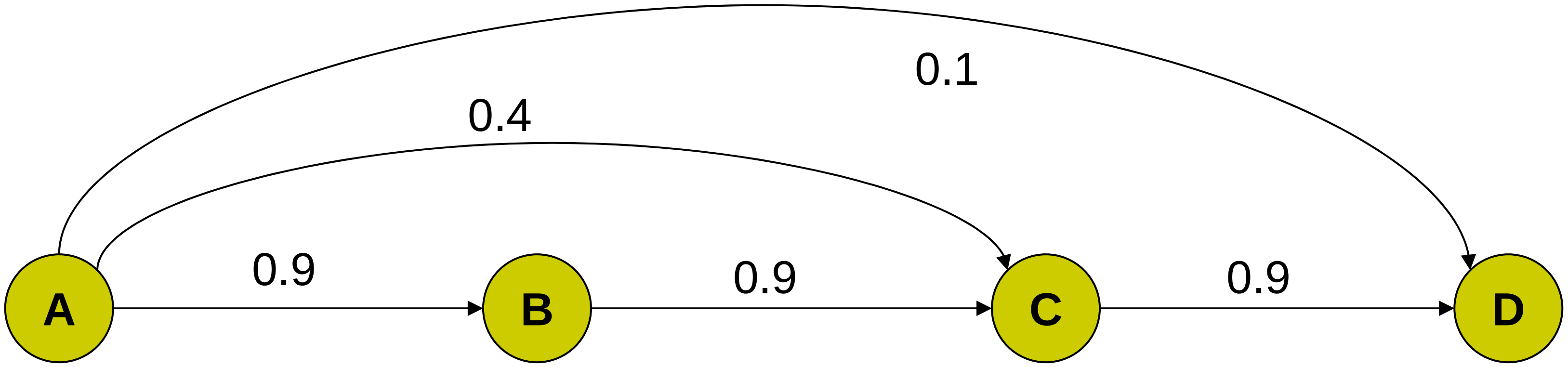
DSR



F ?
F?
S
F?
SA
F?
SAC
F?
SAC
F?
S
F?
SB
F?
SBD
S
A
B
C
D
E
F
I am F
Route1: SACEF
Route2: SBDF
To F, route
is SBDF
Choose
Route2
RREP Unicast

Exploiting Opportunities

- Simple network with delivery ratios



Extremely Opportunistic Routing (ExOR)

- ExOR forwards each packet through sequence of nodes, deferring the choice of each node in the sequence until after the previous node has transmitted the packet on its radio
- ExOR determines which node, of all the nodes that successfully received the transmission, is the closest to the destination; the closest node transmits the packet
- A distributed MAC protocol allows recipients to ensure that only one of them forwards the packet
- An algorithm based on inter-node delivery rates is used to determine which recipient is likely to be the most useful forwarder

Hierarchical Routing

- Hierarchical routing is adopted for large scale networks
- The main characteristic of such routing schemes are:
  - Form clusters and use a routing scheme within the cluster
  - Form a network of the cluster-heads and adopt the same or another routing scheme
  - The inter-cluster routing is facilitated by the network formed by the cluster-heads

Multi-radio Routing

- Advantages:
  - Enables nodes to Tx/Rx simultaneously
  - Network can utilize more of the radio spectrum
  - Multiple heterogeneous radios offer tradeoff that can improve robustness, connectivity, and performance
- In multi-radio routing
  - Shortest path algorithm do not perform well in heterogeneous radio networks
  - Channel selections for the paths have a significant impact

Multi-Radio Link Quality Source Routing (MR-LQSR) Protocol

- Source-routed link-state protocol derived from DSR
- Takes both loss rate and bandwidth of a link into account while considering it for inclusion in the path
- The path metric, which combines the weight of individual links should be increasing
- The path metric should account for the reduction in throughput due to interference among links that operate in the same channel

Routing Performance Metrics

- Metrics:
  - Hop Count – could lead to poor throughput
  - Link quality – all links do not have the same quality
    - Stronger links can support higher effective bit rates and less errors/retransmissions.
    - Interference also can affect link quality.
    - Link quality is proportional to the SINR (Signal to interference and noise ratio)

Hop Count

- Minimum hop counting – the link quality is binary
- Simple and requires no measurements
- Disadvantages:
  - Does not take packet loss or bandwidth into account
  - Route that minimizes hop count does not necessarily maximize the throughput

Per Hop RTT

- Measurement-based average per hop round trip delay with unicast probes between neighboring nodes
- Nodes sends a probe packet and the neighboring node sends and ack with timestamp. Exponentially weighted moving average is maintained at the nodes
- Loss will cause RTT to increase due to ARQ. If ARQ fails, RTT is increased by some percentage.
- This metric is load dependent - Channel contention increases RTT
- Disadvantages:
  - Does not take link data rate into account.
  - High overhead.
  - Load dependent metric may cause route flaps
  - Need to insert probe at head of interface queue to avoid queuing delay
  - Not scalable – every pair needs to probe each other

Per Hop Packet Pair

- Use two back-to-back probes for each neighbor
  - Rectify the distortion due to queuing delay
  - First probe small, second large.
  - Relatively more sensitive to link bandwidth
  - Neighbor measures delay between the arrival of the two probes; reports back to sender.
- Cons:
  - Very high overhead.
  - Load dependent metric.

ETX (Expected Transmission Count)

- ETX provides an estimation of the number of transmissions required to send a unicast packet over a specified link.
- Let the measurement-based probabilities of successful transmissions in the forward and reverse directions of a link be S_f, S_r, respectively, then

$$ETX = \frac{1}{S_f \times S_r}$$

ETX: Measurement Method

- Each node broadcasts probes at a predetermined rate
  - 802.11 does not ack or retransmit broadcast frames.
  - Probe carries info about probes received from neighbors.
- Each node computes the probability of successful transmission in both forward and reverse direction of a link
- The routing protocol finds a path that minimizes the sum of expected number of retransmissions

ETX: Pros and Cons

- Pros:
  - Probing overhead is reduced due to the broadcasting
  - Immune to self-interference – not measuring delays
- Cons:
  - Measuring the successful transmission of small packets at lowest possible data date may not be a good representation of the data packets.
  - Hard to do measurements with probes of different size and rates.
  - Does not directly account for load
  - Focuses only on loss characteristics. Some losses may be dependent on load or data rates

Relative Performance of Metrics

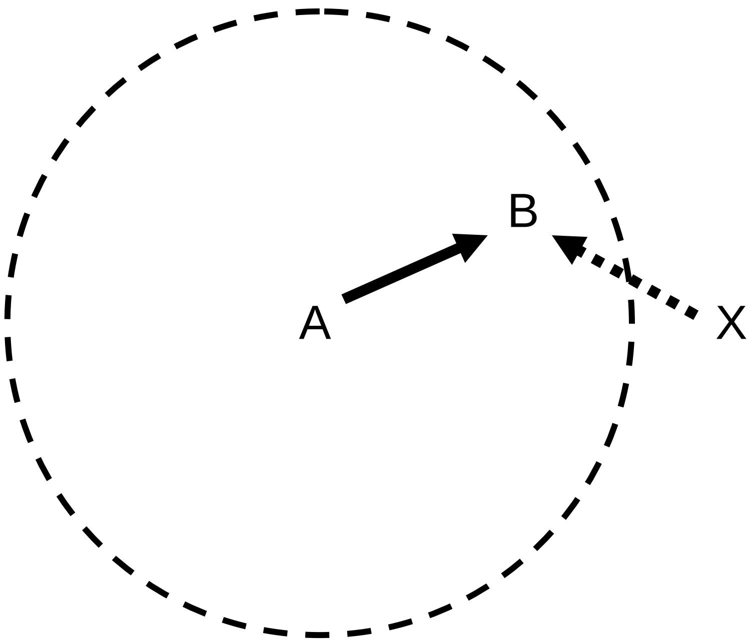
- ETX metric performs best in static scenarios. It is insensitive to load
- RTT is most sensitive to load
- Packet-Pair suffers from self-interference on multi-hop paths.
- Minimum hop count based routing seems to perform best in mobile scenarios
  - Schemes based on measurements of link quality does not converge quickly

5. Medium Access Control

MAC Basics

- Scheduled MAC
- Random Access MAC
- Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA)
  - Problems
    - Hidden terminal problem
    - Exposed terminal problem

Hidden Terminal Problem

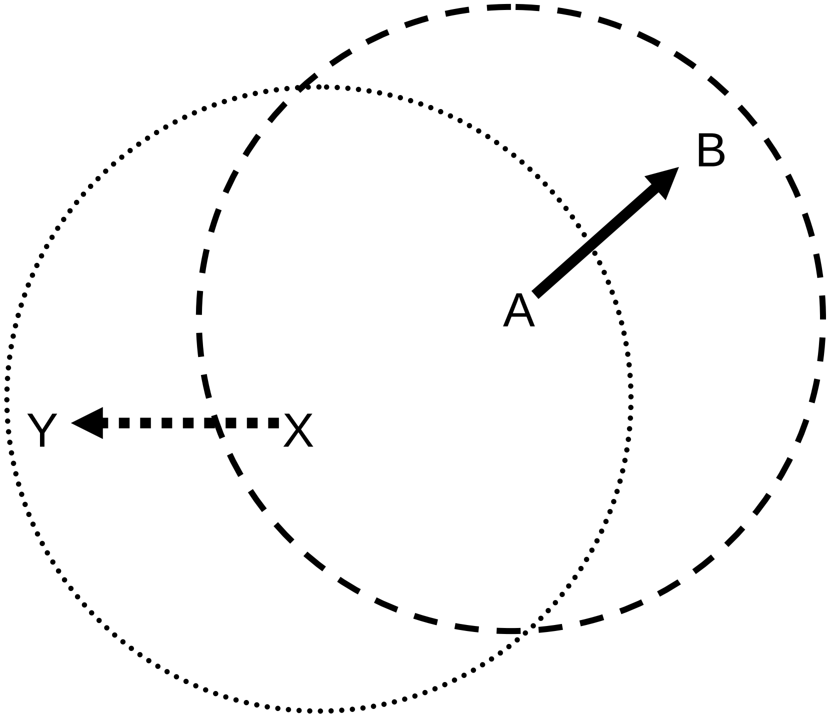


A is transmitting a packet to B

Node X finds that the medium is free, and transmits a packet

No carrier ≠ OK to transmit

Exposed Terminal Problem



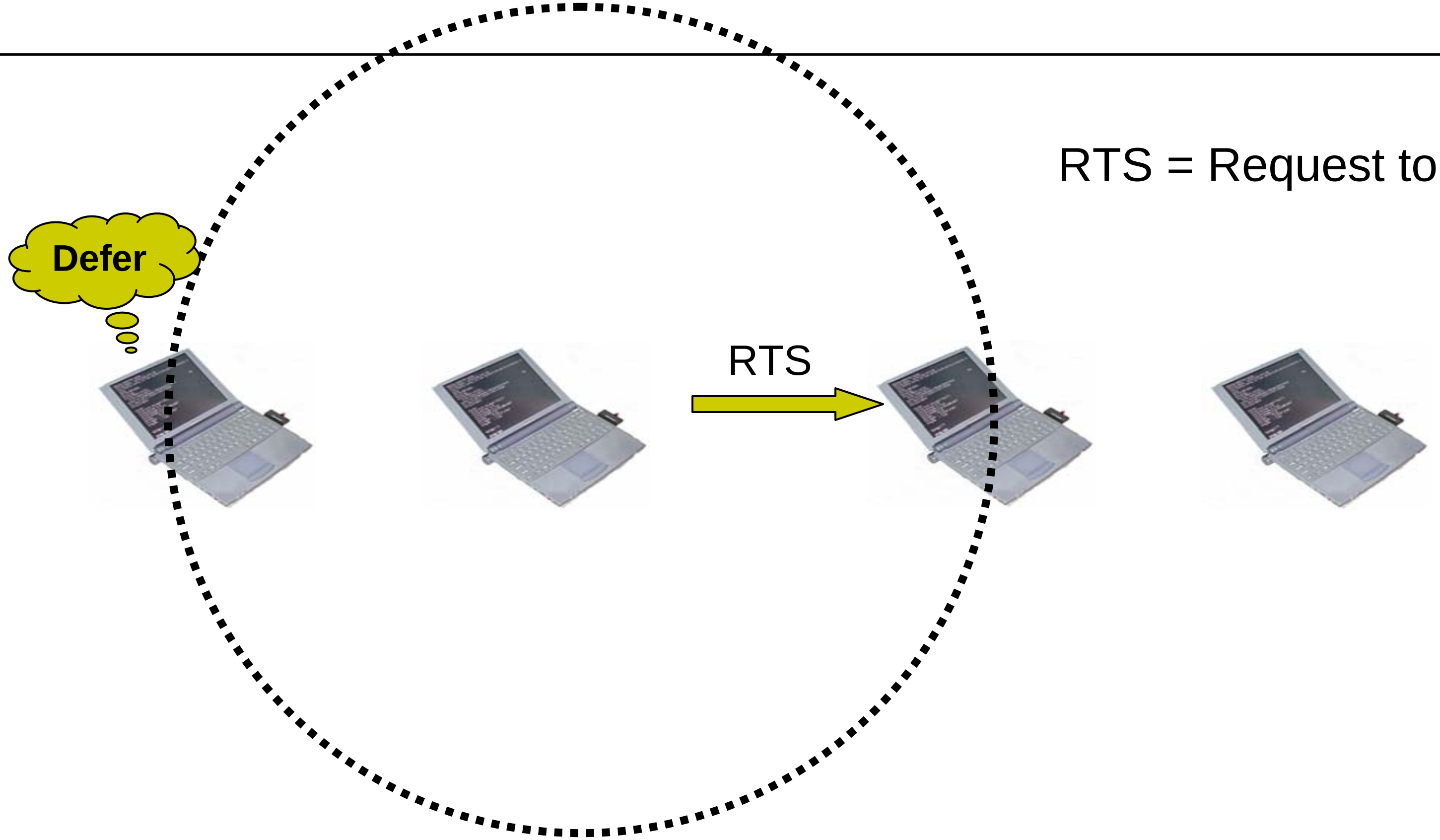
A is transmitting a packet to B

X can not transmit to Y, even though it will not interfere at B

Presence of carrier ≠ holds off transmission

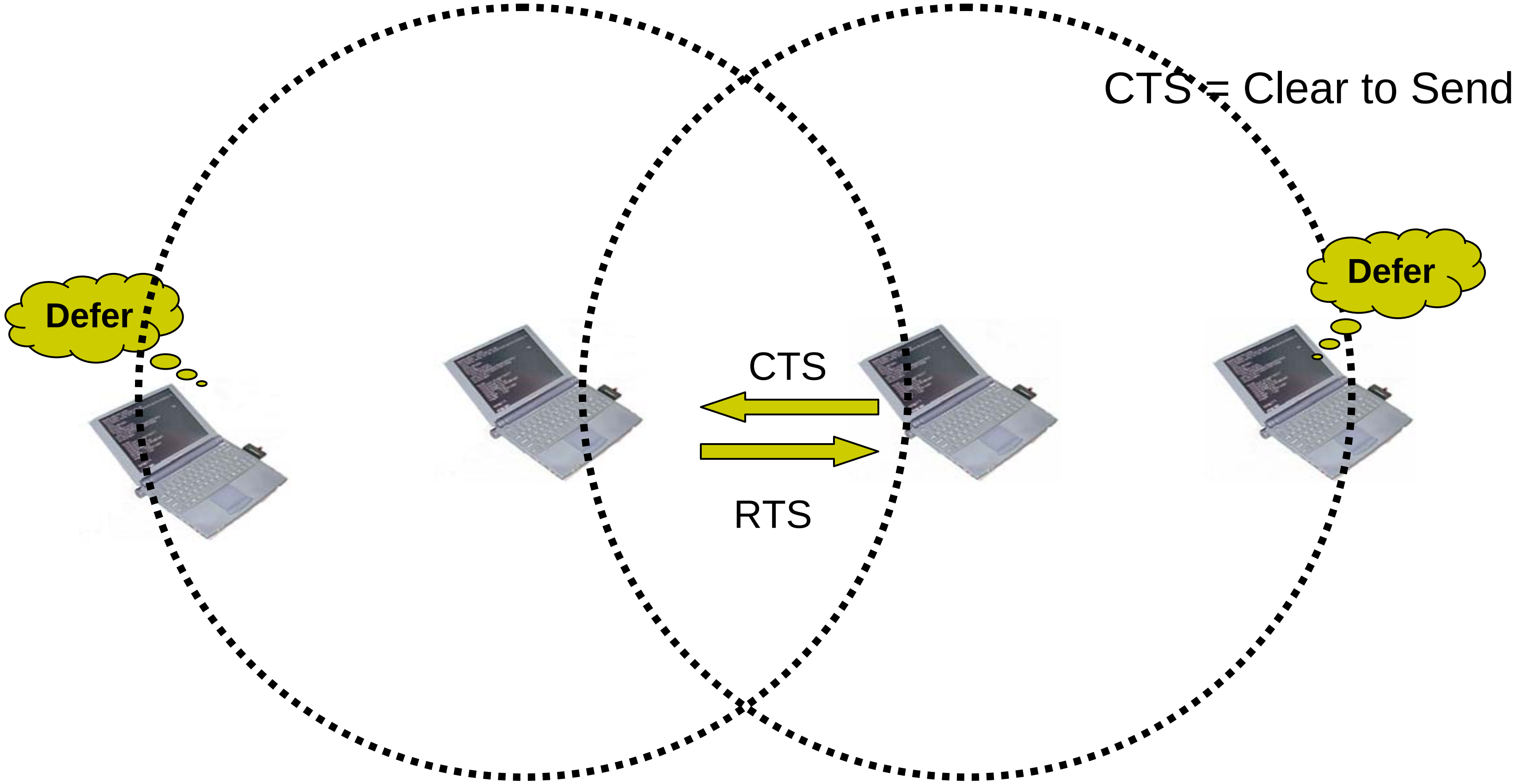
RTS/CTS dialog

RTS = Request to Send



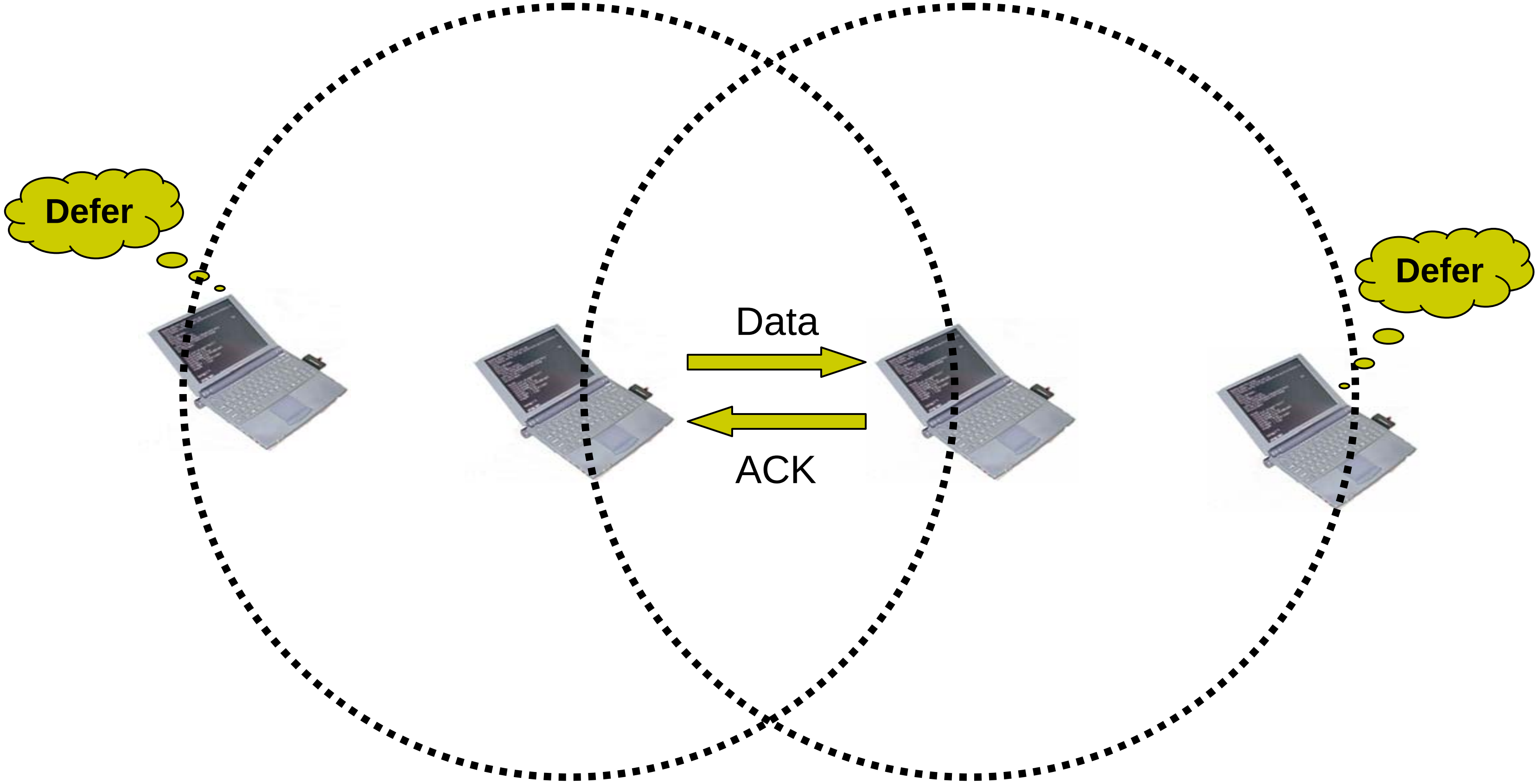
Any node that hears this RTS will defer medium access.

RTS/CTS Dialog



Any node that hears this CTS will defer medium access.

RTS/CTS Dialog



IEEE 802.11 DCF

- Uses RTS-CTS exchange to avoid hidden terminal problem
  - Any node overhearing a CTS cannot transmit for the duration of the transfer
  - Any node receiving the RTS cannot transmit for the duration of the transfer
    - To prevent collision with ACK when it arrives at the sender
- Uses ACK to achieve reliability

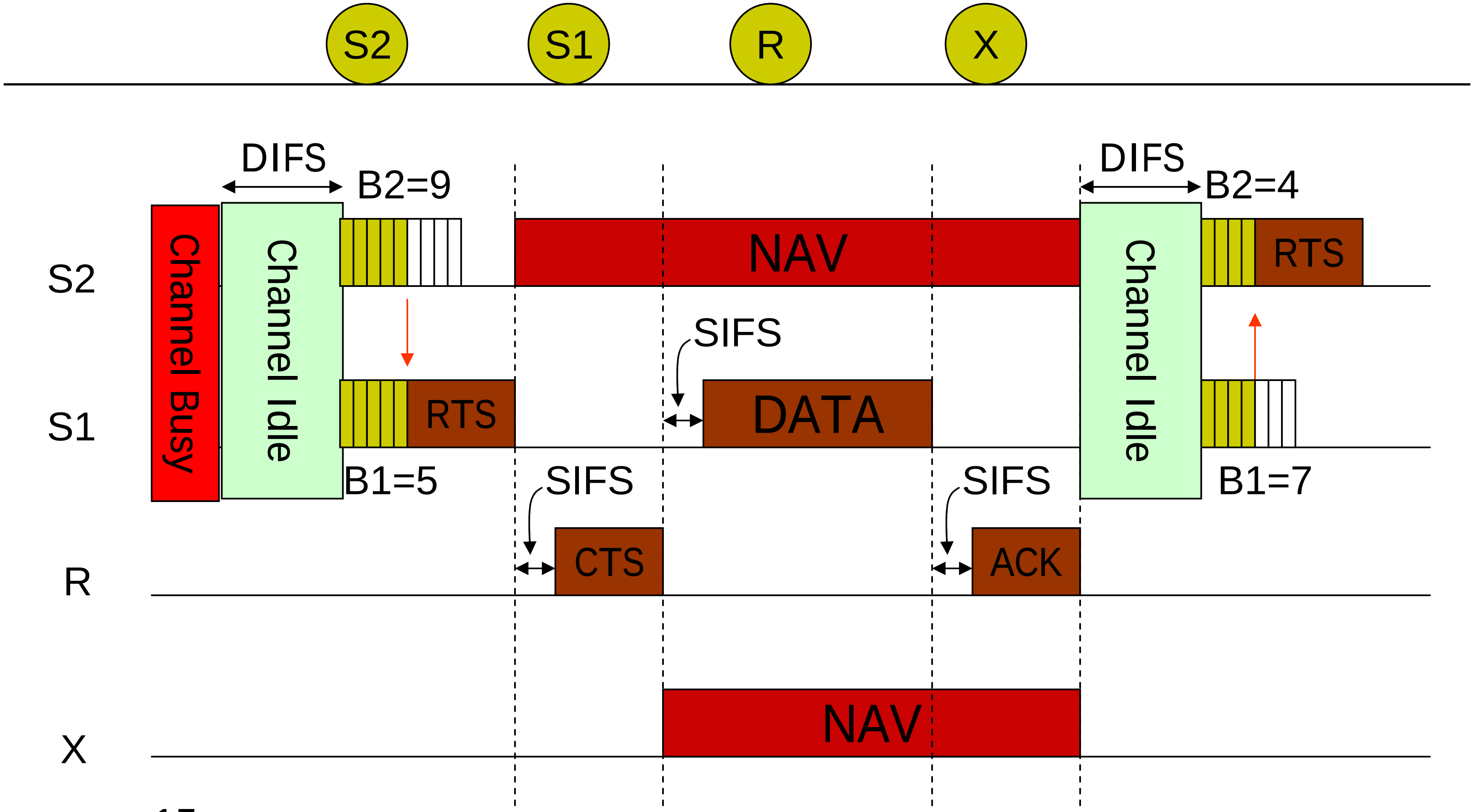
IEEE 802.11 DCF

- CSMA/CA
  - Contention-based random access
  - Collision detection not possible while a node is transmitting
- Carrier sensing in 802.11
  - Physical carrier sense
  - Virtual carrier sense using Network Allocation Vector (NAV)
    - NAV is updated based on overheard RTS/CTS packets, each of which specified duration of a pending Data/Ack transmission
- Collision avoidance
    - Nodes stay silent when carrier sensed busy (physical/virtual)
    - Backoff intervals used to reduce collision probability

Backoff Interval

- When the channel is busy, 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

802.11 CSMA/CA

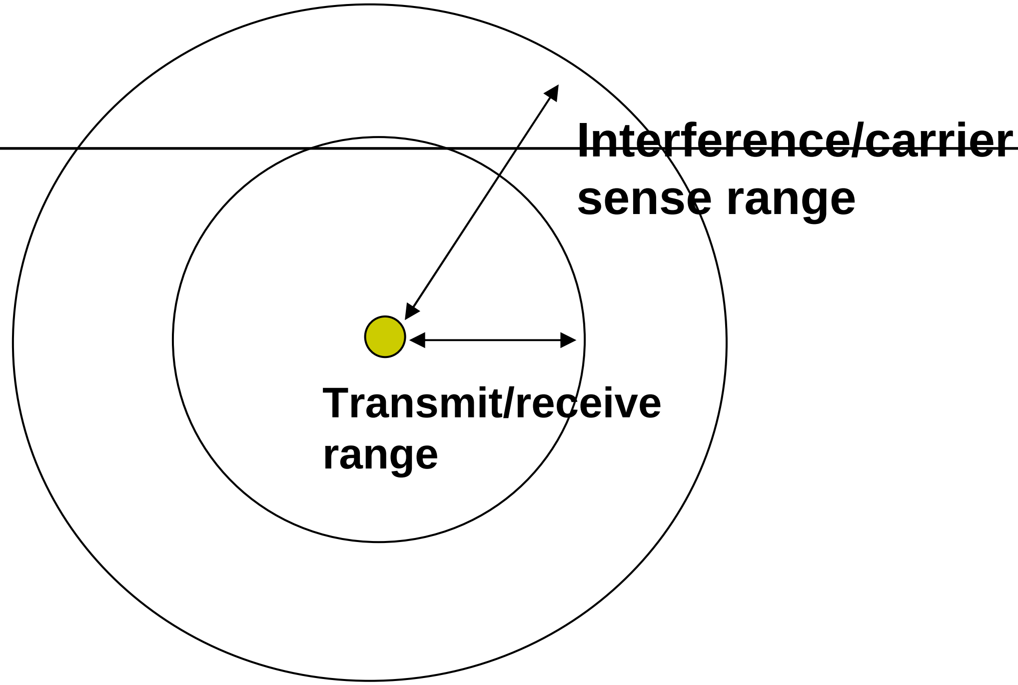


cw = 15

DIFS: DCF Inter-Frame Space

SIFS: Short Inter-Frame Space

More on Interference



- Recall that SINR must be sufficient for successful reception.
- A node can interfere sufficiently at a distance longer than its transmit range.
- Carrier sense threshold is usually adjusted so that the node can sense any potential interferer.

6. Capacity Enhancement

Capacity of Multihop Wireless Networks

- A flow consumes bandwidth at each hop.
  - Also, transmission at each hop interferes with the other hops of same flow.
  - Different flows also interfere.
- Per flow throughput $\leq const \times \dfrac{W}{\sqrt{n \log n}}$
  - Model assumptions: randomly placed n nodes, transmit range sufficient to make network connected, each node has a flow to a random destination.

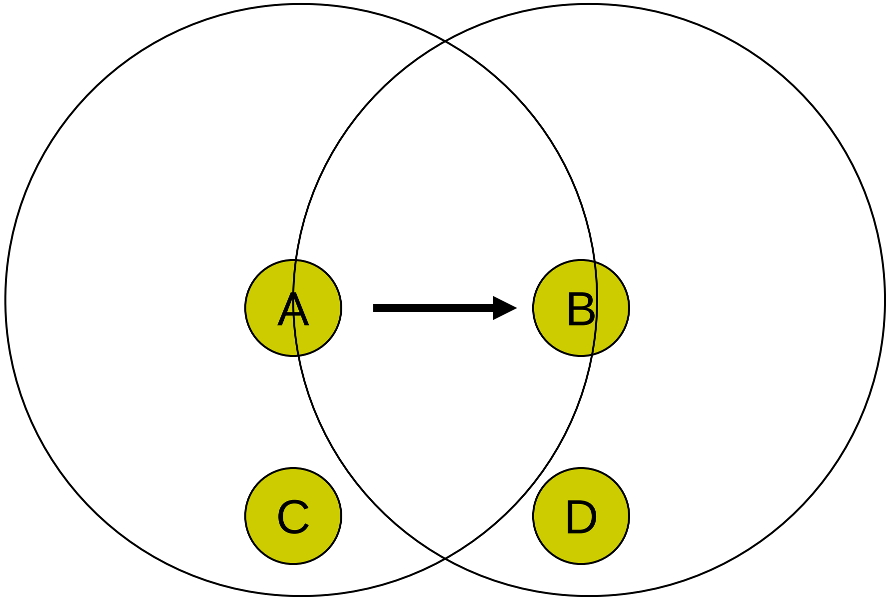
Capacity Enhancement

- Protocol enhancement would provide marginal improvements – shouldn't ignore them though
- Capacity limitation – fundamental
  - Spatial interference
  - Spectrum availability
- Spatial interference: could be handled through effective use of space
  - Directional antenna
  - MIMO
  - Transmission Power Control
- Spectrum availability: enhance channel utilizations
  - Multiple channels
  - Multiple radios

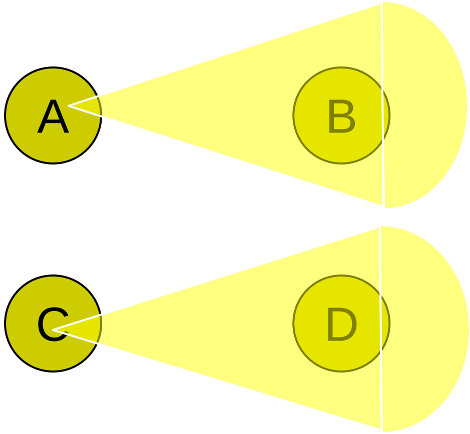
Directional Antenna

- Benefits of Directional Antenna
  - More spatial reuse
    - With omni-directional antenna, packets intended to one neighbor reaches all neighbors as well
  - Increase “range”, keeping transmit power constant
  - Reduce transmit power, keeping range comparable with omni mode
    - Reduces interference, potentially increasing spatial reuse

More Spatial Reuse



Omni-directional antenna



Directional antenna

While A is transmitting to B, C cannot transmit to D

Both A and C can transmit simultaneously

MACs Designed for Directional Antenna

- Most proposals use RTS/CTS dialog
- They differ in how RTS/CTS are transmitted
  - Omni-directional transmit: ORTS, OCTS
  - Directional transmit: DRTS, DCTS
- Current proposals:
  - ORTS/OCTS
  - DRTS/OCTS
  - DRTS/DCTS

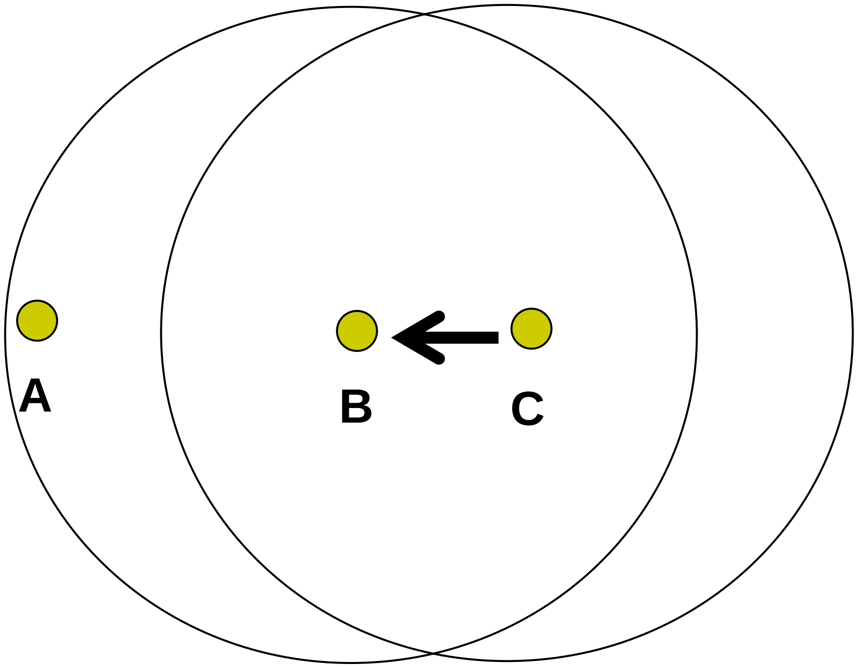
Directional NAV

- Physical carrier sensing still omni-directional
- Virtual carrier sensing be directional – directional NAV
  - When RTS/CTS received from a particular direction, record the direction of arrival and duration of proposed transfer
    - Channel assumed to be busy in the direction from which RTS/CTS received

MIMO

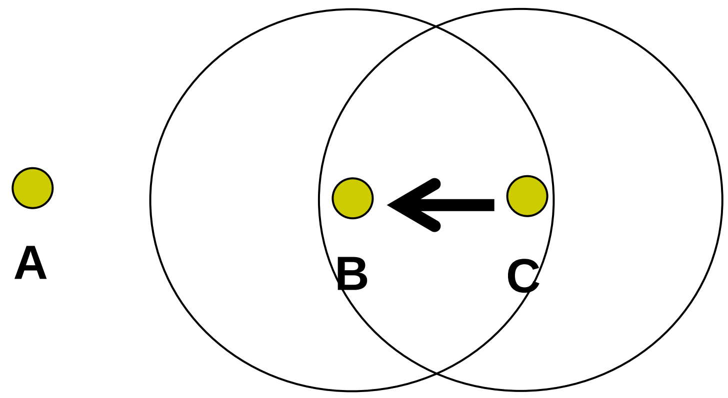
- Multiple Input Multiple Output (MIMO)
  - Multiple antennas at both sender and receiver
- Improved performance and bandwidth efficiency
- Multiple data streams are transmitted over the channel simultaneously
- MIMO signal processing can be done only at the sender, only at the receiver, and at both sender and receiver
- Processing Techniques:
  - Maximum Likelihood Detection (MLD), Vertical Bell Labs Layered Space-Time (V-BLAST), Singular Value Decomposition (SVD), Space Time Coding

Transmission Power Control



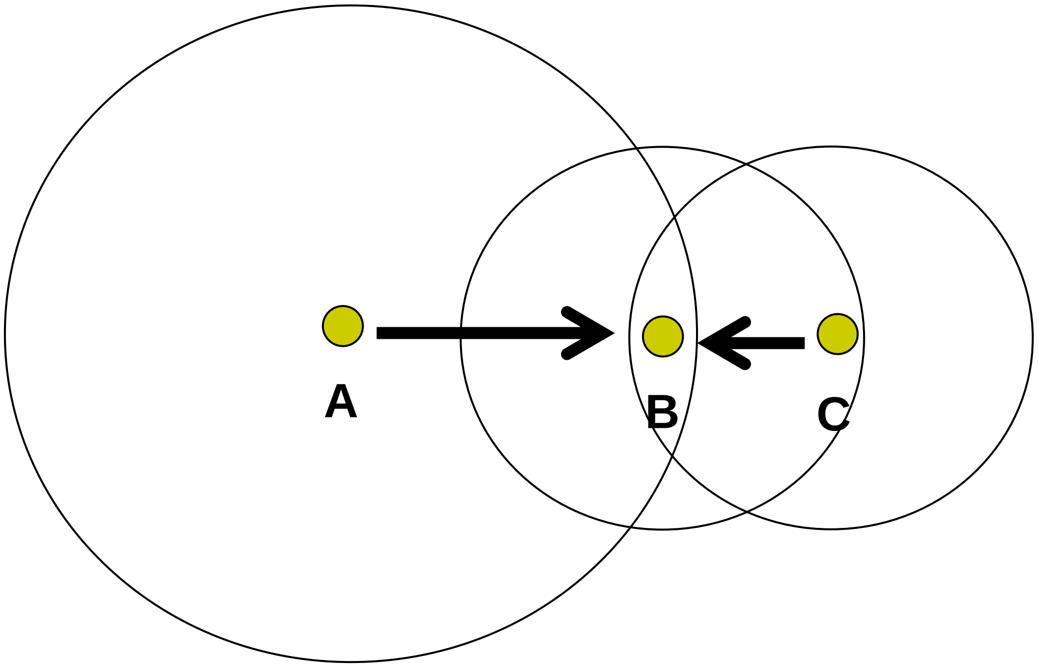
- The transmission power of C can be reduced since B is at a very short distance.

Using Transmit Power Control



- The interference range of C is reduced
- A will no longer sense physical or virtual carrier.

Problem in Transmit Power Control

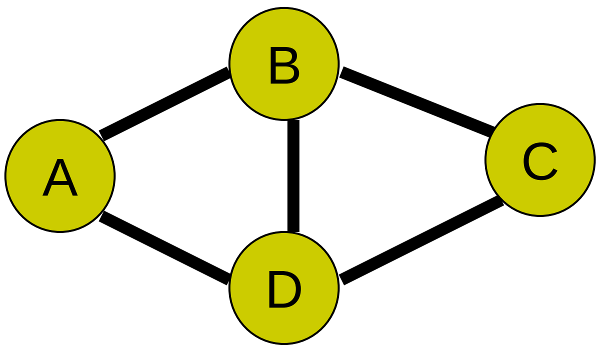


- A could transmit at is normal power creating collision at B

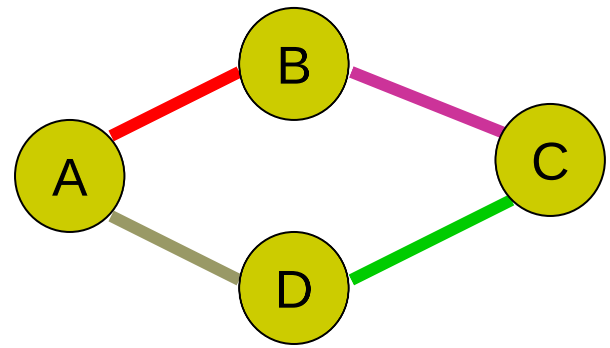
Approaches to Use Multiple Channels

- Number of radio interfaces per node
  - Single
  - Multiple
- Legacy compatibility
  - Use COTS 802.11-based hardware (need multiple interfaces).
  - Use 802.11, but not COTS hardware.
  - Minor extensions to 802.11.
  - Almost new protocol.
- Channel assignment
  - Static (need multiple interfaces).
  - Dynamic (switch channel in packet time-scale).

Channel Assignment Problem



1 channel
1 interface



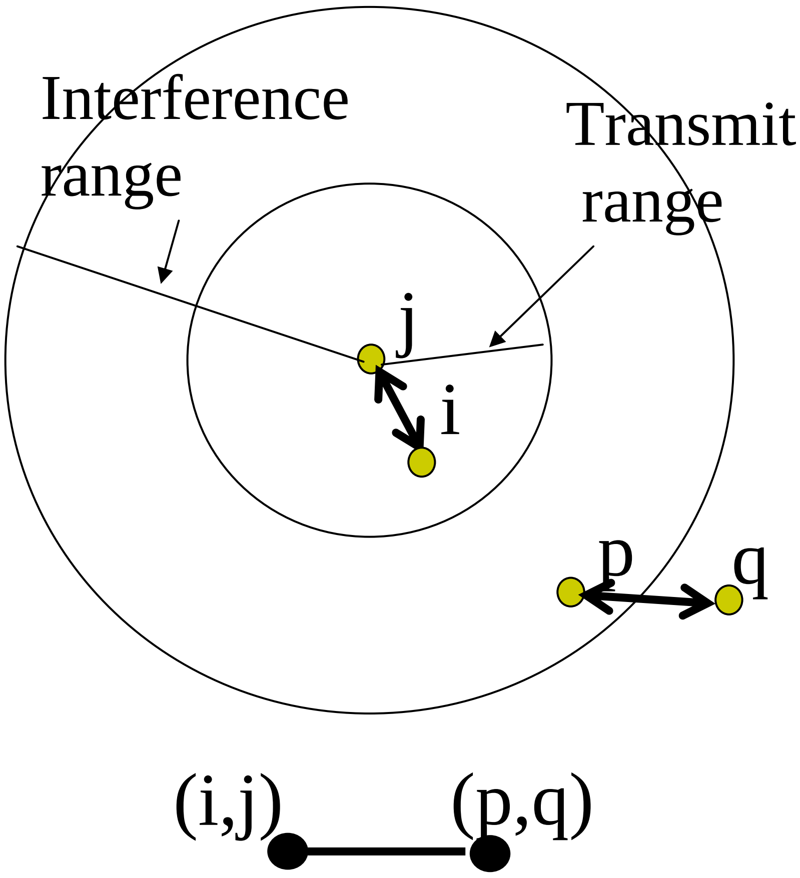
4 channels,
2 interfaces

- Channel assignment can control topology.
- Two nodes can communicate when they have at least one interface in common channel.

Channel Assignment Problem

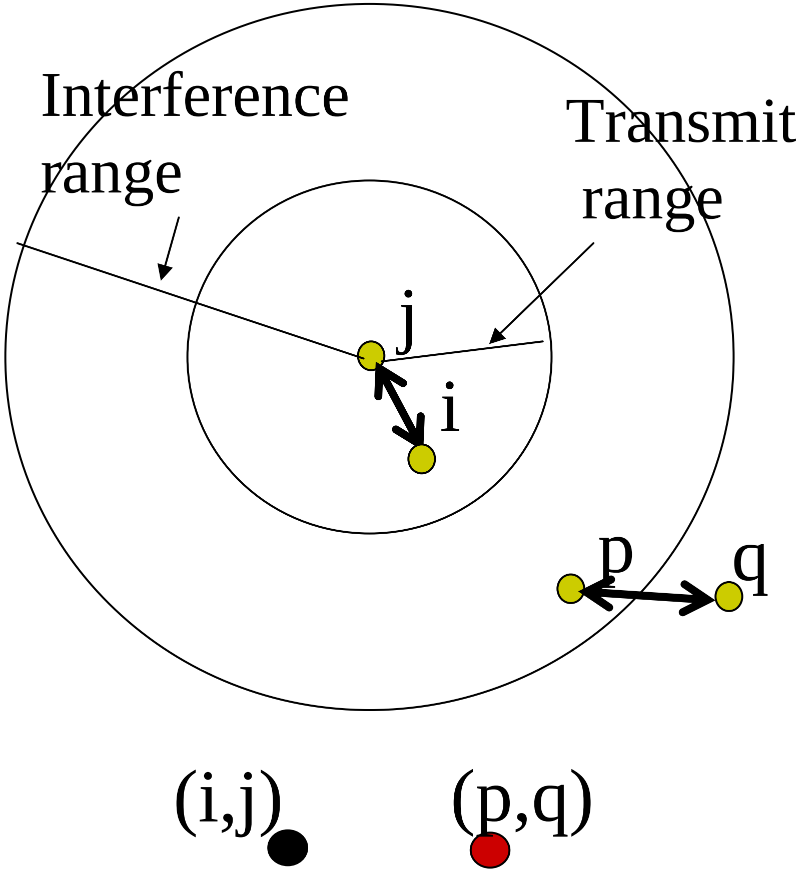
- Similar to a graph coloring problem, except that ..
  - We are given some number of colors (channels).
  - We are looking for coloring with least conflicts.
- Need to model interference.

Representing Interference



- Use conflict graph.
- Link in network graph = node in conflict graph.
- Edge in conflict graph denotes "interference."

Representing Interference



- Use conflict graph.
- Link in network graph = node in conflict graph.
- Edge in conflict graph denotes "interference."

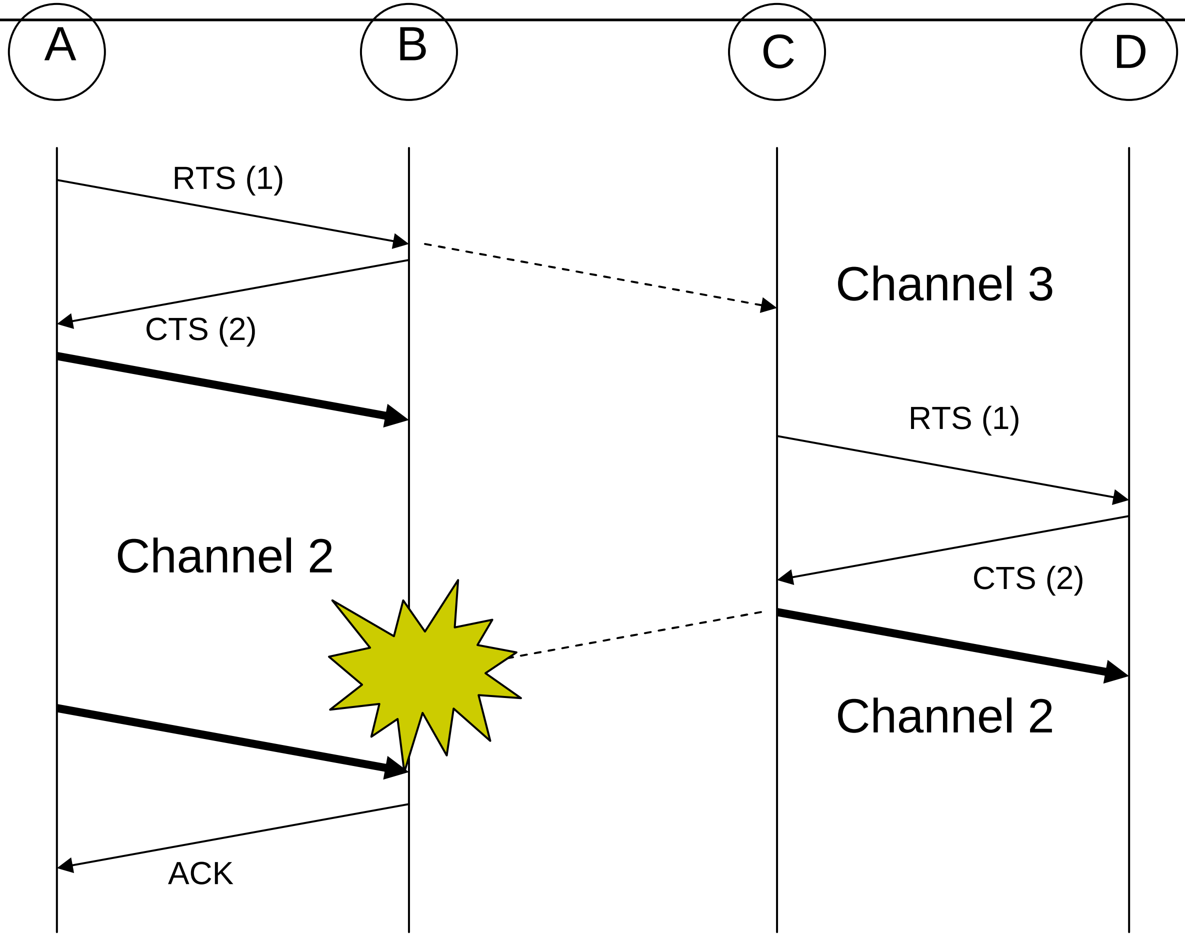
Channel Assignment Problem

- k channels (colors). r ($r < k$) interfaces on each network node.
- Assign colors to ALL nodes in the conflict graph such that the max degree is minimized.
  - Average degree, max. independent set are good metrics.
- Constraint: total no. of colors at a network node <= r.
- NP-complete problem. Heuristic approaches in literature.

Joint Channel Assignment and Routing

- We considered a channel assignment technique that is “topology preserving”
  - Assigns channels to all links that exist in a single channel network.
- Not necessary. Some links can be “routed around.”
  - Conflicts can be “weighted.”
- Solve channel assignment and routing jointly in a network flow maximization framework.

Multi-channel Environment



Issues with Single Radio and Multi-Channel Schemes

- Sender switches to the channel to use. Easy.
- Receiver must know what channel to switch to in order receive. Hard.
- Detecting interferences on other channels
- Several broad approaches:
  - Set up recurring appointments.
  - Negotiate channel before transmission.
  - Receive always on a pre-determined channel.

Setting up Recurring Appointments

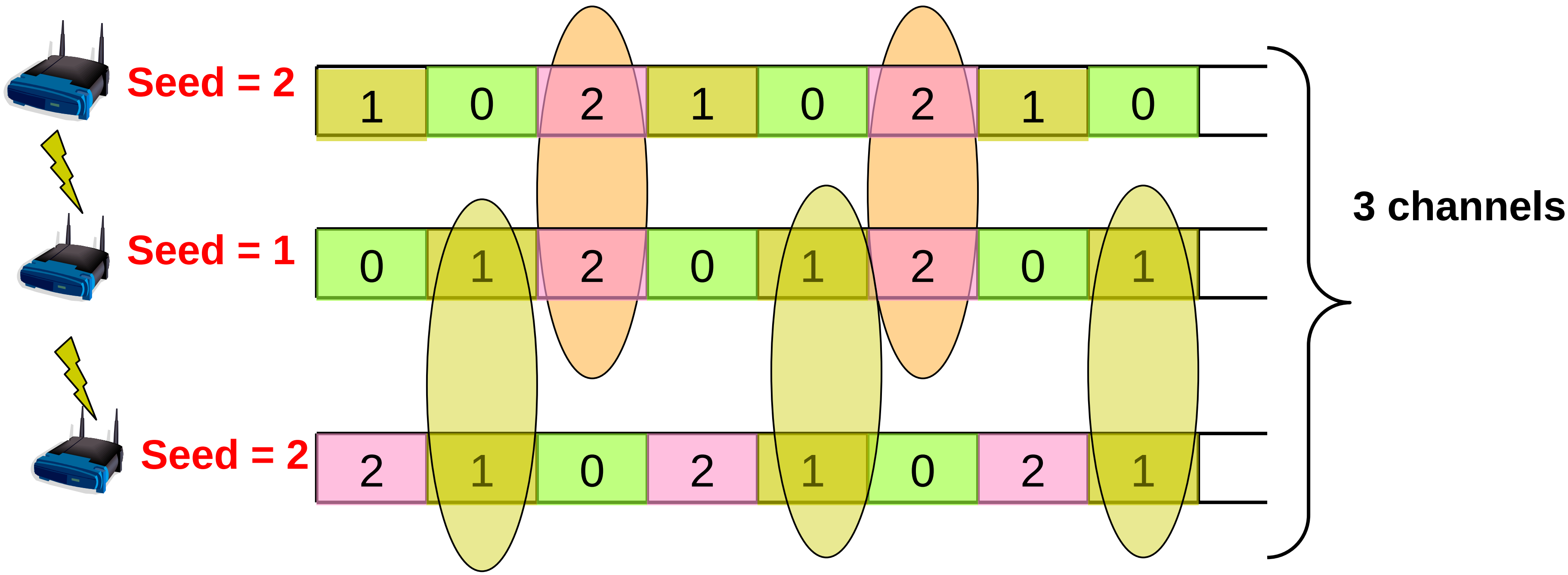
- Each node switches channels synchronously in a pseudo-random sequence so that all neighbors meet periodically in the same channel.
- Spreads usage over all channels.
- No rendezvous to select channels.
- Can use 802.11.
  - But interfaces must be capable of fast synchronous channel switching.

SSCH: Slotted Seeded Channel Hopping

Divide time into slots: switch channels at beginning of a slot

New Channel = (Old Channel + seed) mod (Number of Channels)

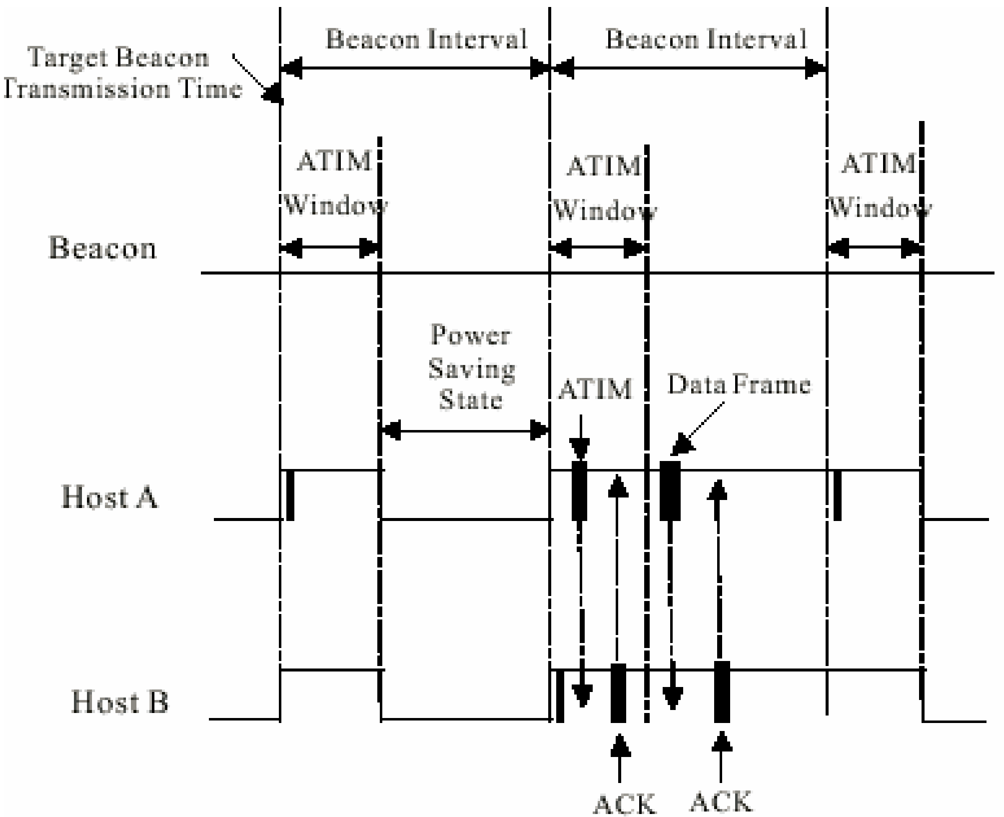
seed is from 1 to (Number of Channels - 1)



Negotiate Channel Before Transmission

- Two approaches.
- Meet periodically at a pre-determined channel to negotiate channels for the next phase of transmissions.
  - Can use minor variation of 802.11.
- Use a separate control channel and interface.
  - Need new MAC protocol.

PS Mode in WLANs



- After the beacon, host can send a direct ATIM frame to each of its intended receivers in PS mode.

- After transmitted an ATIM frame, keep remaining awake

- On reception of the ATIM frame, reply with an ACK and remain active for the remaining period

- Data is sent based on the normal DCF access.

Multi-channel MAC (MMAC) Protocol

- Each node maintains a preferred channel list (PCL) – high, mid, low
- Periodically transmitted beacons divide time into beacon intervals
- A small window called ATIM window is placed at the start of each window
- All nodes listen to a default channel during ATIM window

Protocol:
Sender (S) and Destination (D)

- S sends an ATIM packet including its Preferred Channel List (PCL)
- D selects channel based on the received PCL and own PCL
- D sends an ATIM-ACK packet to S including the channel information
- S sends an ATIM-RES packet if acceptable
- Neighboring nodes update their PCL
- S and D switch to the selected channel and start communicating

Multiple Radio MAC Protcocols

- Single node transmits over multiple channels without channel switching
- Multiple MACs coordinate their respective PHY
- Virtual MAC may be used to coordinate the independent radios
- Examples: Multi-Radio Unification Protocol (MUP)

Multi-radio Unification Protocol (MUP)

- MUP is implemented in the link layer, exposing a single virtual MAC address
- Channel assignment is hard-coded
- MUP uses a channel quality metric for channel selection; channel quality is determined through probe messages
- Neighbor discovery and classification is done by ARP, channel selection (CS), and the MUP table

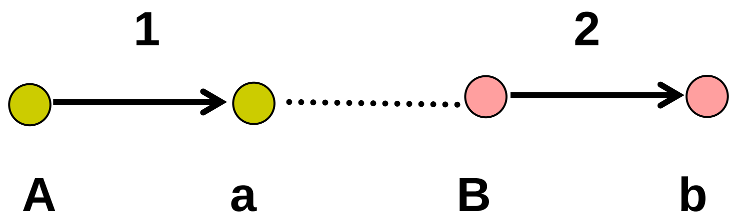
Control Channel Approach

- Form a control channel using a single dedicated radio per node
- Negotiate channels for data communication using this dedicated channel
- Virtual carrier sensing is also done over this channel

Other Problems with 802.11-based Mesh

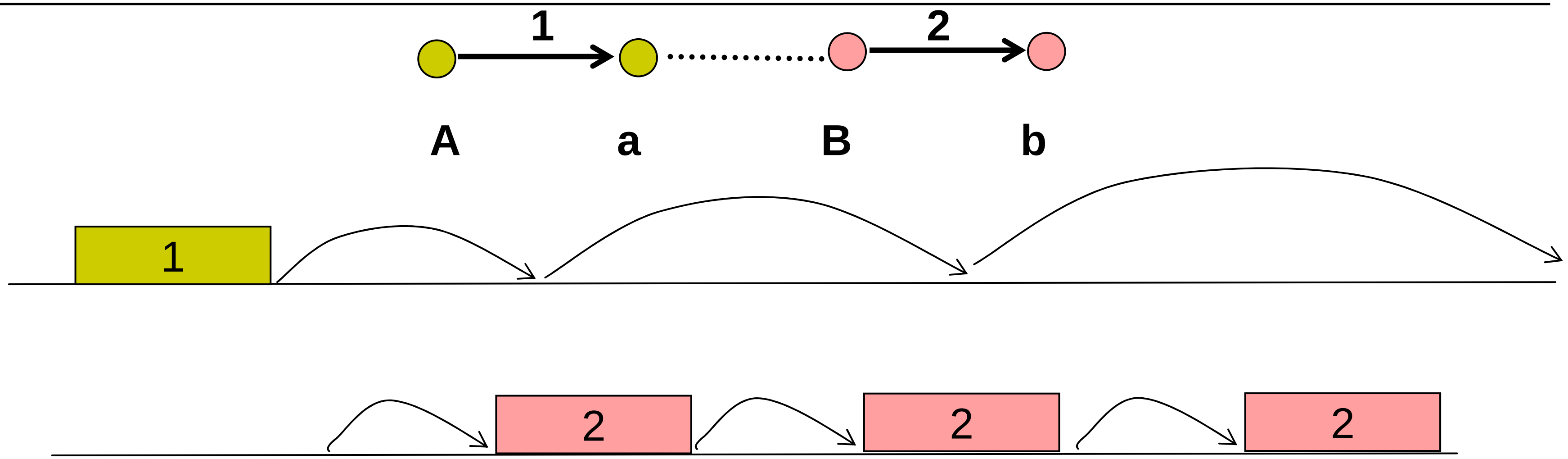
- Fairness at the MAC level
- Interference levels are different at different links.
  - Because neighborhoods are different.
- Two basic problems:
  - Information asymmetry.
  - Flow in the middle problem.

Information Asymmetry



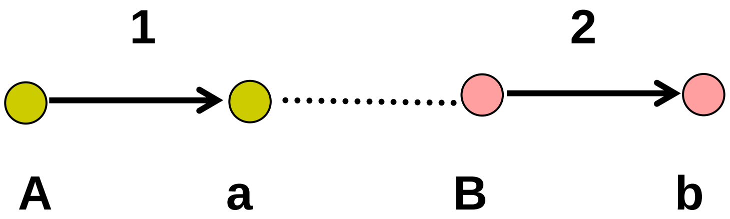
- The senders of two contending flows may have different sets of information.
- Example:
  - Sender of flow 2 is aware of flow 1 (via CTS)
  - Sender of flow 1 is not aware of flow 2.

Information Asymmetry



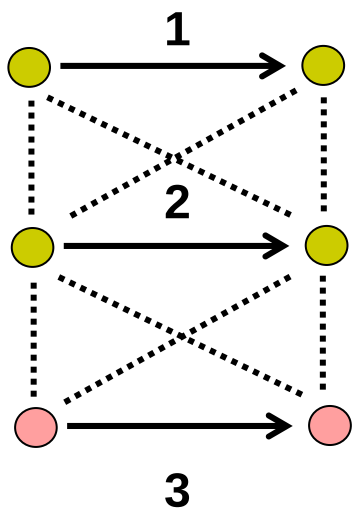
- Flow 2 knows how to contend.
- Flow 1 is clueless – it is forced to timeout and double its contention window.
  - Eventually may be forced to drop packet.
  - Large access delay may also cause overflow in the interface queue.

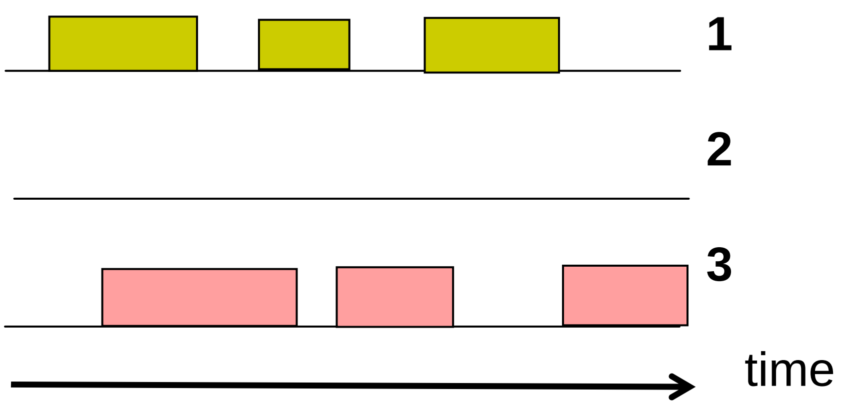
Information Asymmetry



- Happens even when RTS/CTS are not used.
- Flow 1 collides at a. Flow 2 is successful.
- Upstream links still suffer.
- Information asymmetry can be solved by receiver-initiated protocols.
  - Receiver "invites" transmissions when free.

Flow-in-the-Middle Problem





- A flow (2) contends with several flows (1,3) that do not contend with each other.
  - Typically a flow in the middle.
- May suffer from lack of transmission opportunity.

7. Quality of Service (QoS)

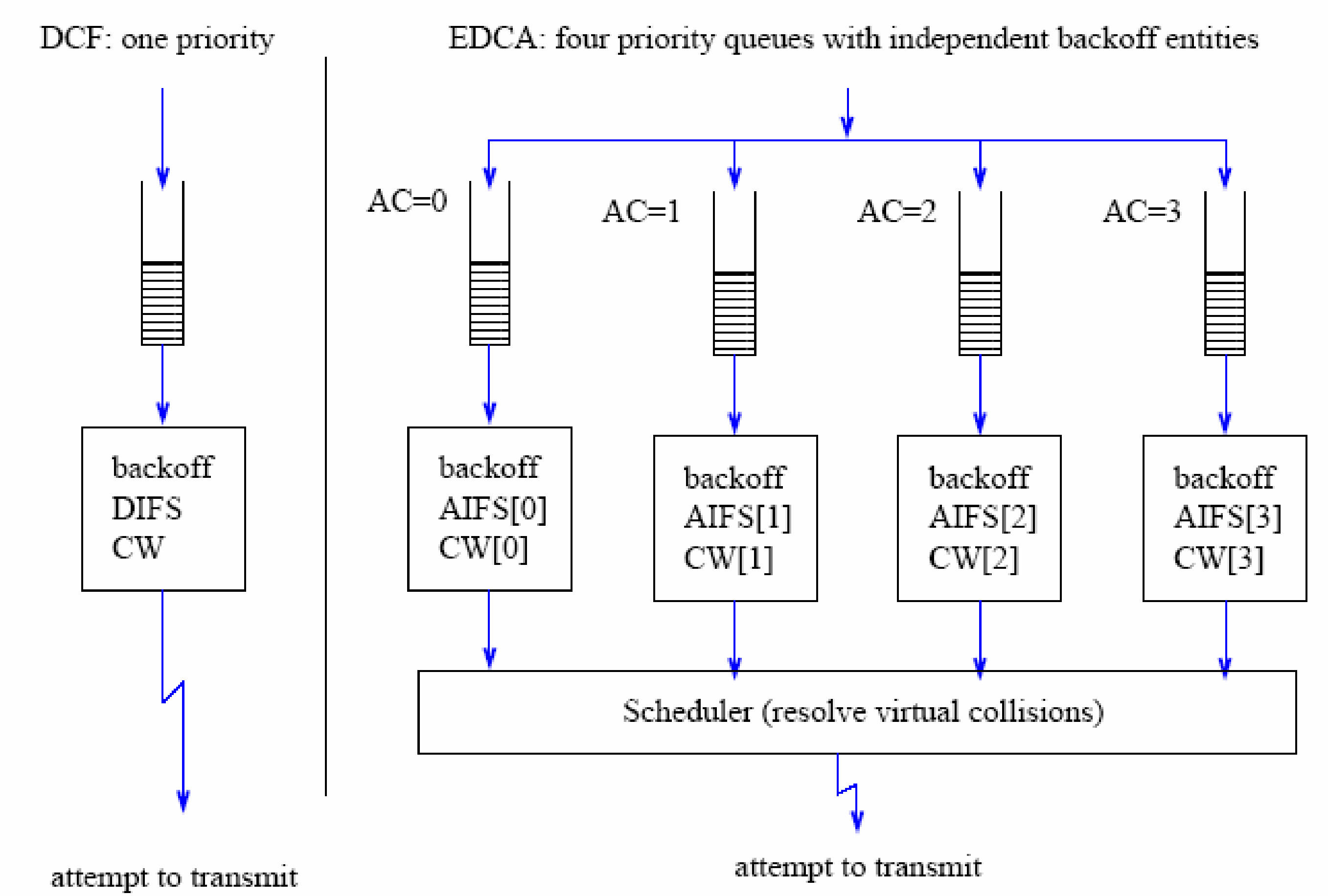
QoS Support in Wireless Mesh

- Evolving applications like media streaming and VoIP would need support for QoS
- IEEE 802.11e extension for Multihop Mesh
- For random access MAC
  - Admission control
  - Scheduling flows
    - Hop-delay budget
- For scheduled MAC
  - Link activation schedule
  - Flow-schedule

IEEE 802.11e EDCA

- 802.11e is proposed to enhance QoS support in WLAN
  - E.g.: QoS support in home networking
- 802.11e defines two modes: HCCA and EDCA
  - HCCA: HCF controlled channel access
  - EDCA: enhanced distributed channel access
- EDCA
  - Introduce four different access categories (ACs)
  - Each AC has own queue and backoff entity
  - Different backoff entity uses per AC contention parameter set
    - AIFS[AC]: arbitration interframe space
    - CWmin[AC] < = CW[AC] < = CWmax[AC]
  - Statistically: higher priority AC will wait for less time and thus go first

DCF v.s. EDCA


DCF: one priority
EDCA: four priority queues with independent backoff entities
AC=0
AC=1
AC=2
AC=3
backoff
DIFS
CW
backoff
AIFS[0]
CW[0]
backoff
AIFS[1]
CW[1]
backoff
AIFS[2]
CW[2]
backoff
AIFS[3]
CW[3]
Scheduler (resolve virtual collisions)
attempt to transmit
attempt to transmit

Extending IEEE 802.11e for Multihop Mesh

- 802.11e is designed for single hop environment
  - Provide single hop service differentiation
  - Has no notion of end-to-end assurance
- How can we extend 802.11e into multihop networking environments?

- What if we can break down end-to-end requirement into per hop requirement (per-hop budget)?
- If so, how to allocate proper portion of budget for a specific hop?
  - Sender-based, evenly divided?
  - Per hop based, adaptively adjusted?
- How to populate per hop budget to intermediate hop nodes?
- At each hop, how to map per-hop budget into a proper service class?
- A proposal: Adaptive Per Hop Differentiation (APHD)

APHD: Overview

- Assume proper Admission Control is in use
  - APHD focuses on per hop priority adaptation to achieve end-to-end requirement
- Inter-layer design approach
  - Information is shared among multiple layers
  - Actions take place at multiple layers to do one task
- Localized and distributed
  - Decision making is per packet, per node
- Efficient network utilization
  - Only raise packet's priority level when needed
- Individual nodes monitor
  - per class delay: PCD[AC]
- Per hop based priority adaptation
  - Matching: per-hop budget ←→ PCD[i]

TDMA-based Scheme for QoS Provisioning in Wireless Mesh

- Integrated scheme for admission control, routing, and flow scheduling
- Flow-based scheduling does not cause unfairness problem as observed in hop based scheduling
- We adopt centralized scheduling approach
- The Admission Controller and Scheduler (ACS) is maintained at a gateway node or a switch/server

Link Scheduling

- The channels are assigned statically
- A multi-channel conflict graph (MCG) is created; the nodes represent links and the edge denote the conflict
- The MCG is used to derive the TDM schedule of the communication links, called link activation schedule (LAS)
- The LAS is maintained at the ACS
- Using the MCG, the ACS derives an LAS (statically or periodically) that maximizes the link utilizations while avoiding conflicts
- In every time slot schedule an independent set of nodes in the MCG
- Goals:
  - Maximize the number of links scheduled in each of the time slots – improves throughput
  - Minimize the TDM frame length – reduces per-hop latency

Scheduling Flows

- The deadline is determined in terms of time slots.
- Flows are scheduled in different time slots in each of the TDM frames using to LAS such the scheduled is completed before the deadline
- The LAS and the flow-schedule are mapped on to an array called Current Schedule Status Array (CSSA)
- CSSA shows the TDM schedule of the channel activations at the links in different time slots as well as the flow-schedules in the TDM frames
- Note: LAS is determined statically, whereas flow-schedule is determined dynamically.

8. Security & Management

Security in Wireless Mesh

- Why have a Secure Wireless Mesh ?
  - Distributed, Wireless Access points easily compromised
  - User and network data may be valuable to owner and for the operation of the network
  - As an access network, must provide reliable service
- Levels of Security ?
  - Protection of User Data
  - Protection of Network Data

Security in Wireless Mesh

- User Data Protection
  - Client to Access Point Encryption
  - Authentication of Access Points and Clients to verify each other's identity
- Current Technologies:
  - Layer 2: 802.1X Port Based Network Access Control
  - Higher Layers: IPSec, application-level encryption

Security in Wireless Mesh

- Network Data Protection
  - Avoid “Man in the Middle” Attacks
    - Insertion of data by a third party in the wireless network
  - Encrypted routing and network data transfers between Access Points (Secure Routing)
  - Secure Key Distribution for Mesh for encryption
  - Access Point Authentication and Authorization to prevent malicious Access Points

Network Management in Wireless Mesh

- Why use Network Management ?
  - Not a static topology.
  - Devices, links, paths and protocols fail
  - Users generate varying traffic
- What does Network Management consist of ?
  - Network Monitoring
  - Network Configuration

Network Management in Wireless Mesh

Physical MAC	Device Statistics, Radio Quality, Noise
Network	Neighbor Connectivity Packet Drops, Congestions
Transport	Flow Characteristics

Network Monitoring

- Use SNMP, CMIP or other Information Management Protocol for tallying and communicating between devices
- Monitor Per Device, per Radio, per Neighborhood Information

Network Management in Wireless Mesh

User	Mobility and Handoff, Load Balancing between AP
Network	Routing and Path Information
Failure	Automatic Recovery, User/Administrative Notification

Network Configuration

- Using monitored information, either let the network administrator make network changes, or automatically generate new topology or parameters to mitigate bad behavior

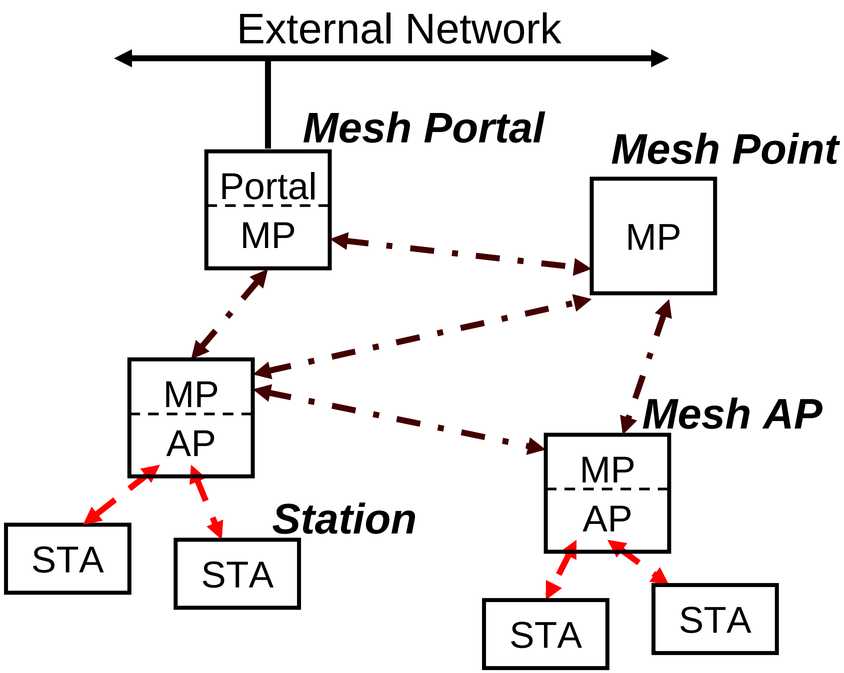
9. Standardization Efforts

Scope of the 802.11s Standard

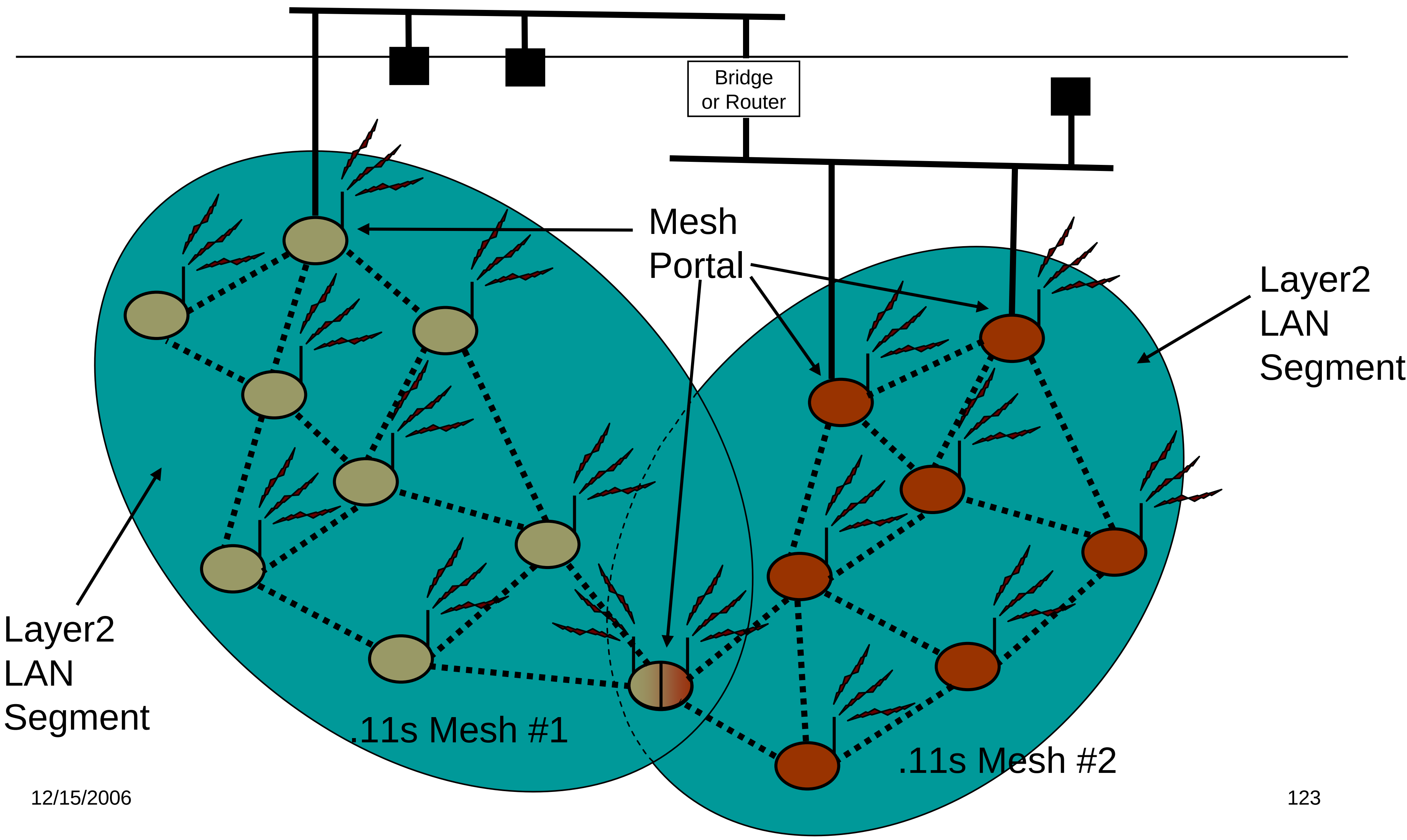
- 802.11s WLAN Mesh Networking
  - Integrates mesh networking services and protocols with 802.11 at the MAC Layer
  - Compatible with 802.11 Infrastructure Mode (supports both mesh APs and mesh-enabled client devices)
    - *Not Ad-Hoc/IBSS Mode*
- Primary Scope:
  - Amendment to IEEE 802.11 to create a Wireless Distribution System with automatic topology learning and wireless path configuration
  - Small/medium mesh networks (~32 forwarding nodes) – can be larger
  - Dynamic, *radio-aware* path selection in the mesh, enabling data delivery on single-hop and multi-hop paths (unicast and broadcast/multicast)
  - Extensible to allow support for diverse applications and future innovation
  - Use 802.11i security or an extension thereof
  - Compatible with higher layer protocols (broadcast LAN metaphor)

Device Classes in a WLAN Mesh Network

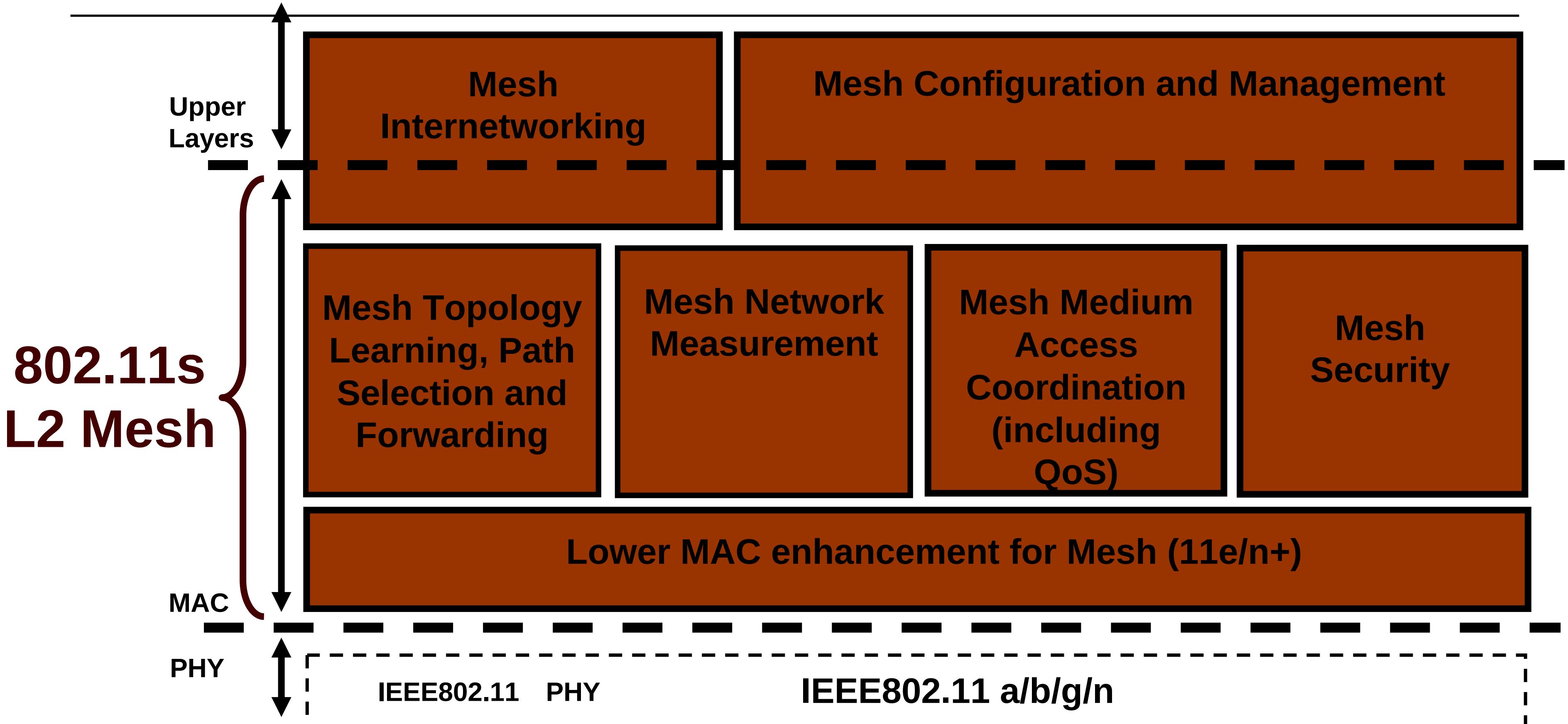
- **Mesh Point (MP):** establishes peer links with MP neighbors, full participant in WLAN Mesh services
  - Light Weight MP participates only in 1-hop communication with immediate neighbors (routing=NULL)
- **Mesh AP (MAP):** functionality of a MP, collocated with AP which provides BSS services to support communication with STAs
- **Mesh Portal (MPP):** point at which MSDUs exit and enter a WLAN Mesh (relies on higher layer bridging functions)
- **Station (STA):** outside of the WLAN Mesh, connected via Mesh AP



802.11s Mesh Network Model



802.11s Functional Component Architecture



Topology Formation: Membership in a WLAN Mesh Network

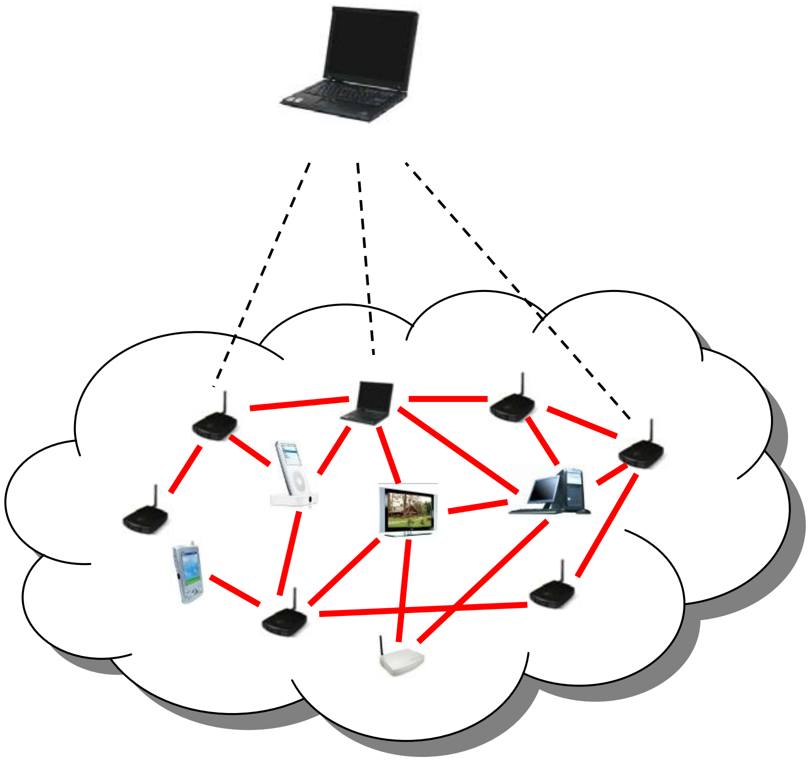
- Mesh Points (MPs) discover candidate neighbors based on new IEs in beacons and probe response frames
  - **WLAN Mesh Capability Element**
    - Summary of active protocol/metric
    - Channel coalescence mode and Channel precedence indicators
  - **Mesh ID**
    - Name of the mesh
- Mesh Services are supported by new IEs (in action frames), exchanged between MP neighbors
- Membership in a WLAN Mesh Network is determined by secure peer links with neighbors

Mesh Security Considerations

- Functions in the scope
  - Transport

    (Access point covered by 11i)
- Functions out of the scope
  - Internal routing
  - External routing
  - Forwarding
- Rationale
  - Current technology is not mature enough to address all vulnerabilities from routing and forwarding
  - There are still research questions

Transport Security



- Prevent unauthorized devices from directly sending and receiving traffic via the mesh
  - Protect unicast traffic between neighbor MPs
  - Protect broadcast traffic between neighbor MPs
- We need
  - Mutually authenticate neighbor MPs
  - Generate and manage session keys and broadcast keys
  - Data confidentiality over a link
  - Detect message forgeries and replays received on a link

Authentication and Initial Key Management

- Basic approach is to re-use 802.11i/802.1X
  - Re-use of 802.11i facilitates implementation
  - Allows other AKM schemes
- 802.1X is widely used and is suitable for many mesh scenarios
  - but can be replaced with small scale alternatives if required
- Provides a basis for secure key distribution (PMK)
- In a mesh, PMK is treated as token of authorization for a MP to join the mesh
  - Authorized to send and receive messages to/from mesh neighbors

Discovery and Role Negotiation

- Discovery
  - Discover the available mesh for joining
  - What Authenticated Key Management (AKM) Protocol, Unicast and Multicast Ciphersuites are available?
- Negotiation—Enable parties to agree on the security roles and security policy to use with a peer link
  - Who's the authenticator, who's the supplicant?
  - Agree on which of those options enabled to use

Extensible Framework Support for Mandatory and Alternative Path Selection Protocols

- **Draft defines one mandatory protocol and metric**
  - ***Any vendor may implement any protocol and/or metric*** within the framework
  - A particular mesh will have only one active protocol
  - Only one protocol/metric will be active on a particular link at a time

- **Mesh Points use the WLAN Mesh Capability IE to indicate which protocol is in use**

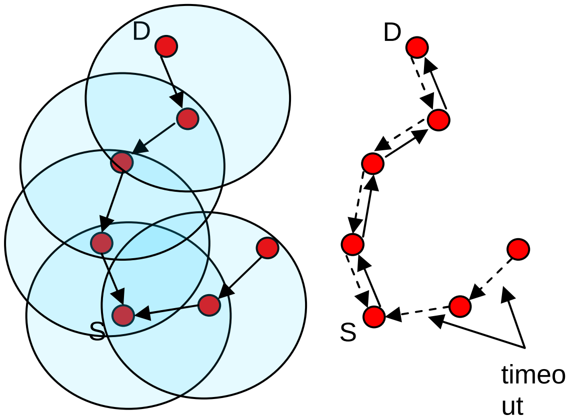
- **A mesh that is using other than mandatory protocol is not required to change its protocol when a new MP joins**
  - Algorithm to coordinate such a reconfiguration is out of scope

Default Routing protocol for Interoperability *Hybrid Wireless Mesh Protocol (HWMP)*

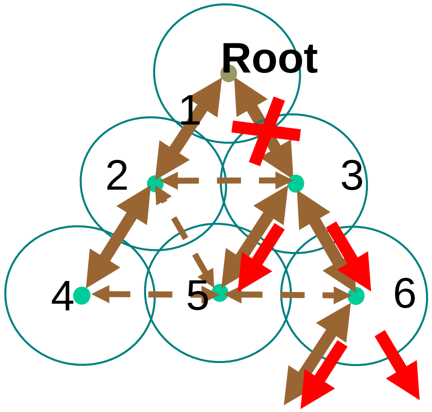
- Combines the flexibility of on-demand route discovery with efficient proactive routing to a mesh portal
  - On demand routing offers great flexibility in changing environments
  - Pro-active tree based routing is very efficient in fixed mesh deployments
  - The combination makes it suitable for implementation on a variety of different devices under consideration in TGs usage models
    - from CE devices to APs and servers
- Simple mandatory metric based on airtime as default, with support for other metrics
  - Extensibility framework allows any path selection metric (QoS, load balancing, power-aware, etc)

Hybrid Wireless Mesh Protocol (HWMP)

- On demand routing is based on Radio Metric AODV (RM-AODV)
  - Based on basic mandatory features of AODV (RFC 3561)
  - Extensions to identify best-metric path with arbitrary path metrics
  - Destinations may be discovered in the mesh on-demand



- Pro-active routing is based on tree based routing
  - If a Root portal is present, a distance vector routing tree is built and maintained
  - Tree based routing is efficient for hierarchical networks
  - Tree based routing avoids unnecessary discovery flooding during discovery and recovery



HWMP Protocol Elements

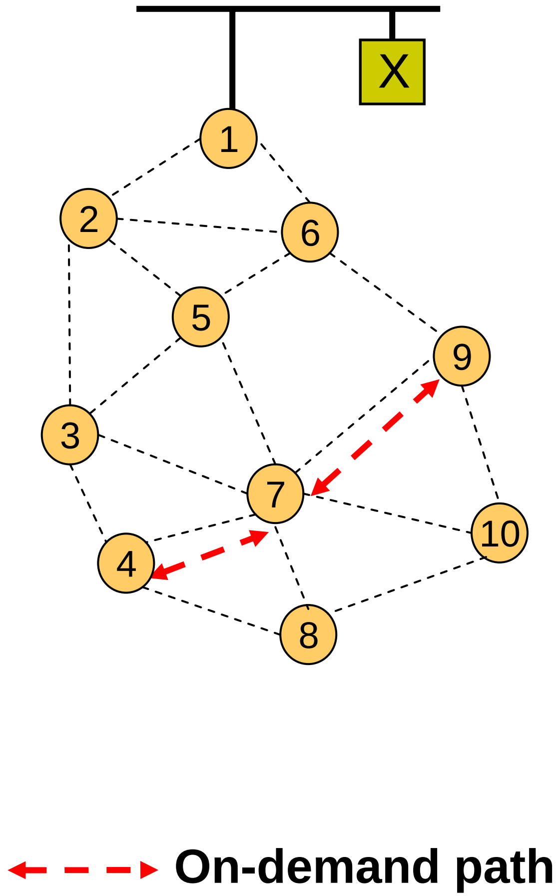
- Root Announcement (broadcast)
- Route Request (broadcast/unicast)
- Route Reply (unicast)
- Route Error (broadcast)

- Tells MPs about presence and distance of Root MP
- Asks destination MP(s) to form a *reverse* route to the originator
- Forms a *forward* route to the originator and confirms the reverse route
- Tells receiving MPs that the originator no longer supports certain routes

HWMP Example #1: No Root, Destination Inside the Mesh

Example: MP 4 wants to communicate with MP 9

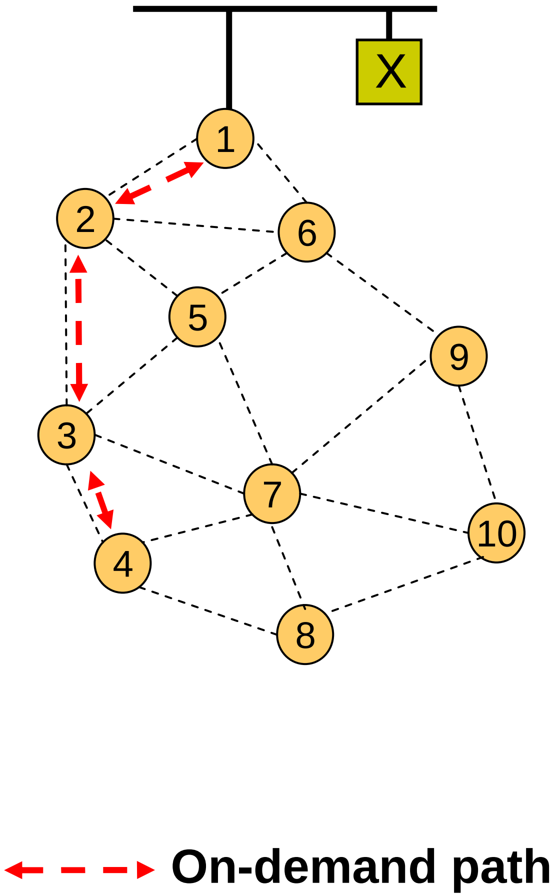
1. **MP 4 first checks its local forwarding table for an active forwarding entry to MP 9**
2. **If no active path exists, MP 4 sends a broadcast RREQ to discover the best path to MP 9**
3. **MP 9 replies to the RREQ with a unicast RREP to establish a bi-directional path for data forwarding**
4. **MP 4 begins data communication with MP 9**



HWMP Example #2: Non-Root Portal(s), Destination Outside the Mesh

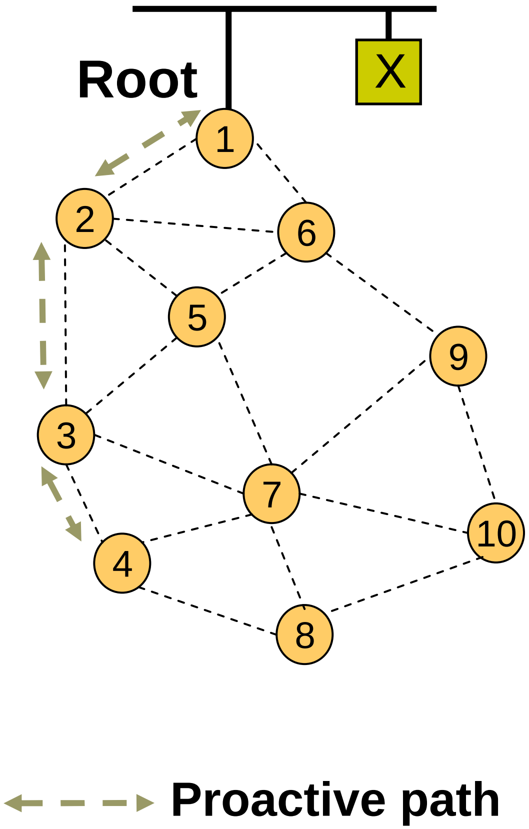
Example: MP 4 wants to communicate with X

1. **MP 4 first checks its local forwarding table for an active forwarding entry to X**
2. **If no active path exists, MP 4 sends a broadcast RREQ to discover the best path to X**
3. **When no RREP received, MP 4 assumes X is outside the mesh and sends messages destined to X to Mesh Portal(s) for interworking**
4. **Mesh Portal MP 1 forwards messages to other LAN segments according to locally implemented interworking**



HWMP Example #3: Root Portal, Destination Outside the Mesh

<u>Example: MP 4 wants to communicate with X</u>



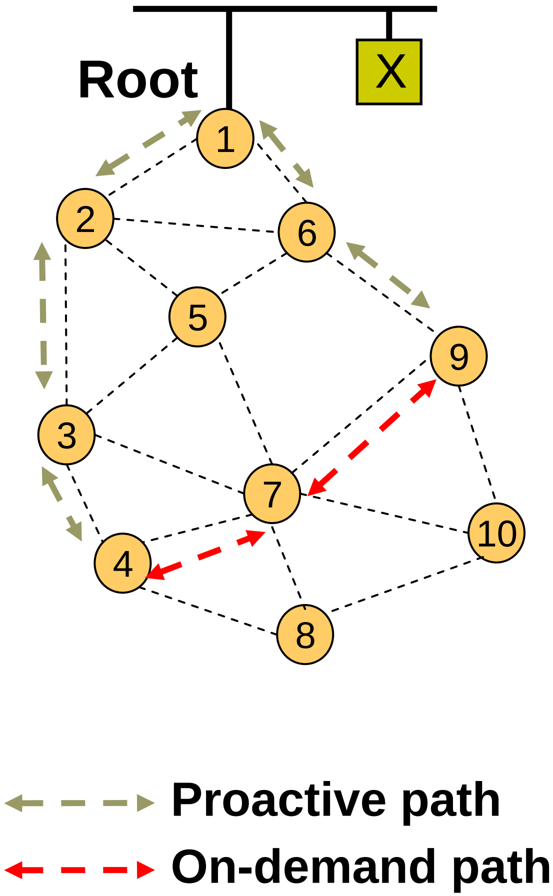
1. **MPs learn Root MP 1 through Root Announcement messages**
2. **If MP 4 has no entry for X in its local forwarding table, MP 4 may immediately forward the message on the proactive path toward the Root MP 1**
3. **When MP 1 receives the message, if it does not have an active forwarding entry to X it may assume the destination is outside the mesh**
4. **Mesh Portal MP 1 forwards messages to other LAN segments according to locally implemented interworking**

Note: No broadcast discovery required when destination is outside of the mesh

HWMP Example #4: With Root, Destination Inside the Mesh

Example: MP 4 wants to communicate with MP 9

1. **MPs learn Root MP 1 through Root Announcement messages**
2. **MP 4 first checks its local forwarding table for an active forwarding entry to MP 9**
3. **If no active path exists, MP 4 *may* immediately forward the message on the proactive path toward the Root MP 1**
4. **When MP 1 receives the message, it flags the message as "intra-mesh" and forwards on the proactive path to MP 9**
5. **MP 9, receiving the message, *may* issue a RREQ back to MP 4 to establish a path that is more efficient than the path via Root MP 1**

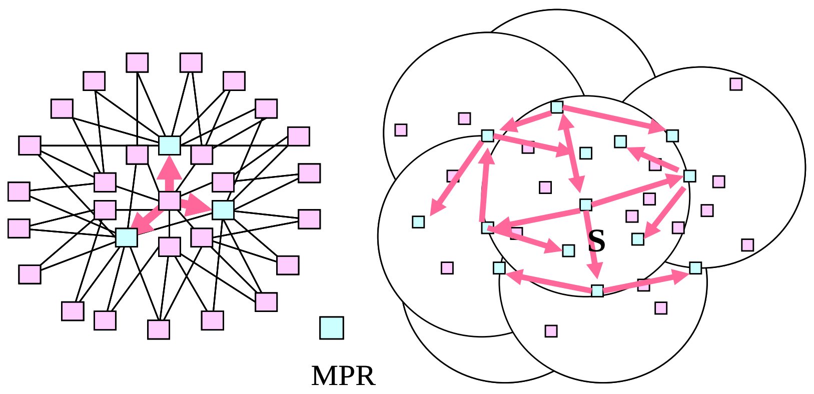


Example Optional Path Selection Protocol *Radio Aware OLSR (RA-OLSR)*

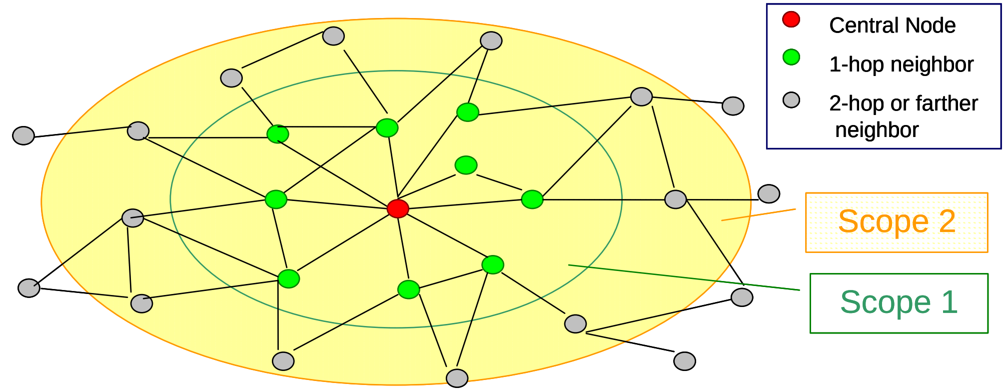
- Proactively maintains link-state for routing
  - Changes in link state are communicated to “neighborhood” nodes
- Extensible routing scheme based on the two link-state routing protocols:
  - OLSR (RFC 3626)
  - (Optional) Fisheye State Routing (FSR)
- Extended with:
  - Use of a radio aware metric in MPR selection and routing path selection
  - Efficient association discovery and dissemination protocol to support 802.11 stations

RA-OLSR – Key Features

- Multi Point Relays (MPRs)
  - A set of 1-hop neighbor nodes covering 2-hop neighborhood
  - Only MPRs emit topology information and retransmit packets
    - Reduces retransmission overhead in flooding process ***in space***.



- (Optional) message exchange frequency control (fish-eye state routing)
  - Lower frequency for nodes within larger scope
    - Reduce message exchange overhead ***in time***.



Upcoming Technology: WiMax/802.16

IEEE 802.16

- IEEE 802.16 defines the WirelessMAN air interface specification for wireless metropolitan area networks (MANs)
- It will facilitate broadband wireless access
- Designed for point-to-multipoint broadband access applications using roof-top or tower-mounted antennas
- Addresses the need for very high bit rates
- Types:
  - 802.16d: fixed wireless acess – air interface for 10-60 GHz or 2-11 GHz (licensed frequencies)
  - 802.16e: support for mobile client devices

Services

- Digital audio/video multicast
- Digital telephony
- ATM
- Internet Protocol
- Bridged LAN
- Back-haul

Physical Layer

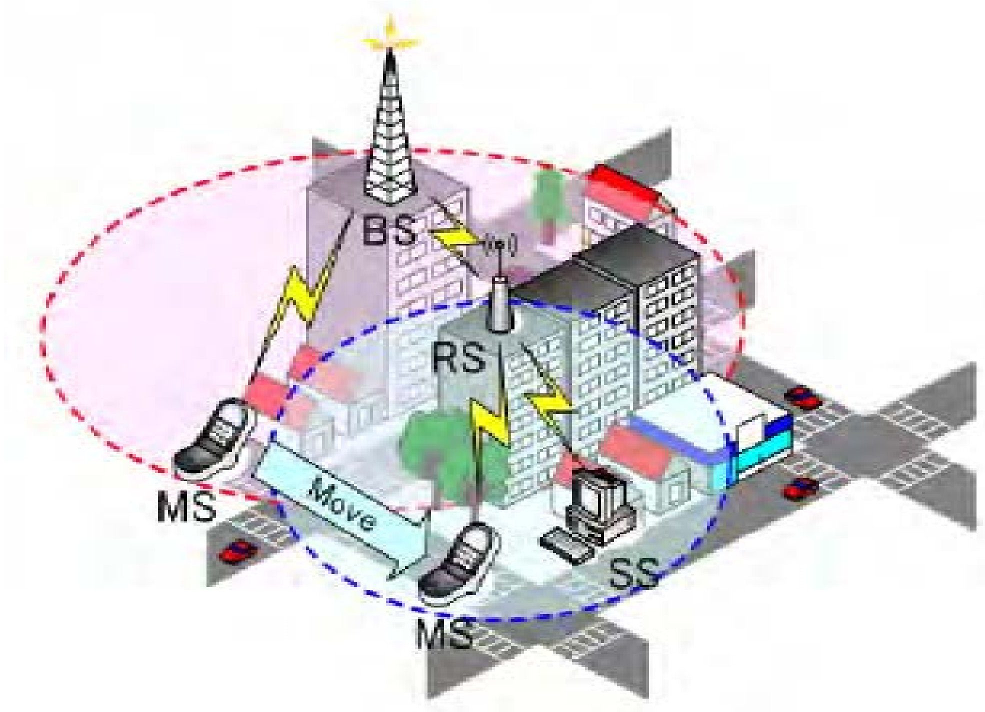
- 10-66 GHz:
  - Line of sight propagation
  - The BS transmits a TDM signal with individual subscriber stations (SSs) allocated time slots serially
  - Both TDD and FDD are used for uplink/downlink
- 2-11 GHz:
  - Non line-of-sight (NLOS) operations
  - Use of OFDM

Connection Setup

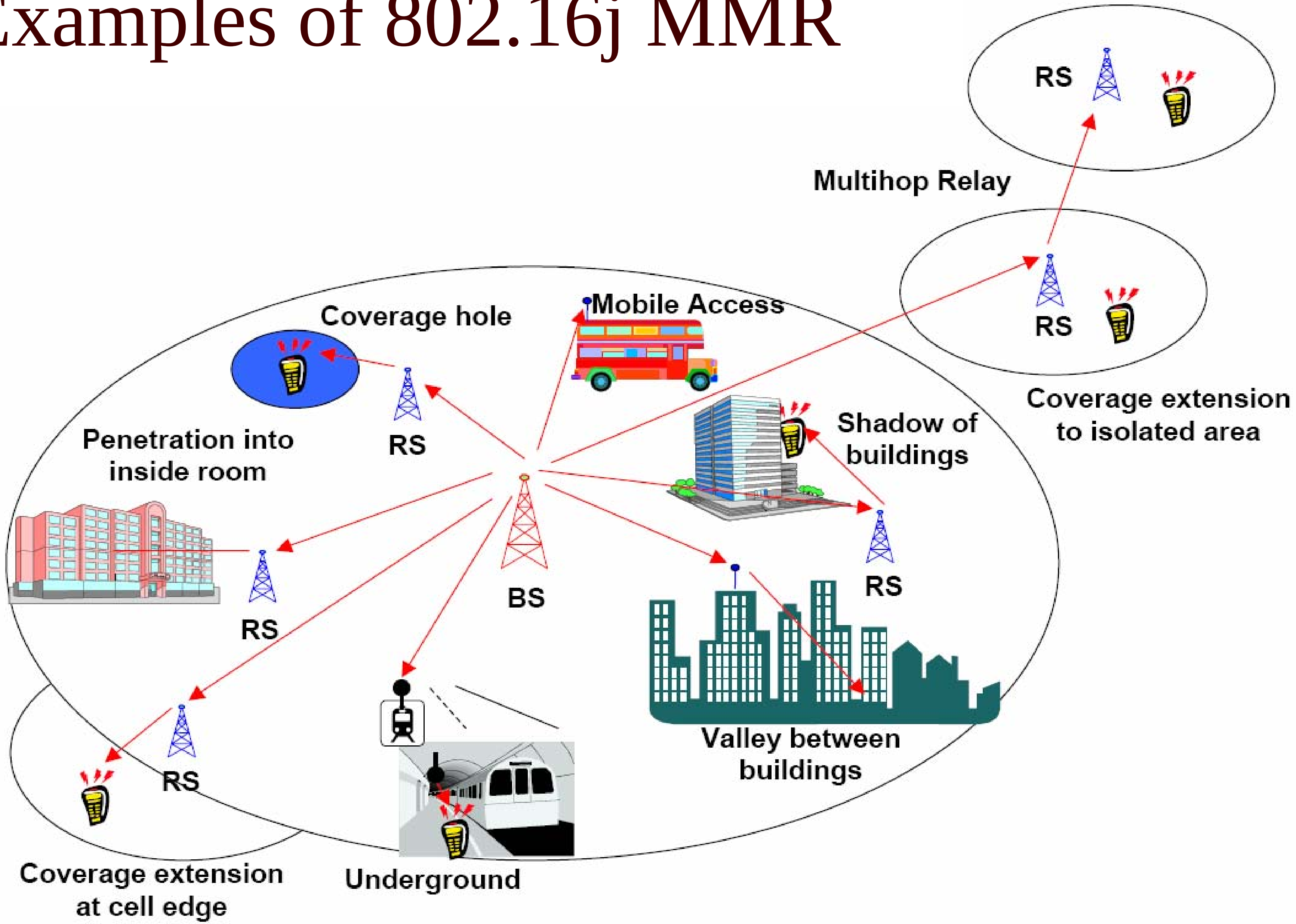
- IEEE 802.16 uses the concept of service flows to define unidirectional transport of packets on either downlink or uplink
- Each admitted or active service flow is mapped to a MAC connection with a unique CID
- Service flows are pre-provisioned, and setup of the service flows is initiated by the BS during SS initialization
- Dynamic service establishment and dynamic service changes are also supported

802.16j Mobile Multihop Relay (MMR)

- Relay mode based on IEEE 802.16e
- Introduces Relay Stations to gain:
  - Coverage Extension, and
  - Throughput Enhancement



Examples of 802.16j MMR



10. Experimental Systems

Experimental and Commercial Systems

- An incomplete list (Jan 2005)
- Academia
  - University Research Efforts
- Community Networks
- Industry
  - Commercial Products

Academia (14+)

- Roofnet
  - MIT
  - pdos.csail.mit.edu/roofnet/doku.php
- BWN-Mesh
  - Georgia Institute of Technology
  - www.ece.gatech.edu/research/labs/bwn/mesh/work.html
- UCSB MeshNet
  - moment.cs.ucsb.edu/
- Orbit Project
  - Rutgers WinLab
  - www.winlab.rutgers.edu/pub/docs/focus/ORBIT.html
- Digital Gangetic Plains
  - Media Lab Asia - Kanpur Lucknow Lab
  - www.iitk.ac.in/mladgp/
- Stony Brook Mesh Router
  - www.cs.sunysb.edu/~samir
- Hyacinth (Stony Brook)
  - www.ecsl.cs.sunysb.edu/multichannel/
- VMesh
  - University of Thessaly, Volos, Greece
  - vmesh.inf.uth.gr/
- Wireless Networking Group, UIUC
  - www.crhc.uiuc.edu/wireless/
  - University of Illinois at Urbana-Champaign
- 802.11 Testbed for Cooperation
  - www.cs.washington.edu/homes/djw/
- Transit Access Points
  - Rice University
  - taps.rice.edu/taps-overview.html
- Multi-radio Mesh Networking Testbed
  - Rice University
- Mesh Wireless LANs
  - dvd1.ecs.umass.edu/wireless/publications/mesh/index.html
- Quail Ridge Mesh – UC Davis
  - www.cs.ucdavis.edu/~prasant/projects

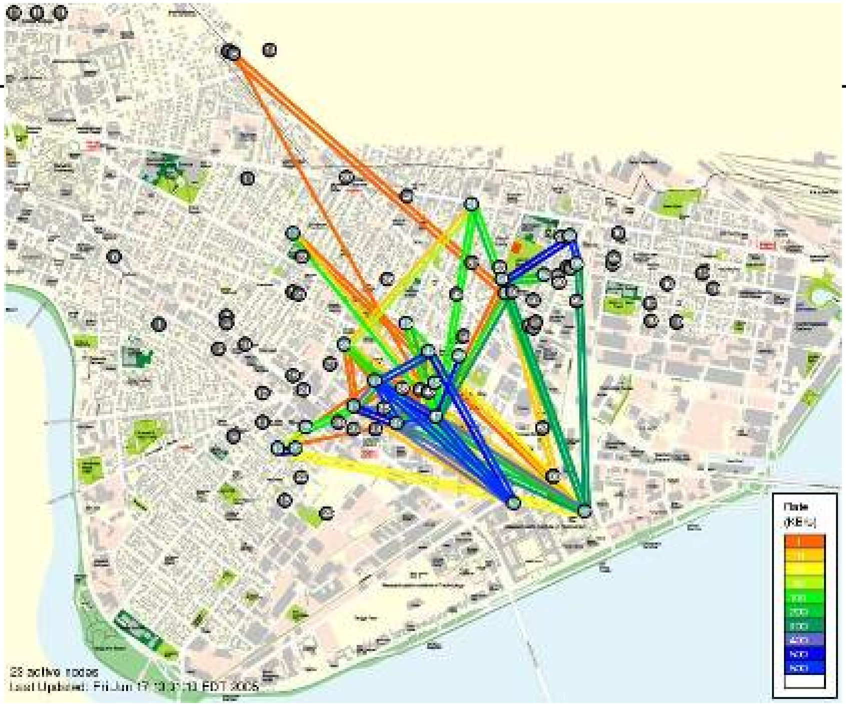
Community Networks (8+)

- Manchester Wireless
  - www.manchesterwireless.net
- Champaign-Urbana Community Wireless Network
  - www.cuwireless.net
- SeattleWireless
  - www.seattlewireless.net
- Bay Area Wireless Users Group (BAWUG)
  - www.bawug.org/
- Southampton Open Wireless Network
  - www.sown.org.uk/
- NYC Wireless
  - www.nycwireless.net/
- Personal Telco
  - www.personaltelco.net/static/index.html
- FreeNetworks
  - www.freenetworks.org/

Industry (23+)

- Microsoft Mesh Testbed
  - research.microsoft.com/mesh/
- BelAir Networks
  - www.belairnetworks.com
- MeshDynamics
  - www.meshdynamics.com
- Motorola - MeshNetworks
  - mesh.nowwireless.com/
- NowWireless
  - nowwireless.com/
- Cisco Systems, Inc
  - www.cisco.com
- MITRE
  - www.mitre.org/work/tech_transfer/mobilemesh/index.html
- Nortel
  - www.nortel.com
- 3Com
  - www.3com.com
- Proxim Wireless Networks
  - www.proxim.com
- 4g-Systems
  - http://www.4g-systems.biz/
- Intel
  - www.intel.com
- Engim inc.
  - www.engim.com
- Firetide Networks
  - www.firetide.com
- Ascentry Technologies
  - www.ascentry.com/
- Nokia
  - www.nokia.com
- NovaRoam
  - www.novaroam.com/
- PacketHop
  - www.packethop.com/technology/network.html
- Strix Systems
  - www.strixsystems.com/
- RoamAD
  - www.roamad.com/
- Tropos Networks
  - www.tropos.com/
- Kiyon Autonomous Networks
  - www.kiyon.com/

MIT Roofnet



- Experimental outdoor testbed with real users.
- 40-60 nodes.
- Research focus on link layer measurements and routing studies.
- Open source software for Prism and Atheros platforms.

ORBIT Radio Grid at WinLab/Rutgers

- 400 node indoor radio grid.
- Custom hardware platform with Atheros 802.11a/b/g radios
  - More control on the radio than typical.
- Distributed signal generators producing interference
  - Brings up noise floor.

- Goal: Remotely accessible laboratory-based wireless network emulation.

Wireless Mesh Networking in Microsoft Research

- Indoor testbed.
- Mesh connectivity layer (MCL) software
  - Implemented in between layer 2 and 3.
  - Acts as a virtual interface to layer 3.
- Current research focus routing, multi-radio/multichannel studies.
- Future visions of self-organizing neighborhood mesh network.

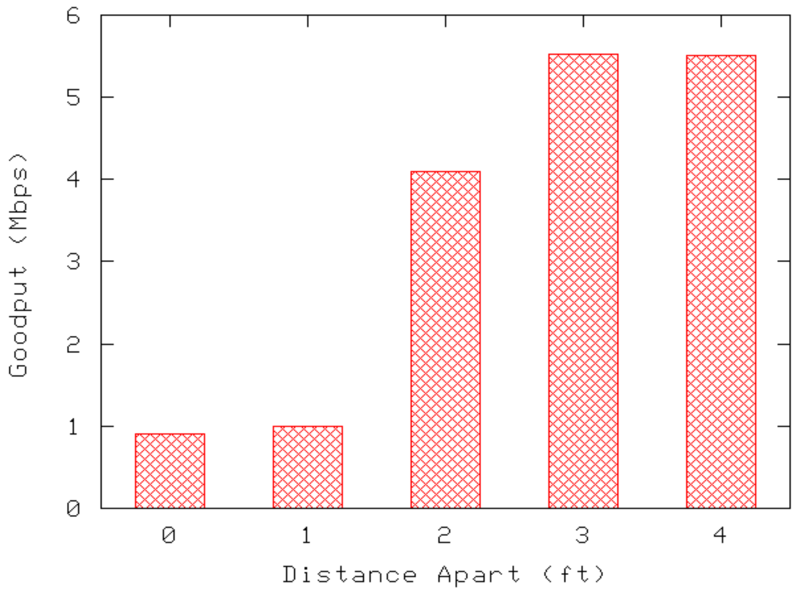
Experimental Setup at UCD

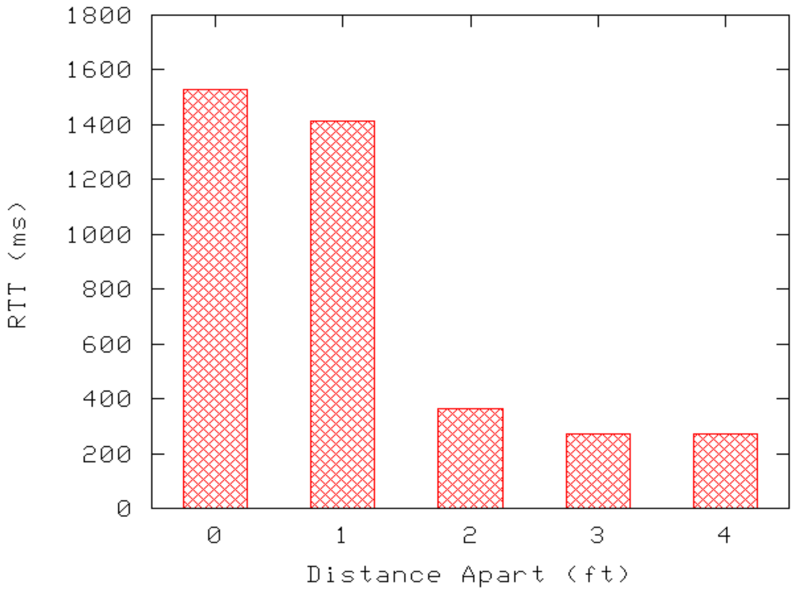
- IEEE 802.11b ORiNOCO AP-2000
- ORiNOCO Classic Gold PC Cards
- 8 Laptops running Fedora Core 3
- Wireless Distribution System running between access points
- Experiments performed in an interference-free environment
- Goodput calculated with the average of five 20 second TCP bulk data transfers from end to end

Network Setup

- 4 Access Points in a linear topology
- Multi-radio, Multi-Channel, Multi-Hop Tests
- 5 dBi gain antennas elevated 4 ft and separated 4 ft
- 100 ft between APs

Impact of Antenna Proximity

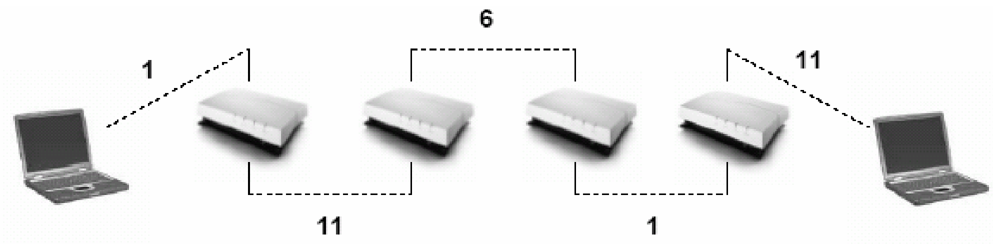




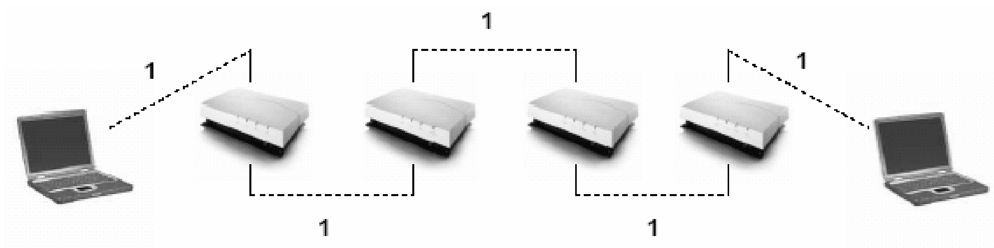
Topology and Channel Assignments

- Impact of channel interference versus radio-to-radio processing overhead

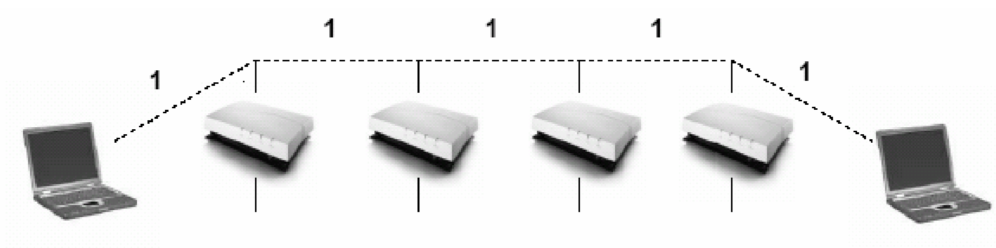
Two Cards Multiple Channels (TCMC)



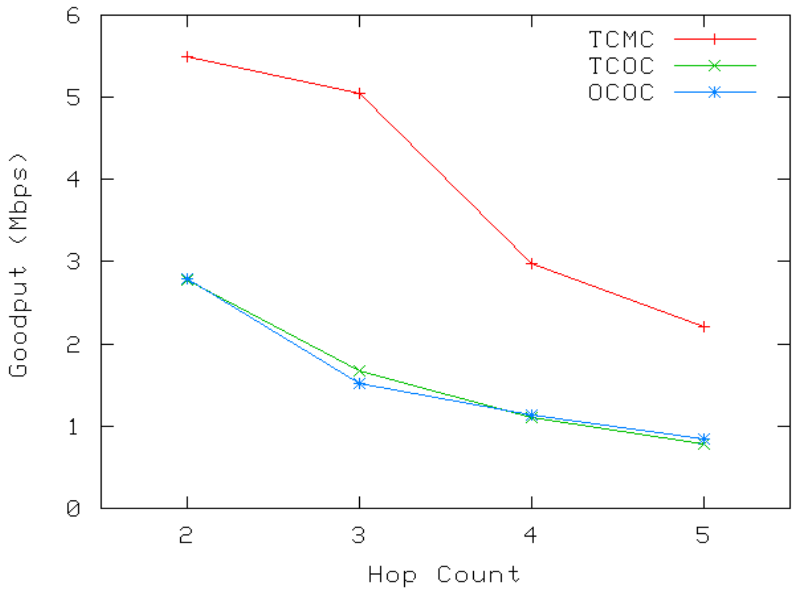
Two Cards One Channels (TCOC)

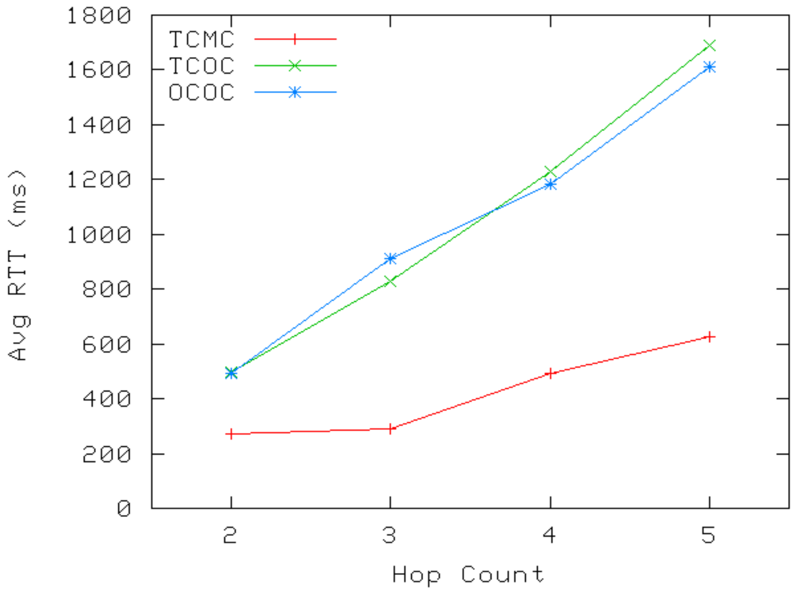


One Card One Channel (OCOC)

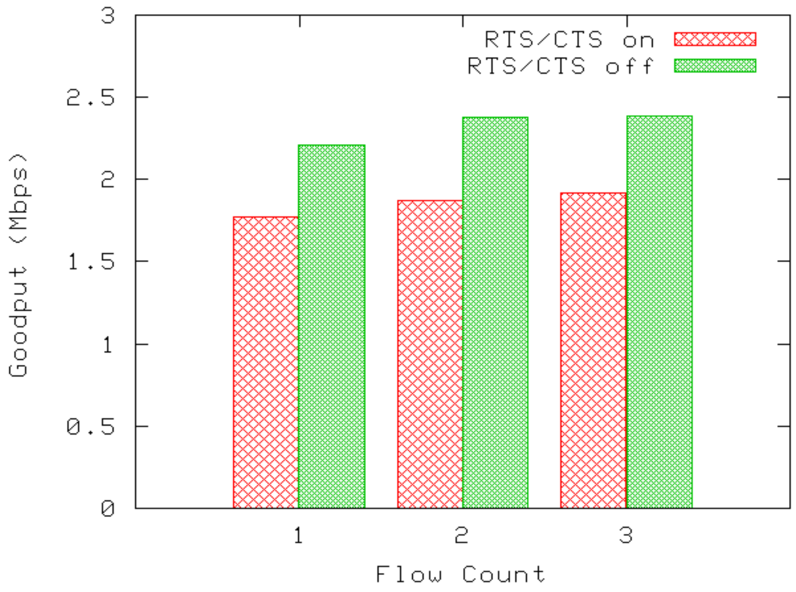


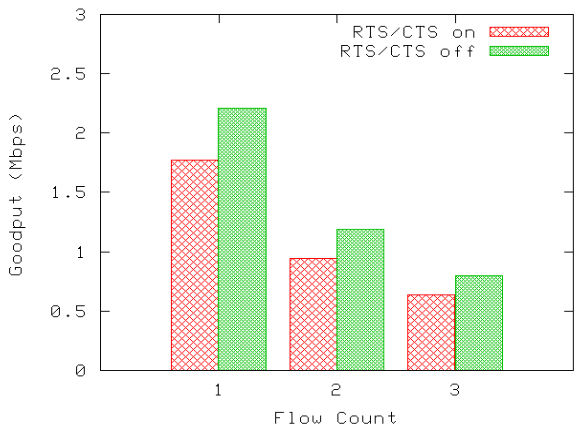
Impact of Various Channel Allocations

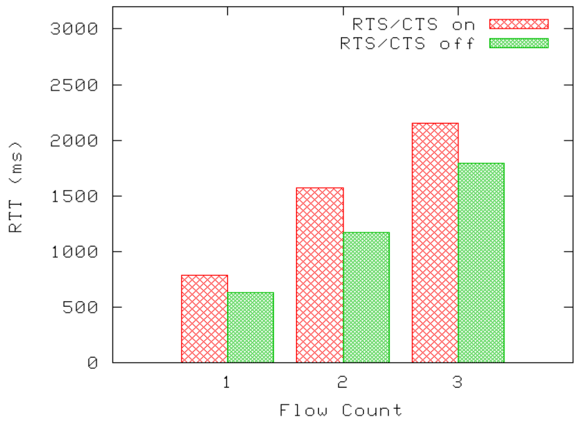




Impact of RTS/CTS





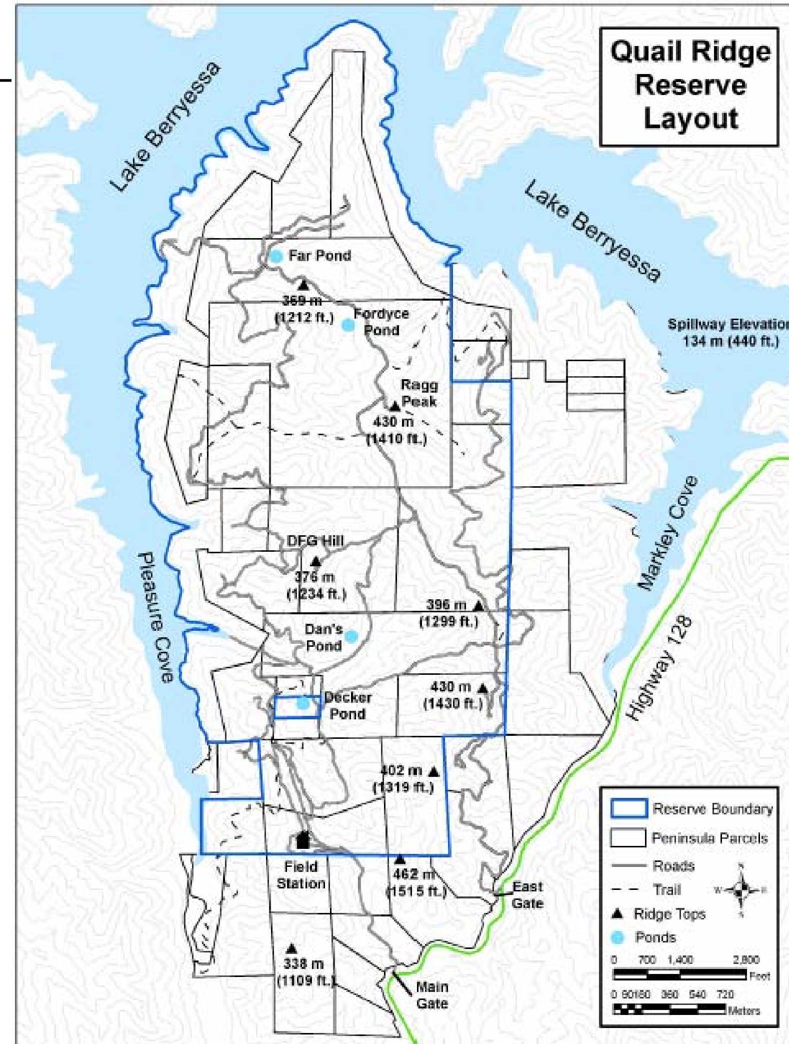


Quail Ridge Reserve Wireless Mesh Network

- Help out the ecological studies within Quail Ridge
- Create a test-bed for running experiments

Topology

- Rough terrain
- Varied elevation
- Overgrowth of trees and vegetation
- Varied weather conditions
- Long link distances
- Lack of onsite power (solar)

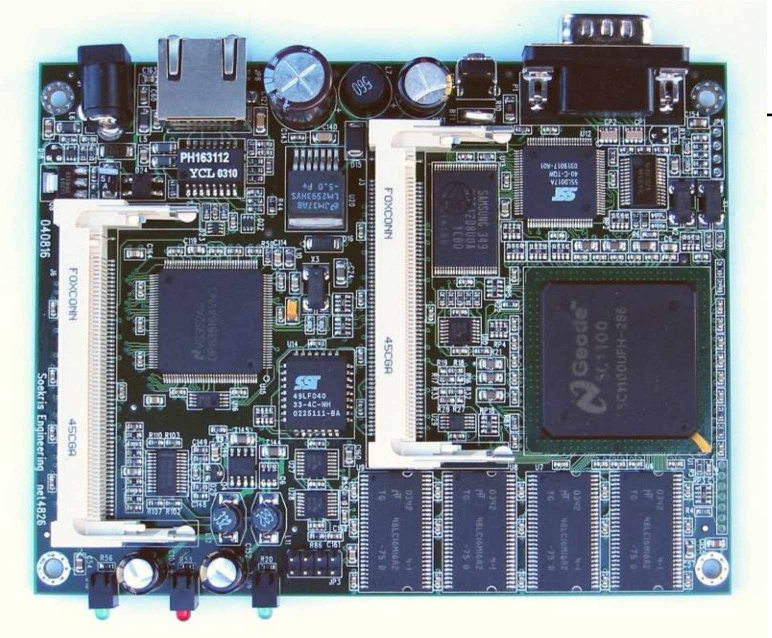


Network Architecture

- Three layers:
  - Backbone (directional antenna)
  - Midlayer (omnidirectional)
  - Sensor Network: functionality-specific networks at various locations
- Need QoS for multimedia streaming
- Data reliability vs network reliability
- Evaluating new MAC protocols

Hardware

- Soekris net4826
  - 2 miniPCI slots
  - 64 MB of Flash Memory
  - 128 MB of RAM
  - 266 MHZ AMD Geode SC1100
- Wireless Cards
  - 400mW Atheros 802.11b/g cards



Current Status

- Eight operational nodes – planned expansion to 30 during the next year.
- Bandwidth varies from 6-22Mbps (node to gateway)
- Multiple radios, multiple antennas, multiple channels, multiple rates, in multi-hop set-up.
- Used by ecological researchers and environmental scientists
- Varied data being collected for analysis
- Several audio and video sensors
- Can be access remotely for observations, data collection, measurements
  - sprit.cs.ucdavis.edu/~quailridge


11. Concluding Remarks

Summarizing: Technical Issues and Hurdles

- Applications – still evolving
- Interoperability
  - WiFi, WiMax, Bluetooth, Zigbee, … the wireless mess!
  - Overlays or BGP like?
- Multi-*(channel, radio, path, flow, layer, rate, antenna) protocols – MAC and routing
- Exploit and enhance capacity: the multi-* stuff!
- Robust Communication
  - Without this aspect, no one will adopt
- Shouldn't leave out the most hyped phrase: *Cross-Layer Designs*

Future Visions

- Self-managed, rather than unmanaged ones!
- Cost of deployment and maintenance will be the main driving factor for its success!
- Need for development of tools for wireless mesh design, maintenance, and monitoring, and management
- Need for trade-off assessment: various topology, radios per node, number of channels, hops, channel assignment, communication flows, antenna proximity, control overheads, type of antenna, exploiting interferences, etc.