Advanced Topics of Wireless Networking

Wireless and Mobile Networks

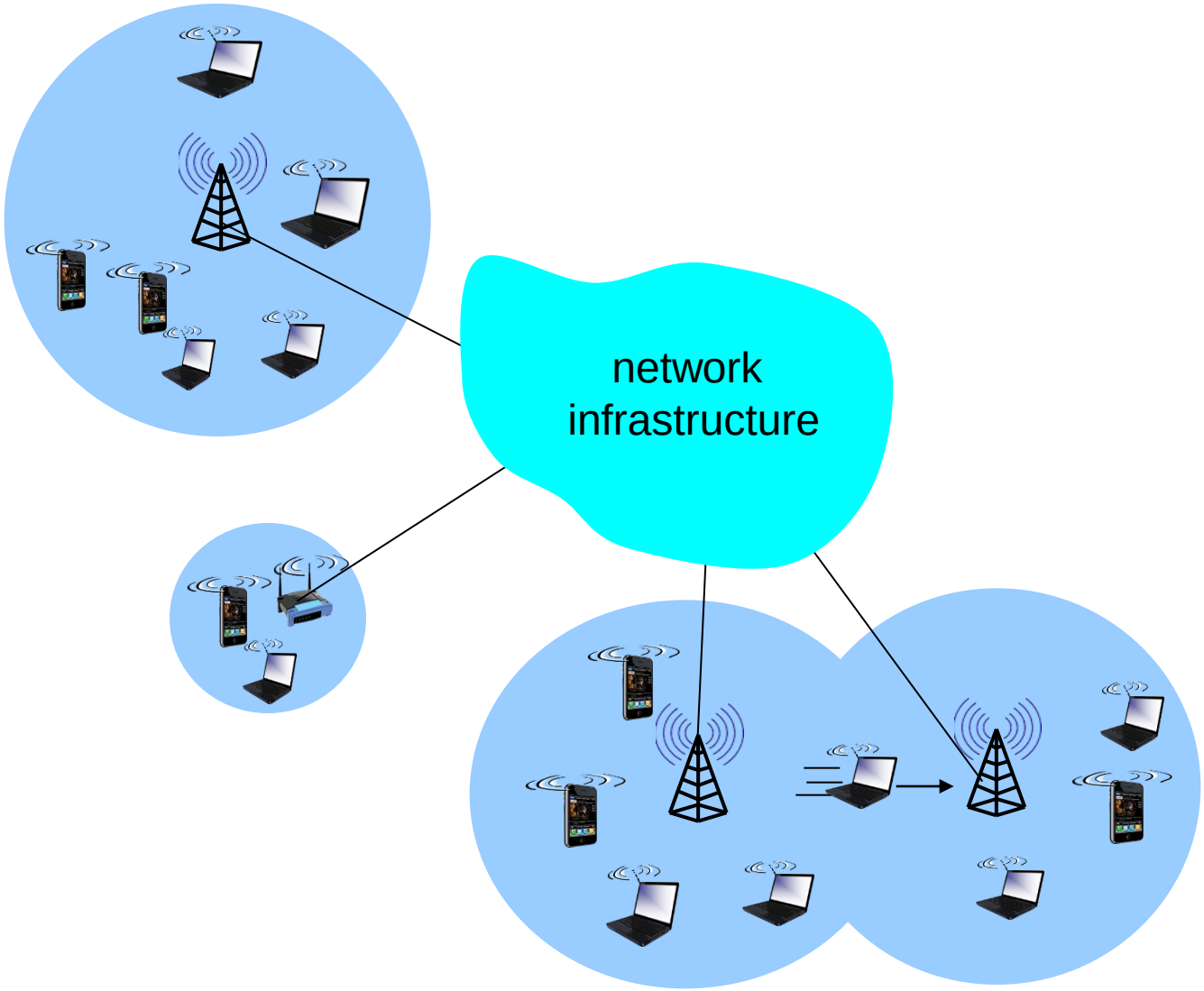
Background:

- # wireless (mobile) phone subscribers now exceeds # wired phone subscribers (5-to-1)!
- # wireless Internet-connected devices equals # wireline Internet-connected devices
  - laptops, Internet-enabled phones promise anytime untethered Internet access
- two important (but different) challenges
  - *wireless:* communication over wireless link
  - *mobility:* handling the mobile user who changes point of attachment to network

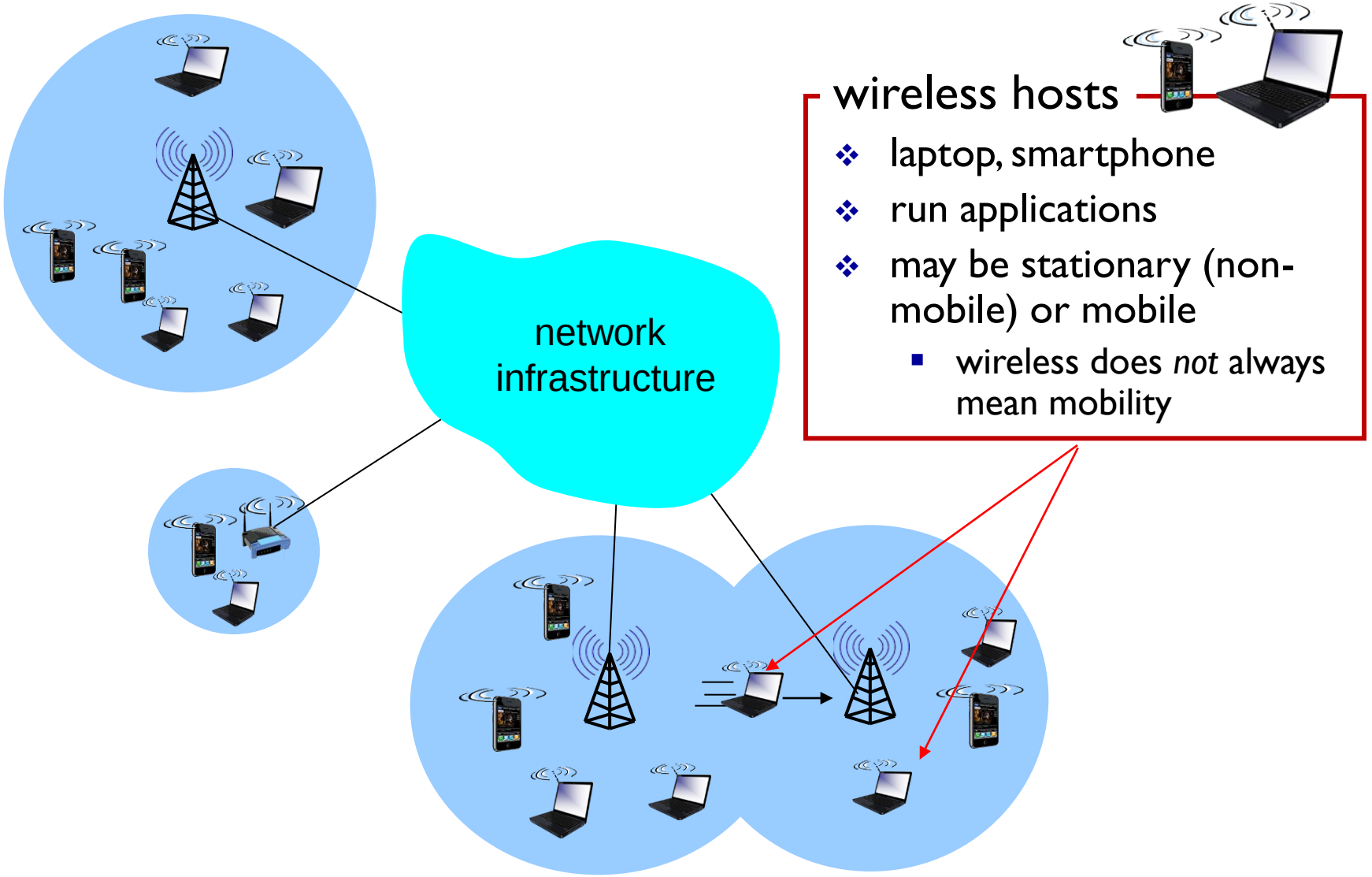
Outline

- Overview
- MAC
- Routing
- Wireless in real world
- Leverage broadcasting nature
- Explore the characteristic of wireless signal

Elements of a wireless network



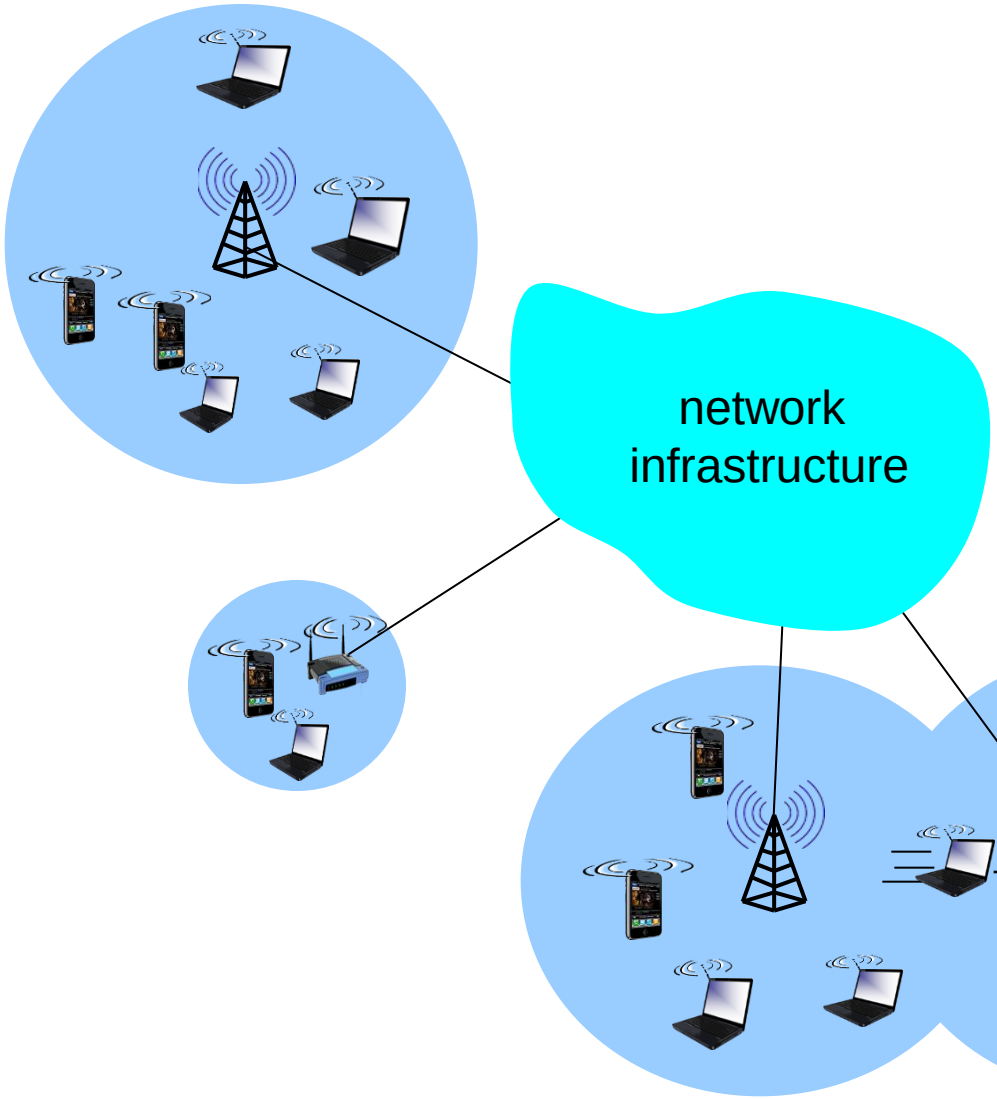
Elements of a wireless network



wireless hosts

- laptop, smartphone
- run applications
- may be stationary (non-mobile) or mobile
  - wireless does *not* always mean mobility

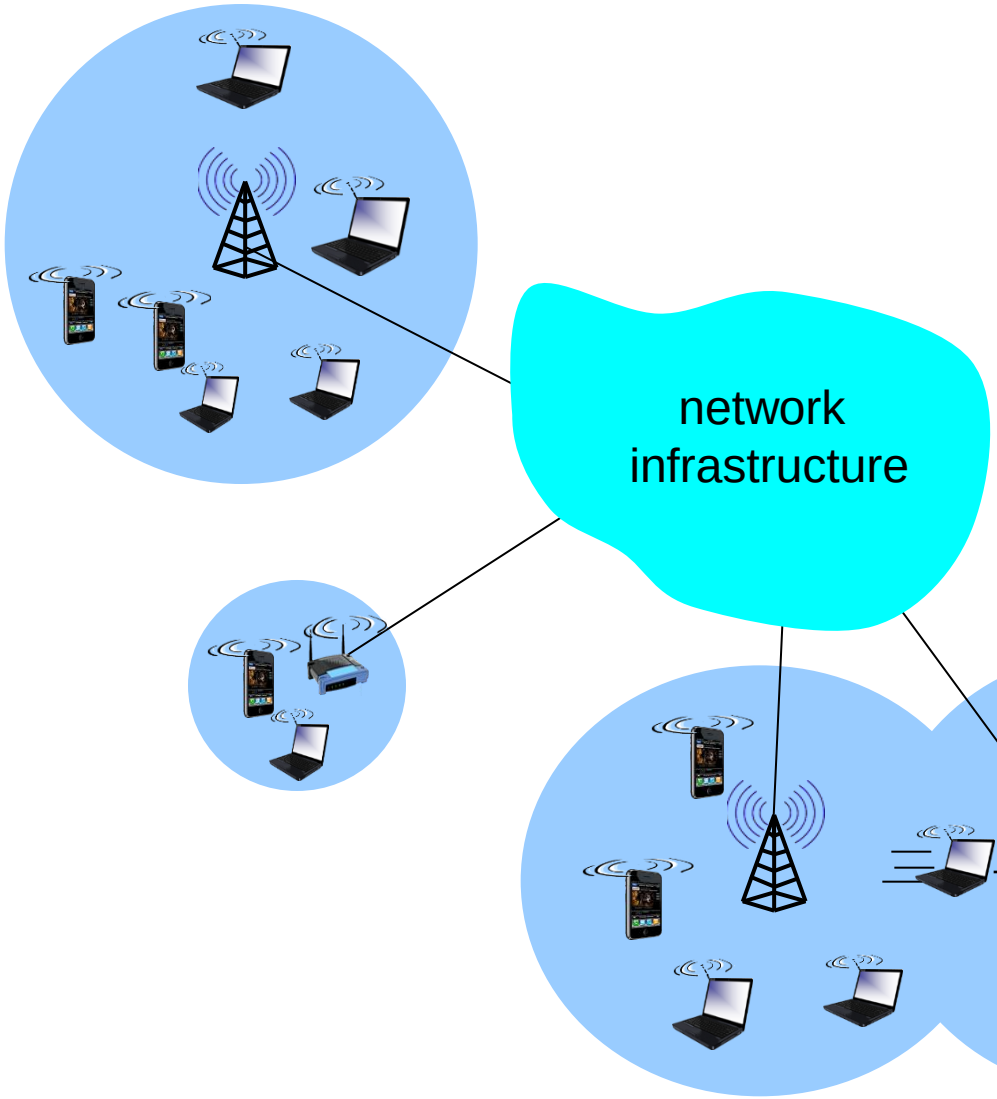
Elements of a wireless network



base station

- typically connected to wired network
- relay - responsible for sending packets between wired network and wired network and wireless host(s) in its "area"
  - e.g., cell towers, 802.11 access points

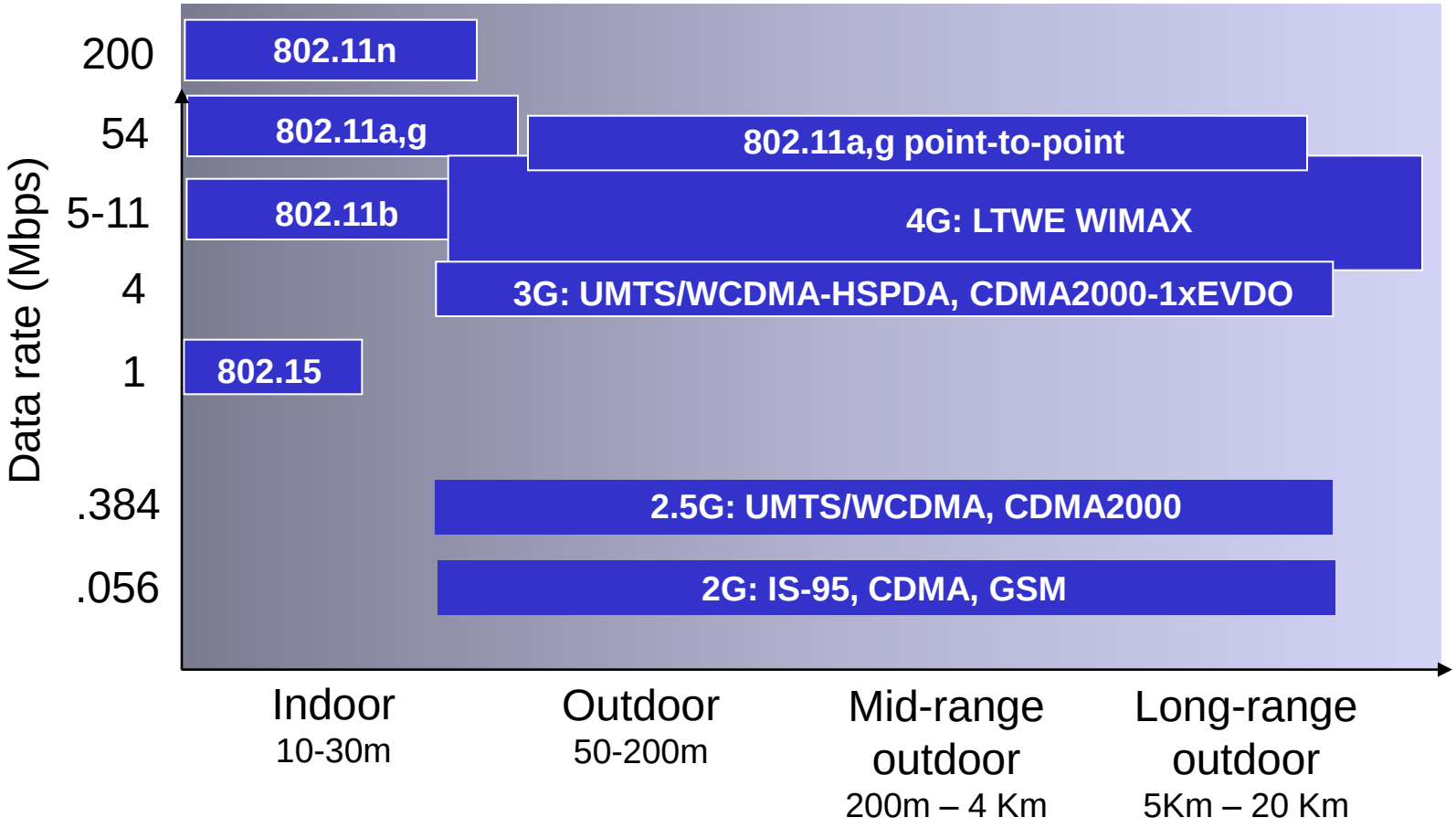
Elements of a wireless network



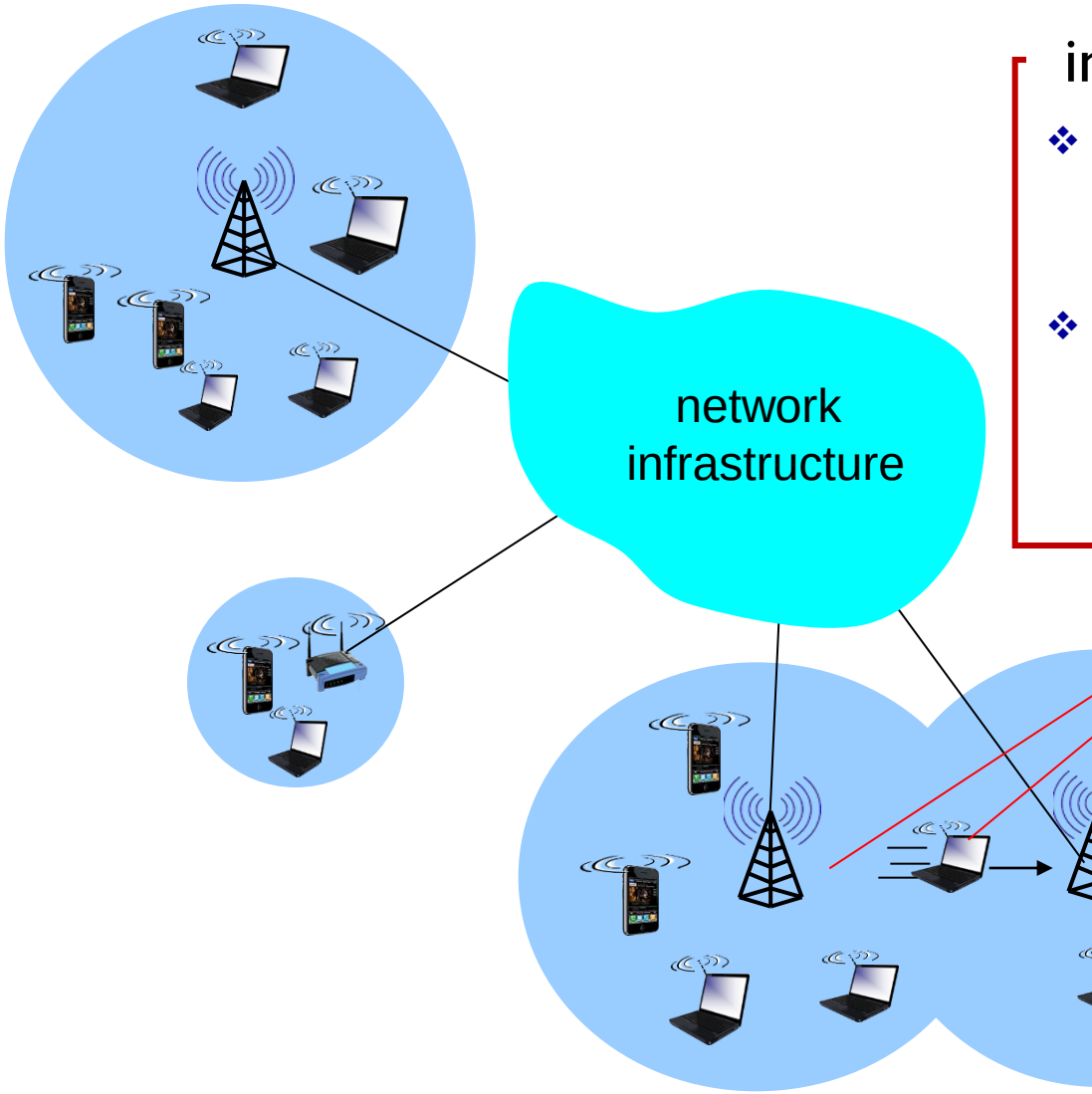
wireless link

- typically used to connect mobile(s) to base station
- also used as backbone link
- multiple access protocol coordinates link access
- various data rates, transmission distance

Characteristics of selected wireless links



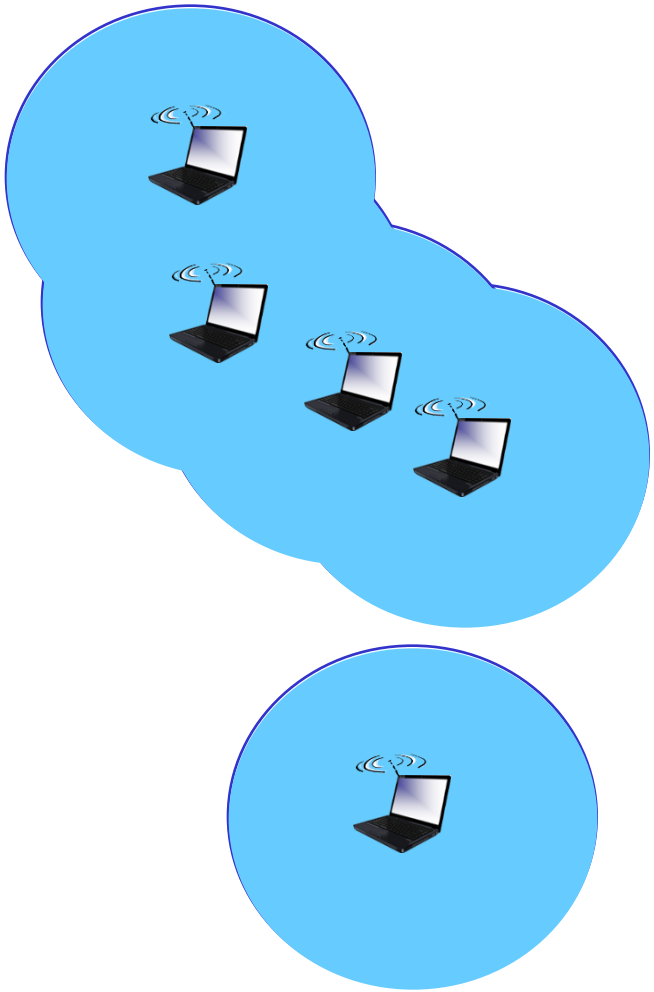
Elements of a wireless network



infrastructure mode

- base station connects mobiles into wired network
- handoff: mobile changes base station providing connection into wired network

Elements of a wireless network



ad hoc mode

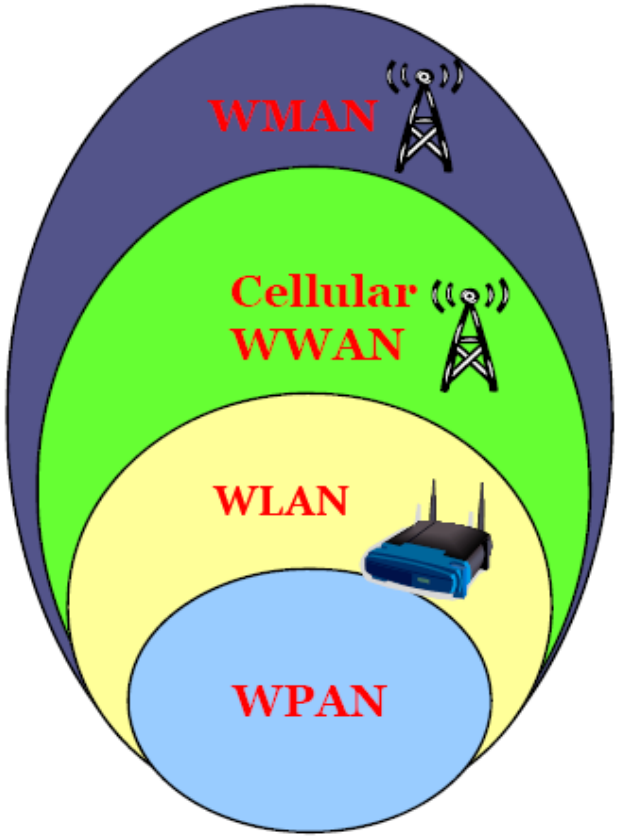
- no base stations
- nodes can only transmit to other nodes within link coverage
- nodes organize themselves into a network: route among themselves

Wireless network taxonomy

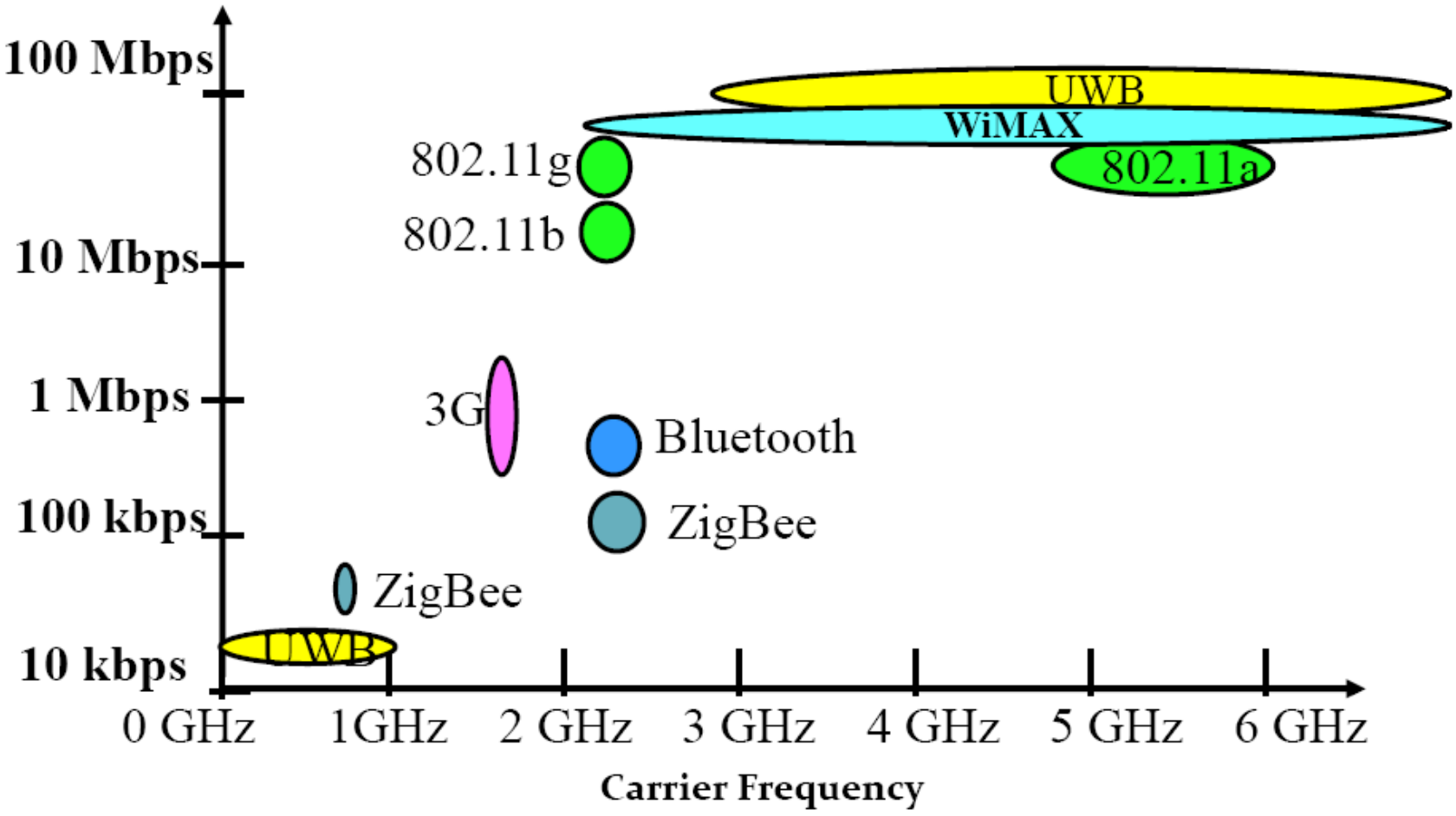
	single hop	multiple hops
infrastructure (e.g., APs)	host connects to base station (WiFi, WiMAX, cellular) which connects to larger Internet	host may have to relay through several wireless nodes to connect to larger Internet: *mesh net*
no infrastructure	no base station, no connection to larger Internet (Bluetooth, ad hoc nets)	no base station, no connection to larger Internet. May have to relay to reach other a given wireless node MANET, VANET

Existing Wireless Networks

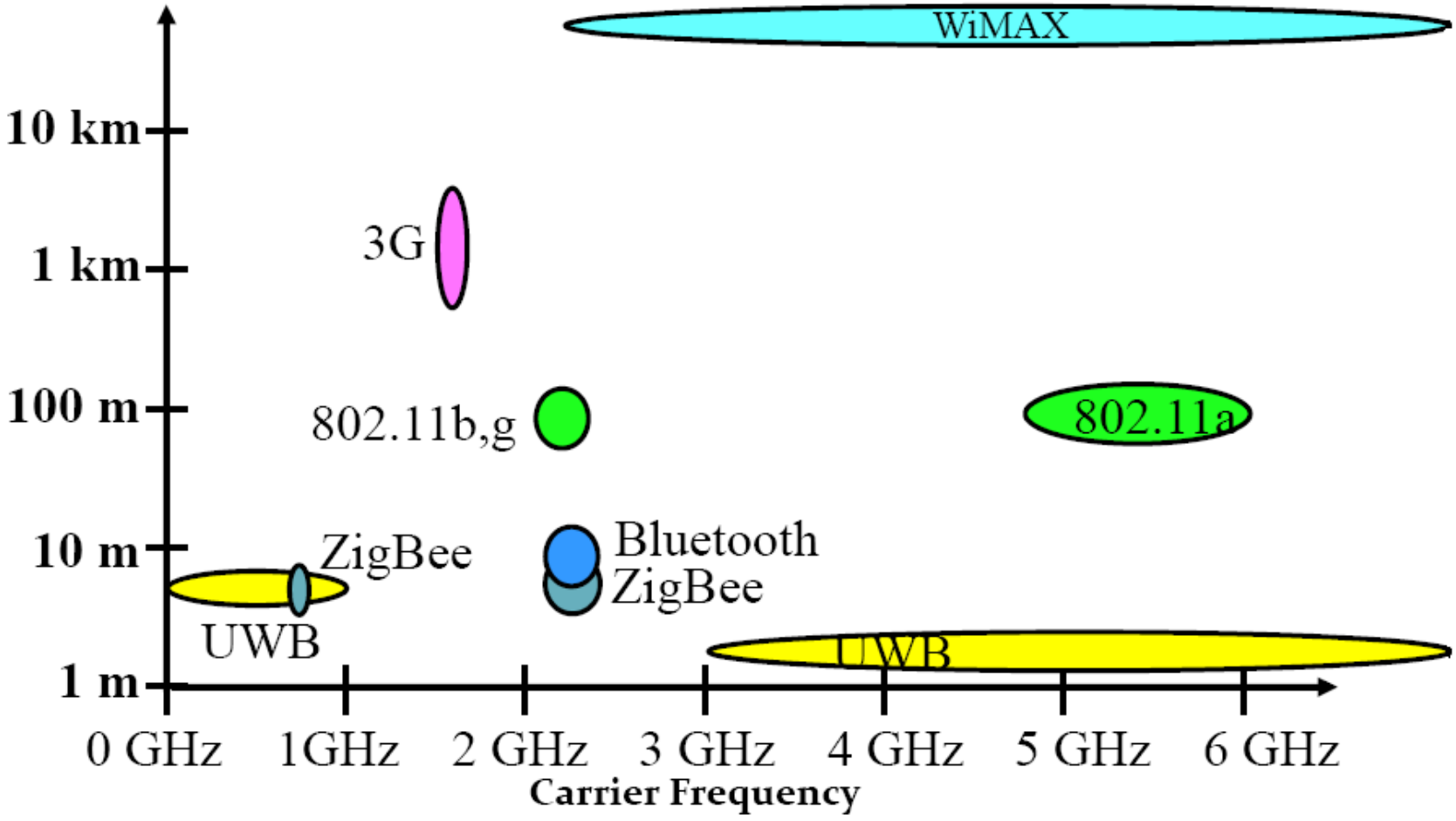
- Wireless Metropolitan Area Network (WMAN)
- Cellular/Wireless Wide Area Network (WWAN) (GSM, WCDMA, EV-DO)
- Wireless Local Area Network (WLAN)
- Wireless Personal Area Network (WPAN)
- Ad hoc networks
- Sensor networks
- Emerging networks (variations of ad hoc networks
  - Info-stations
  - Vehicular networks
- Cognitive Radio Networks
  - IEEE 802.22



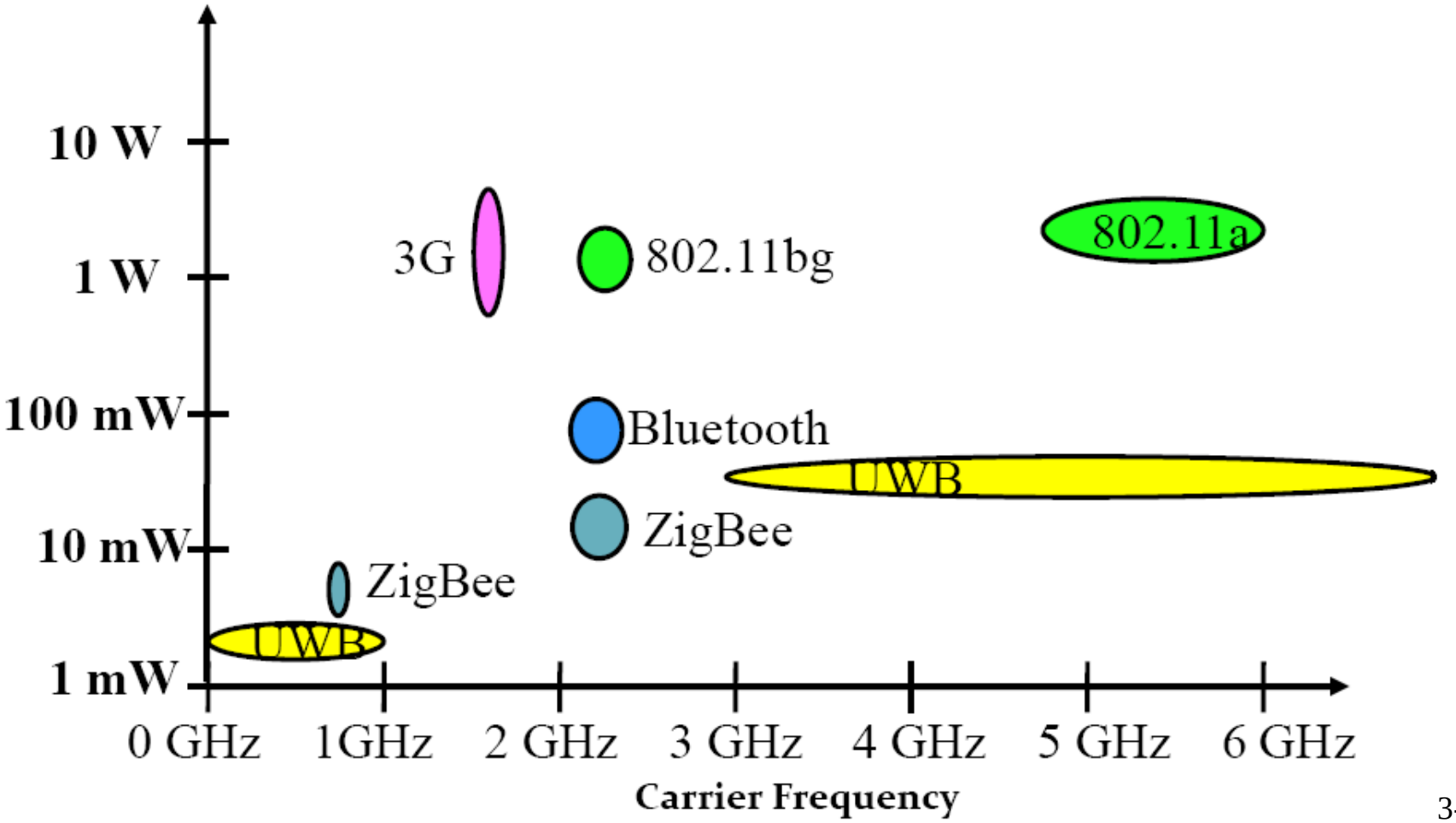
Data Rate


100 Mbps
10 Mbps
1 Mbps
100 kbps
10 kbps
UWB
WiMAX
802.11a
802.11g
802.11b
3G
Bluetooth
ZigBee
ZigBee
UWB
0 GHz
1GHz
2 GHz
3 GHz
4 GHz
5 GHz
6 GHz
Carrier Frequency

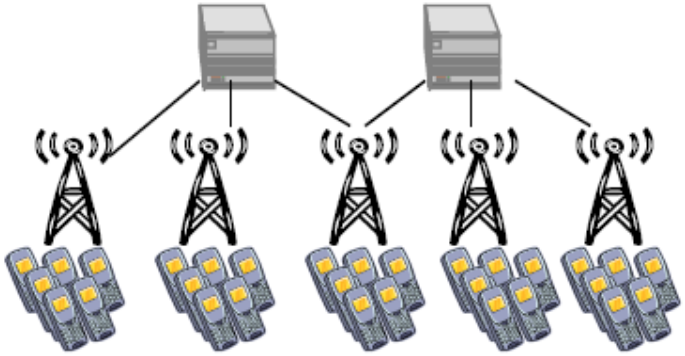
Transmission Range



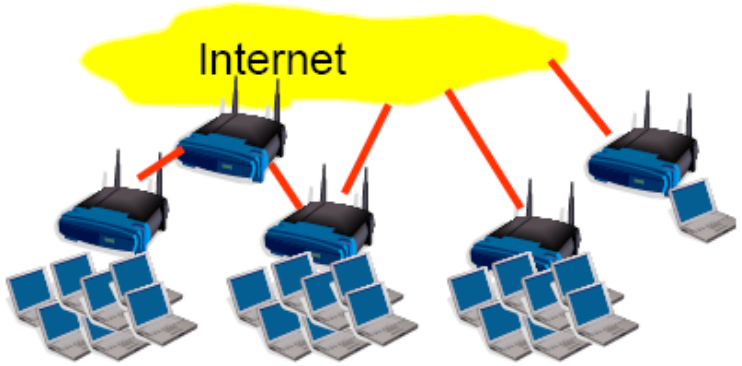
Power Dissipation



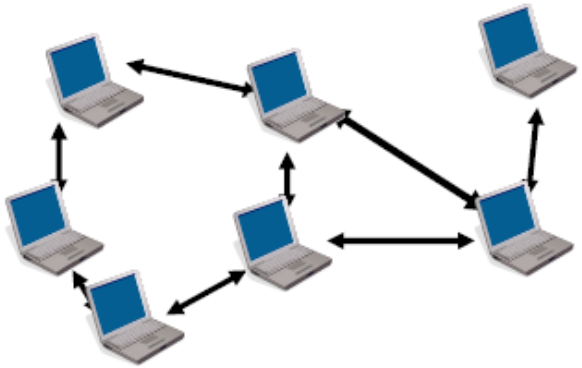
Network Architectures



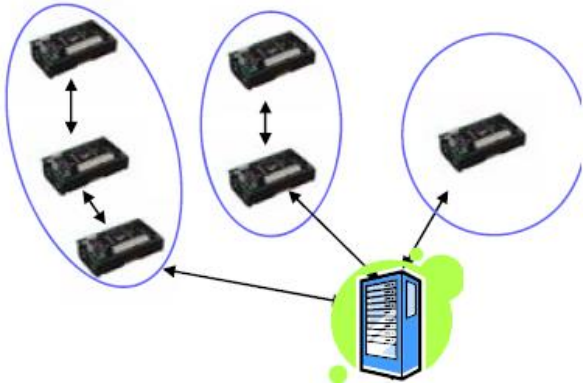
Cellular Networks (hierarchical systems)
☺ QoS + mobility ☹ $$$, lack of



WLAN / Mesh networks
☺ Simple, cheap ☹ Poor management



Ad hoc networks
☺ no infrastructure cost ☹ no guarantee



Sensor networks
☹ Energy limited, low processing power

Wireless Link Characteristics (1)

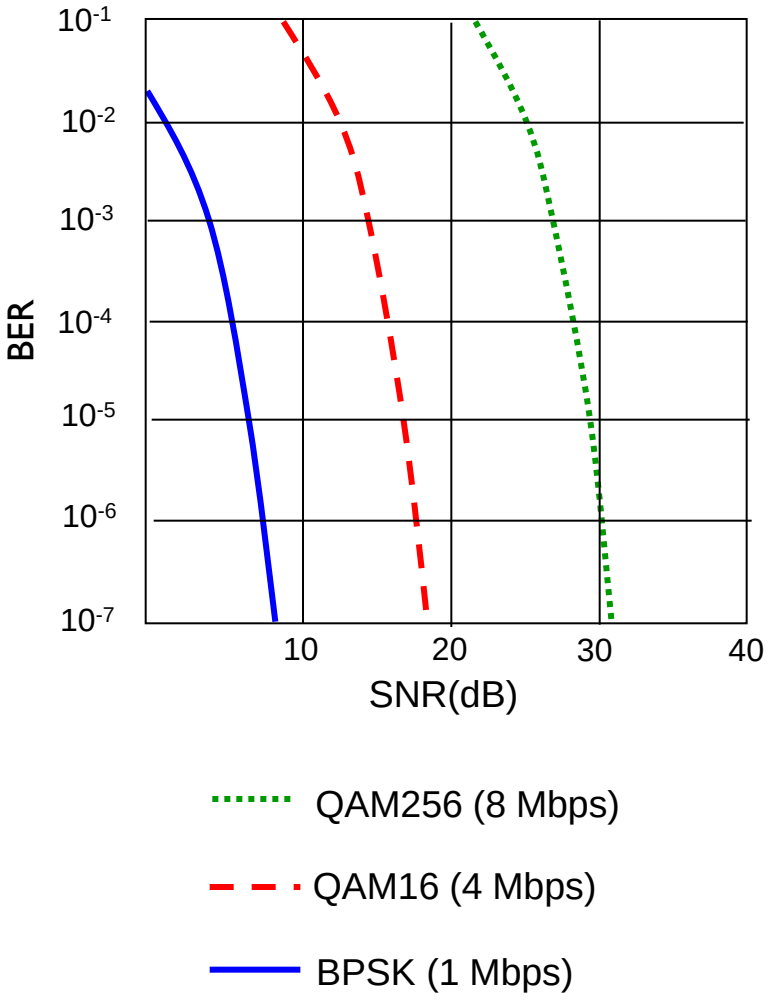
important differences from wired link ….

- *decreased signal strength:* radio signal attenuates as it propagates through matter (path loss)
- *interference from other sources:* standardized wireless network frequencies (e.g., 2.4 GHz) shared by other devices (e.g., phone); devices (motors) interfere as well
- *multipath propagation:* radio signal reflects off objects ground, arriving ad destination at slightly different times

…. make communication across (even a point to point) wireless link much more "difficult"

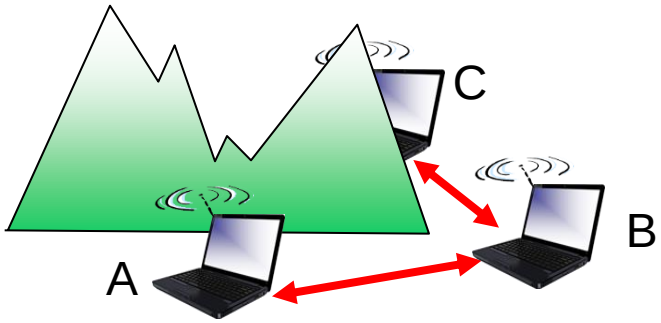
Wireless Link Characteristics (2)

- SNR: signal-to-noise ratio
  - larger SNR – easier to extract signal from noise (a "good thing")
- *SNR versus BER tradeoffs*
  - *given physical layer:* increase power -> increase SNR->decrease BER
  - *given SNR:* choose physical layer that meets BER requirement, giving highest thruput
    - SNR may change with mobility: dynamically adapt physical layer (modulation technique, rate)



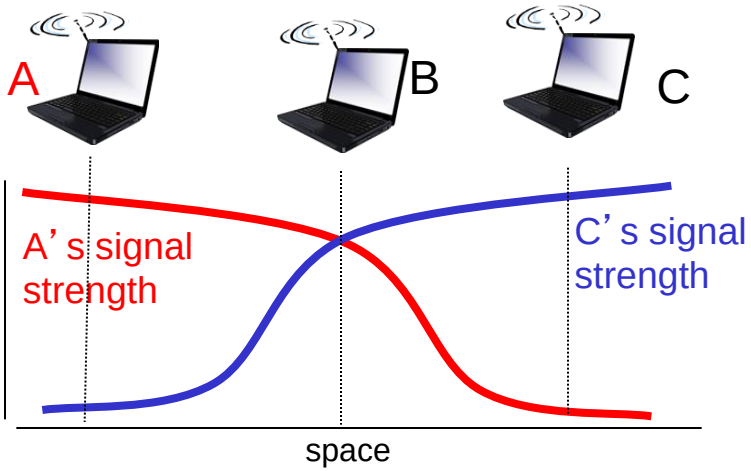
Wireless network characteristics

Multiple wireless senders and receivers create additional problems (beyond multiple access):



Hidden terminal problem

- B, A hear each other
- B, C hear each other
- A, C can not hear each other means A, C unaware of their interference at B



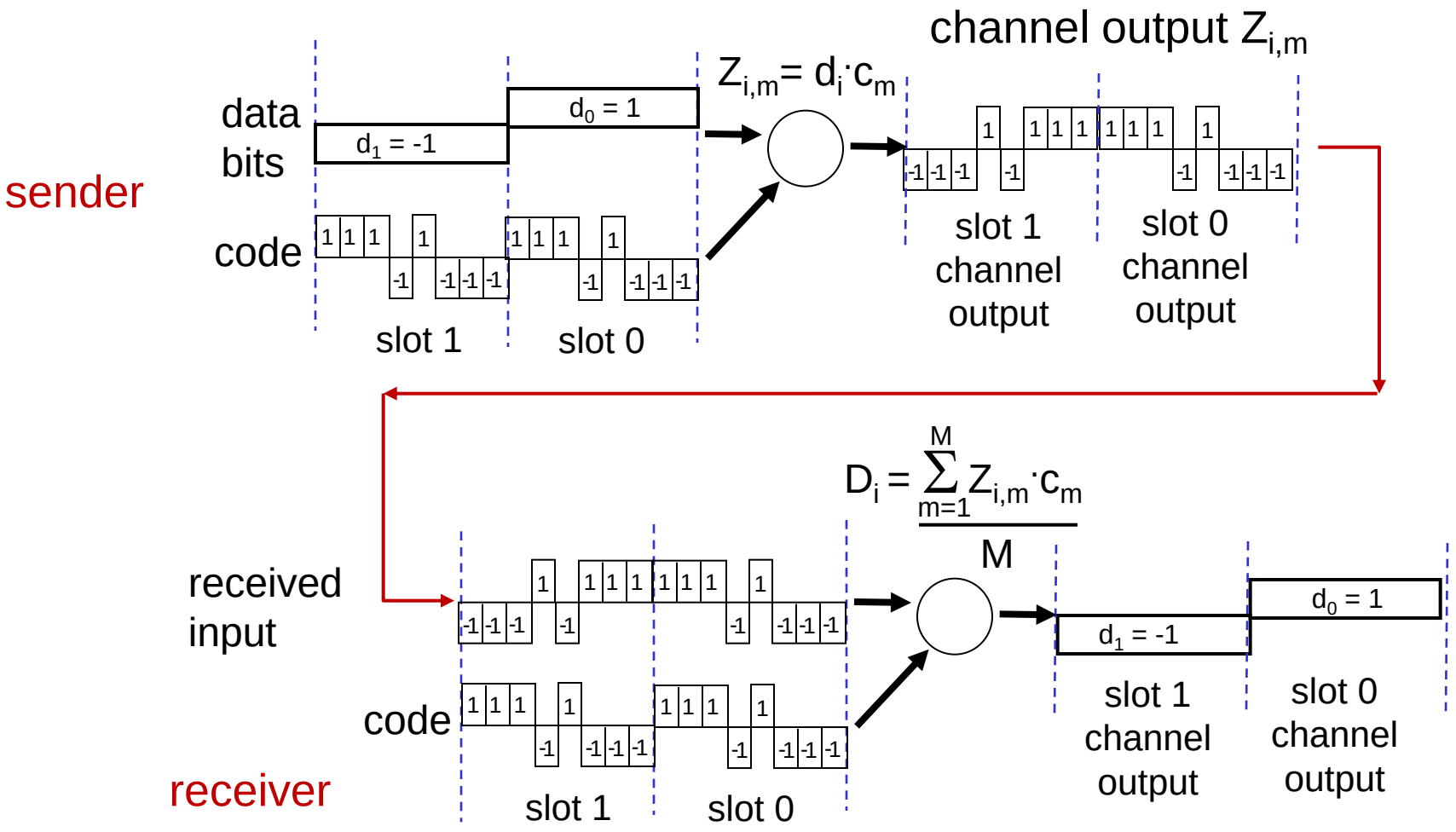
Signal attenuation:

- B, A hear each other
- B, C hear each other
- A, C can not hear each other interfering at B

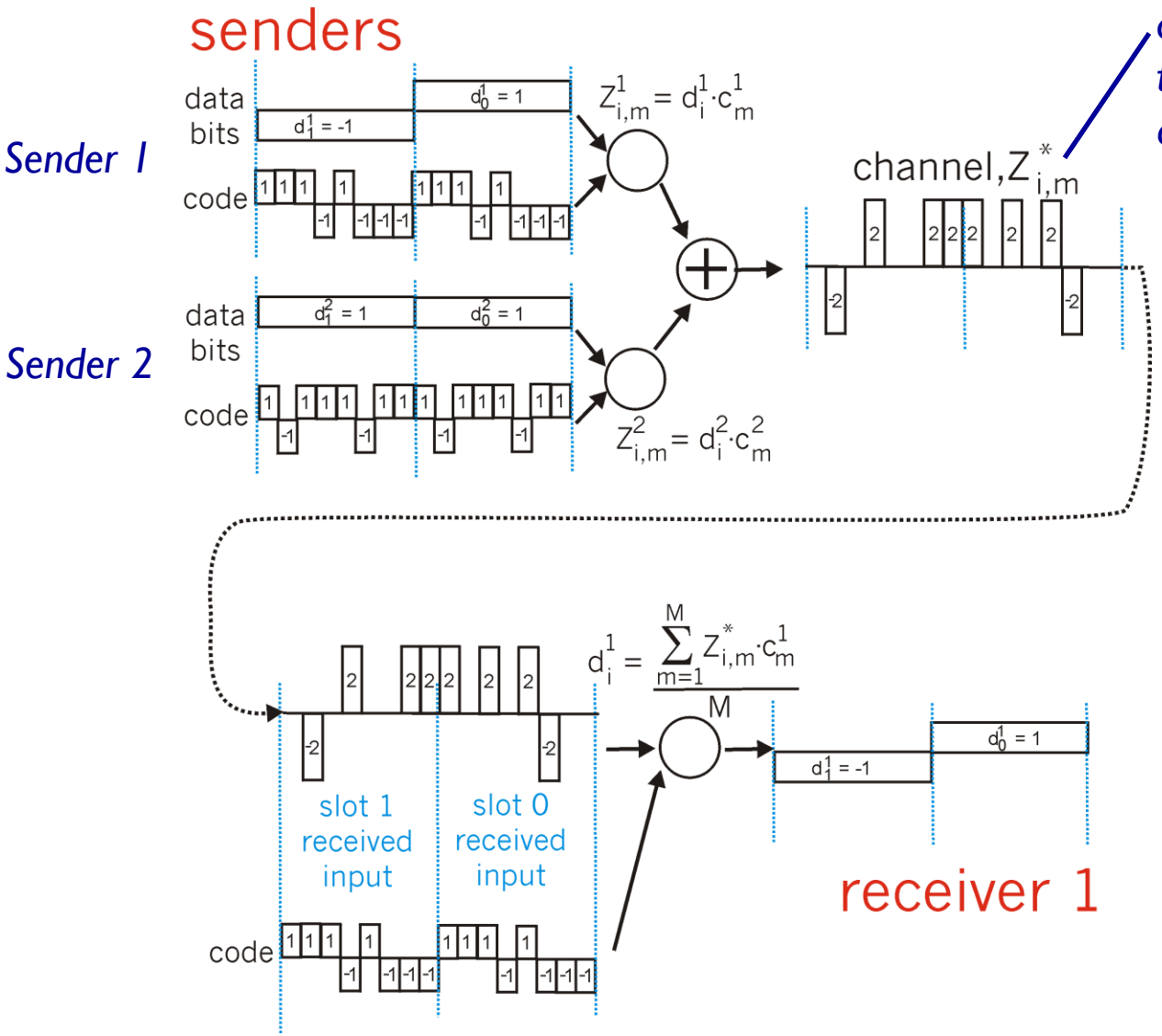
Code Division Multiple Access (CDMA)

- unique "code" assigned to each user; i.e., code set partitioning
  - all users share same frequency, but each user has own "chipping" sequence (i.e., code) to encode data
  - allows multiple users to "coexist" and transmit simultaneously with minimal interference (if codes are "orthogonal")
- *encoded signal* = (original data) X (chipping sequence)
- *decoding:* inner-product of encoded signal and chipping sequence

CDMA encode/decode



CDMA: two-sender interference

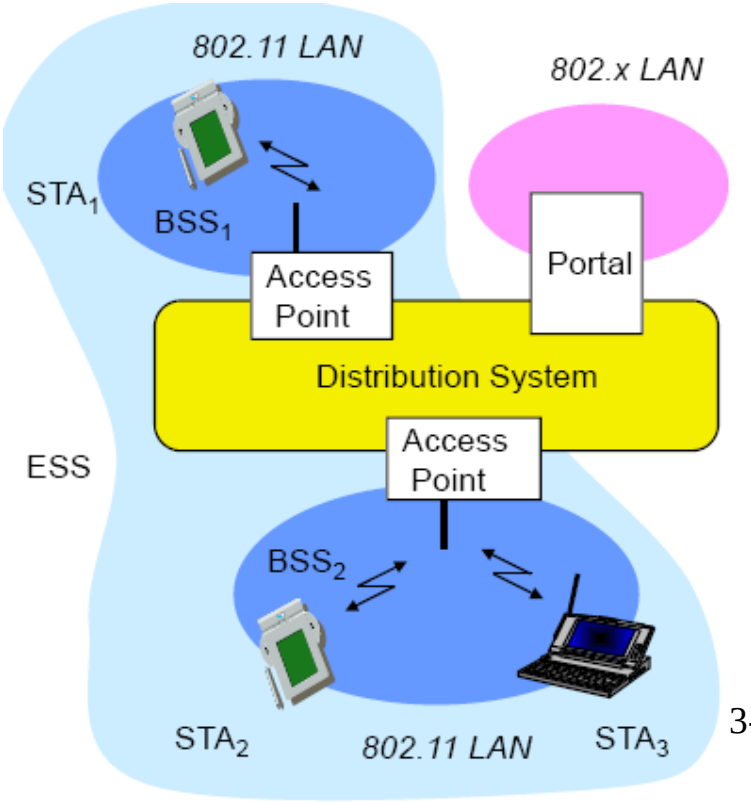


Challenges in Cellular Networks

- Explosion of mobile phones, 1.5billion users (2004)
- Scalability issues (particularly at radio network controller)
  - Better architecture design
- Lack of bandwidth (we need mobile TV)
  - Give us more spectrum

IEEE 802.11 - Architecture of an Infrastructure Network

- Station (STA)
  - Terminal with access mechanisms to the wireless medium and radio contact to the access point
- Basic Service Set (BSS)
  - Group of stations using the same radio frequency
- Access Point
  - Station integrated into the wireless LAN and the distribution system
- Portal
  - bridge to other (wired) networks
- Distribution System
  - Interconnection network to form one logical network



Challenges in WiFi

- Again, explosion of users, devices…
- Interference, interference, interference
  - Heavy interference /contention when accessing the AP, no QoS support
  - Inter-AP interference
  - Interference from other devices (microwave, cordless phones) in the same frequency band
- Mobility support
  - Seamless roaming when users move between APs
  - Normally low speed (3-10mph)

Challenges in Ad-hoc Networks

- A flexible network infrastructure
  - Peer-to-peer communications
  - No backbone infrastructure
  - Routing can be multi-hop
  - Topology is dynamic
- Challenges
  - Devices need to self-manage to survive
    - Manage interference (similar to WiFi but without AP, much harder)
    - Manage connectivity and routing (node mobility and unreliable links)
  - Transmission, access, and routing strategies for ad-hoc networks are generally ad-hoc
  - User collaboration is a good direction but there are always selfish / malicious users

How does Wireless affect Networking?

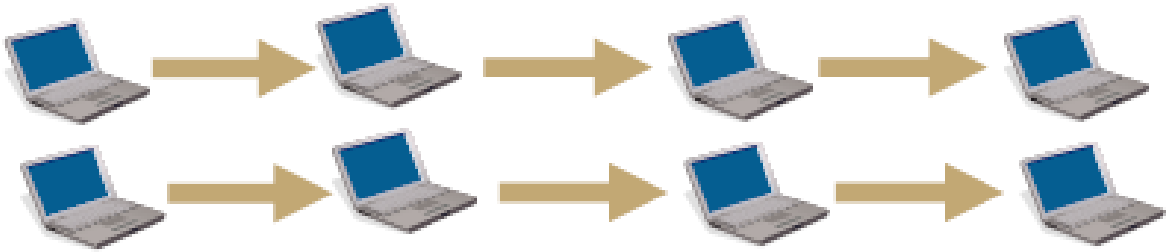
- Wireless access is different from Ethernet access
- Wireless routing is different from IP routing
- Wireless security is different from wired security

Wireless Access vs. Ethernet Access

- Ethernet: fixed connection, always on, stable, fixed rate
- Wireless: unreliable connection, competition based, fading/unreliable, dynamic rate, limited bandwidth
  - Critical: how to coordinate among devices to avoid interference
    - Cellular: centralized, base station tells each device when and how to send/receive data
    - WLAN + Ad hoc: distributed, CSMA, compete and backoff
  - Mobility
    - neighbor discovery + topology control
  - Rate adaptations

Wireless Routing vs. Wired Routing

- Aside from traditional multi-hop routing
  - Mobility: route discovery and maintenance
  - Interference, interference, interference
    - Multi-hop interference mitigation
    - Spectrum assignment, multi-channel networks



So far

- Understand different types of wireless networks:
  - WPAN, WLAN, WWAN, WMAN and their challenges
- Understand the difference between infrastructure and ad hoc networks
- Understand the challenges in MAC, networking …

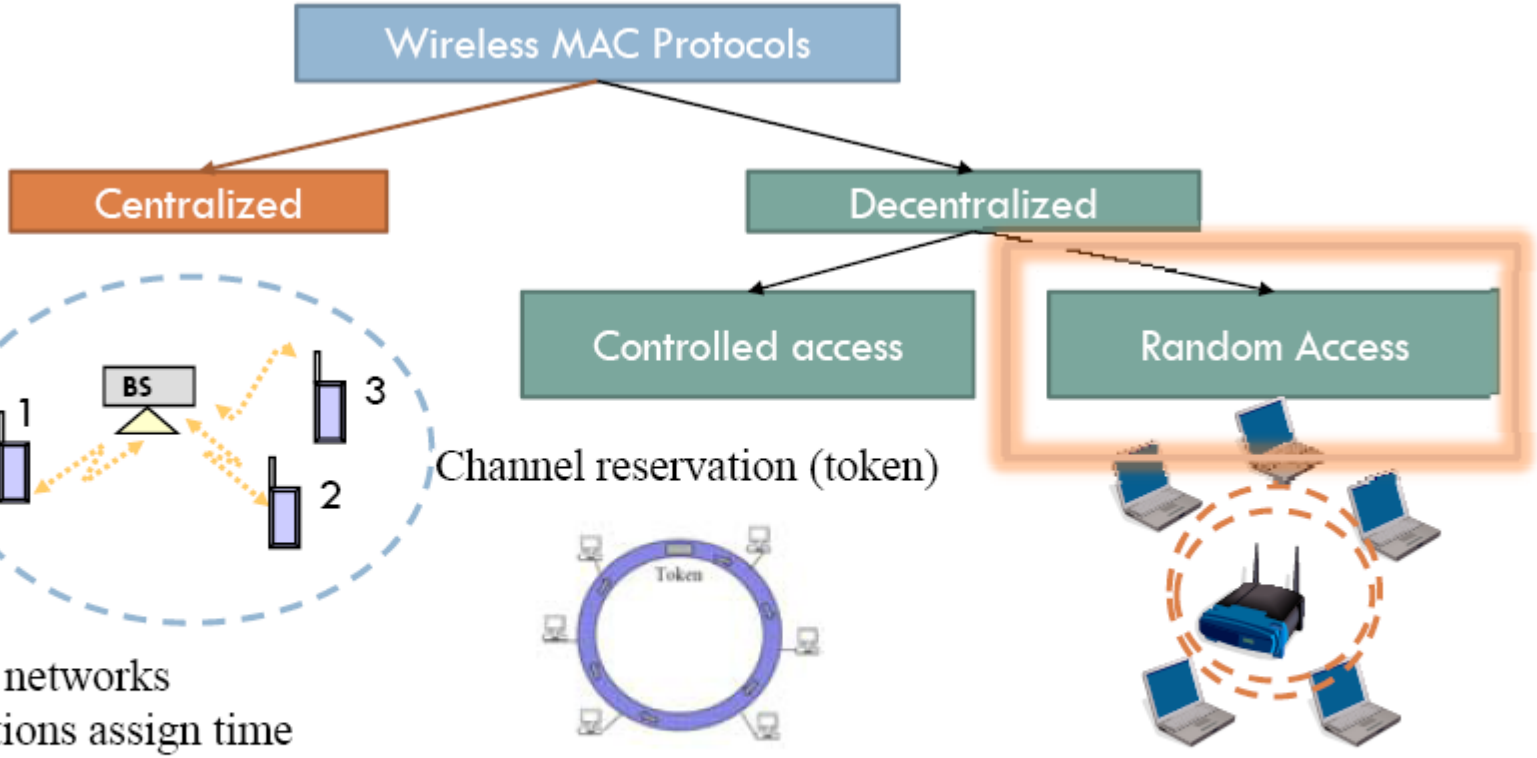
Outline

- Overview
- **MAC**
- Routing
- Wireless in real world
- Leverage broadcasting nature
- Explore the characteristic of wireless signal

Why Control Medium Access

- Wireless channel is a shared medium
  - When conflict, interference disrupts communications
- Medium access control (MAC)
  - Avoid interference
  - Provide fairness
  - Utilize channel variations to improve throughput
    - Independent link variations

MAC Categories

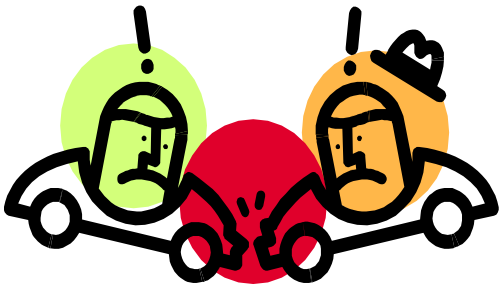


Cellular networks
base stations assign time slots/frequencies/codes to users
TDMA, FDMA, CDMA

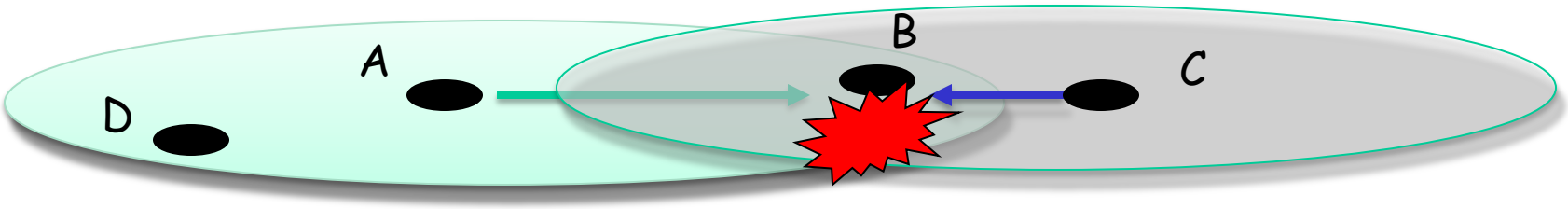
1) Aloha
2) 802.11, CSMA/CA, backoff if conflict
3) Ethernet, CSMA/CD

Random Access

- Random Access vs. Controlled Access
  - No fixed schedule, no special node to coordinate
  - Distributed algorithm to determine how users share channel, when each user should transmit
- Challenges: two or more users can access the same channel simultaneously → Collisions
- Protocol components:
  - How to detect and avoid collisions
  - How to recover from collisions

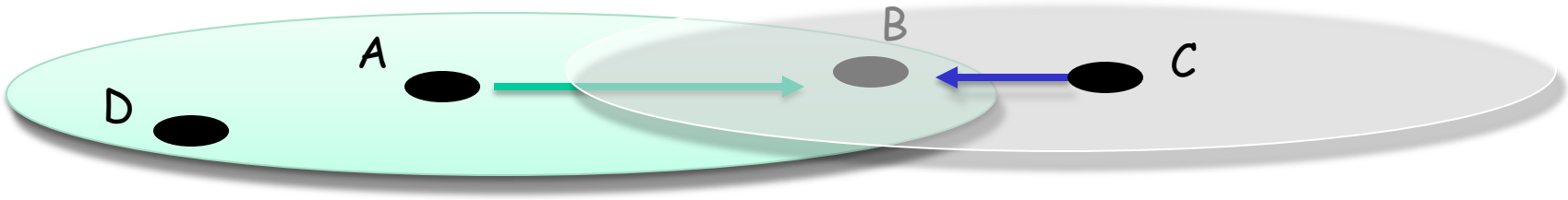


Collision Detection Difficult



- Signal reception based on SINR
  - Transmitter can only hear itself
  - Cannot determine signal quality at receiver

Calculating SINR

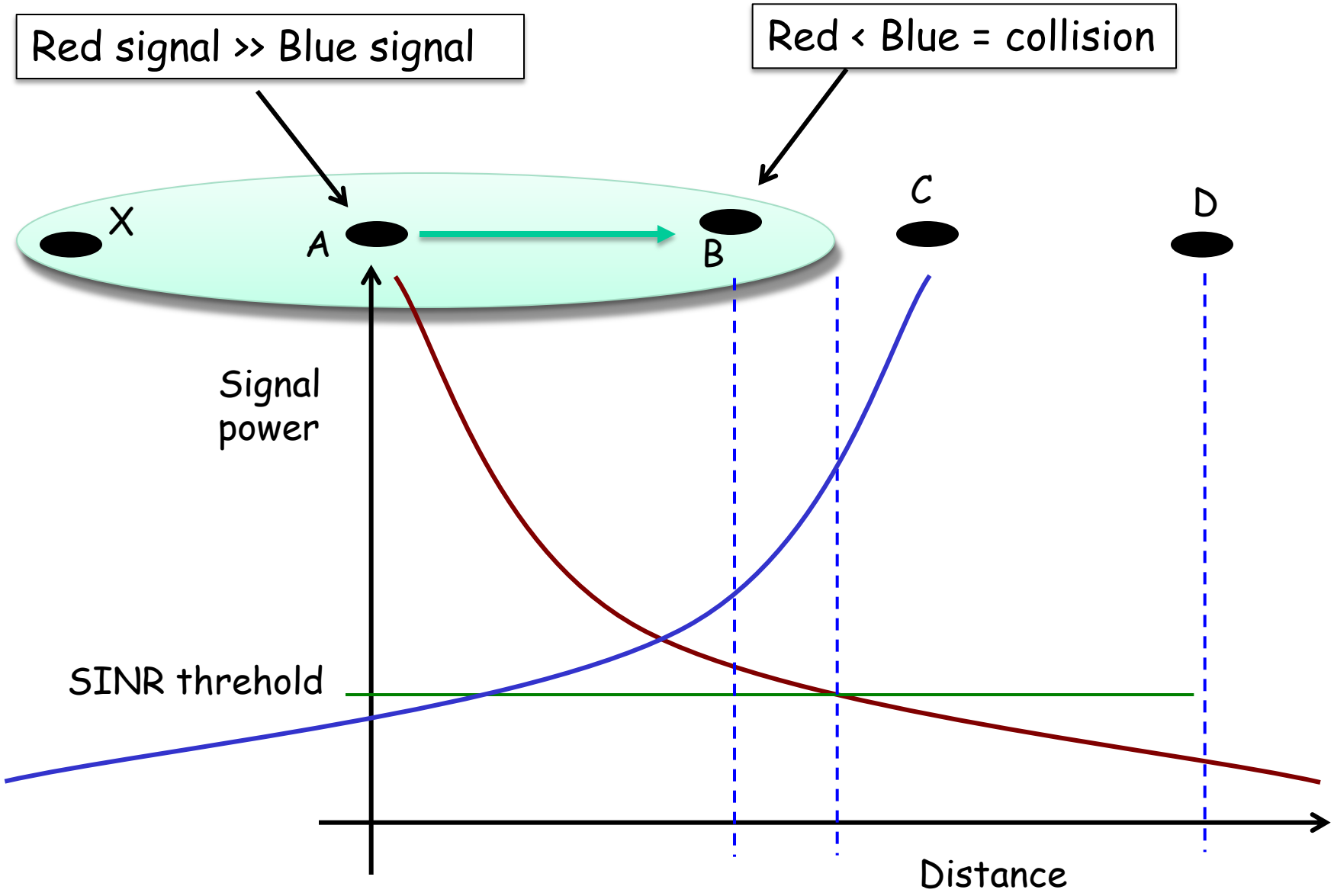


$$SINR = \frac{SignalOfInterest(SoI)}{Interference(I) + Noise(N)}$$

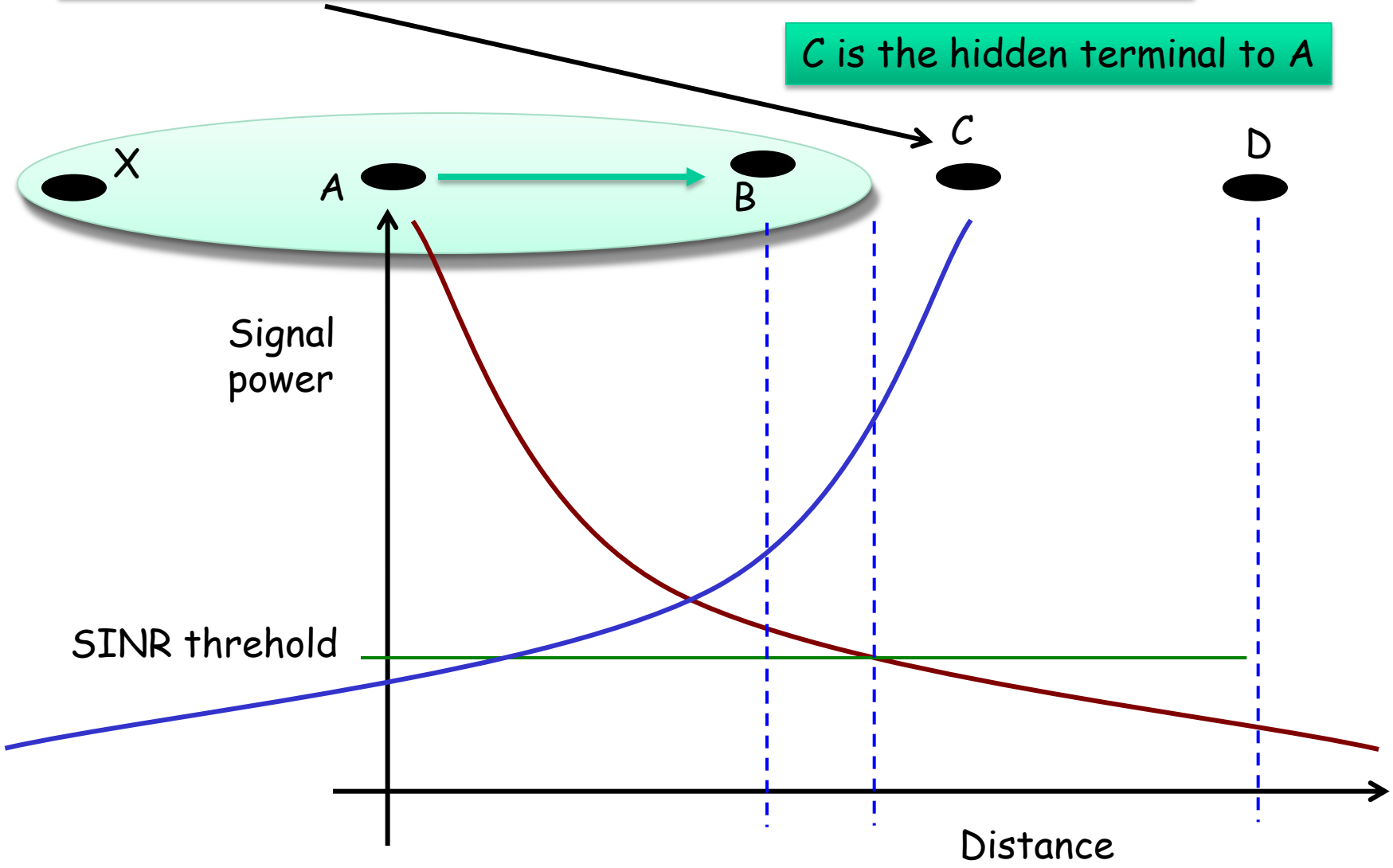
$$SoI_B^A = \frac{P^A_{transmit}}{d^{\alpha}_{AB}}$$

$$I_B^C = \frac{P^C_{transmit}}{d^{\alpha}_{CB}}$$

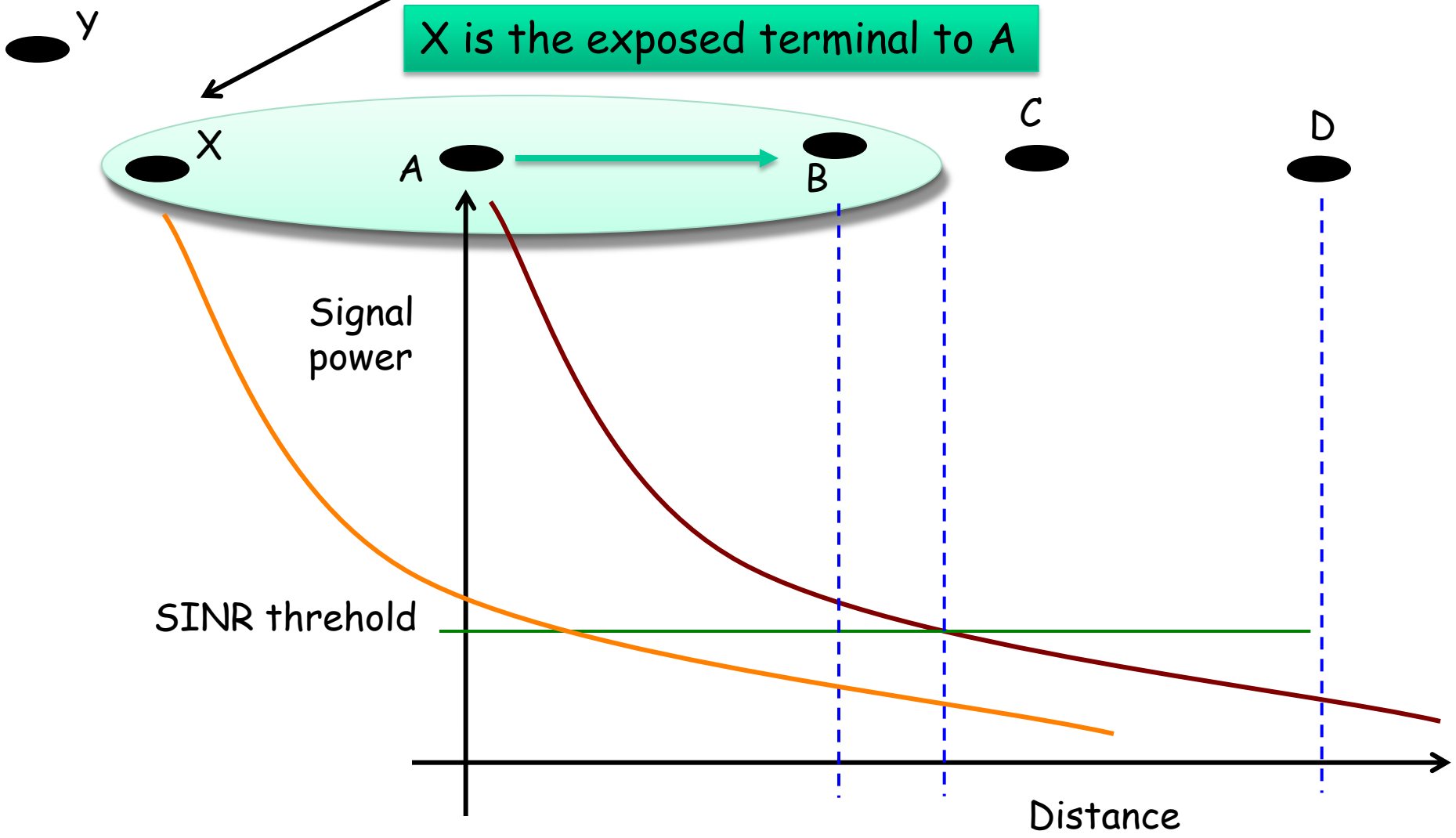
$$SINR_B^A = \frac{\frac{P^A_{transmit}}{d^{\alpha}_{AB}}}{N + \frac{P^C_{transmit}}{d^{\alpha}_{CB}}}$$


Red signal >> Blue signal
Red < Blue = collision
X
A
B
C
D
Signal power
SINR threhold
Distance

Important: C has not heard A, but can interfere at receiver B



Important: X has heard A, but should not defer transmission to Y



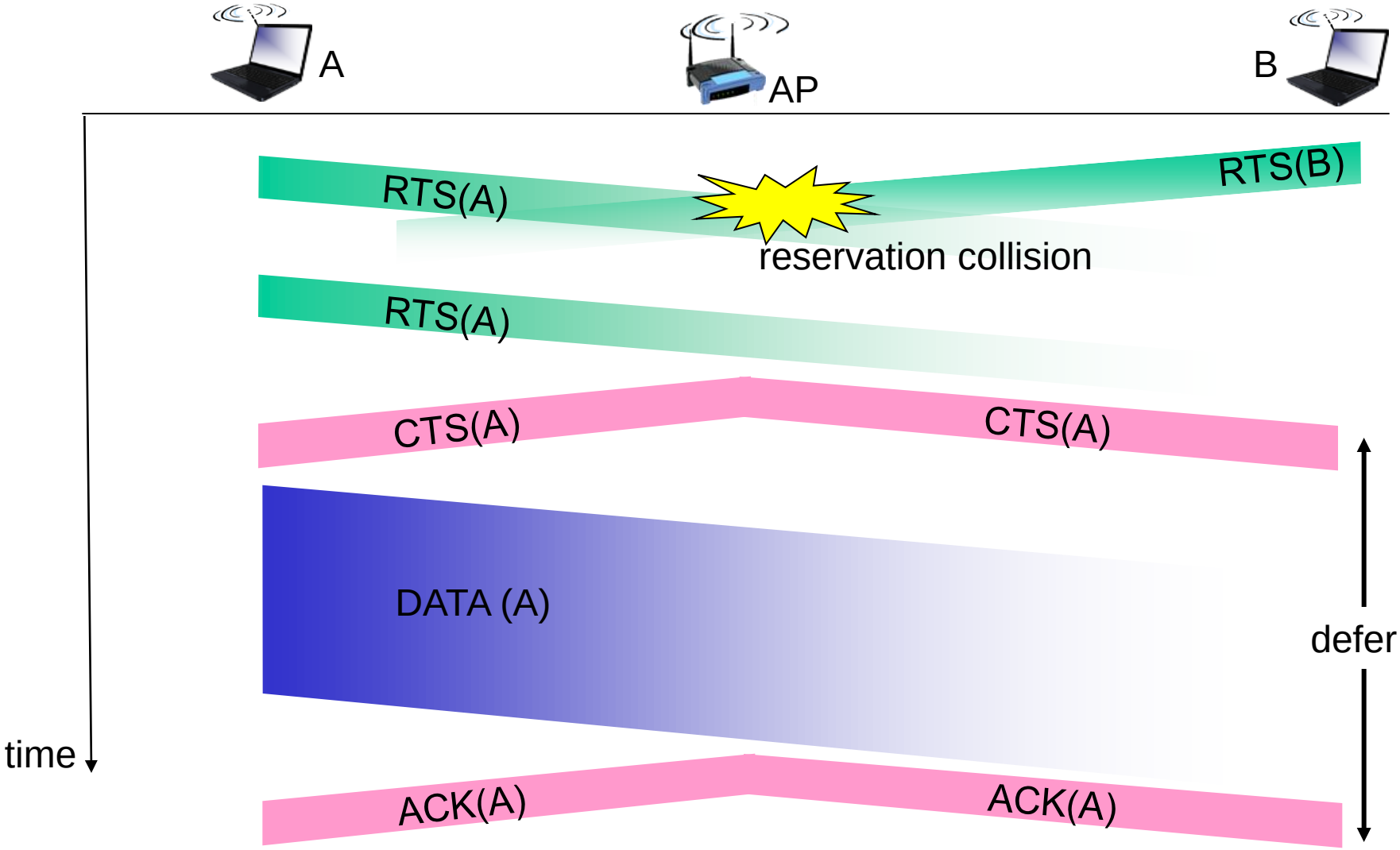
CSMA/CA-Avoiding Collisions

Idea: allow sender to "reserve" channel rather than random access of data frames: avoid collisions of long data frames

- Sender first transmits *small* request-to-send (RTS) packets to BS using CSMA
- BS broadcasts clear-to-send CTS in response to RTS
- RTS heard by all nodes
  - Sender transmits data frame
  - Other stations defer transmissions

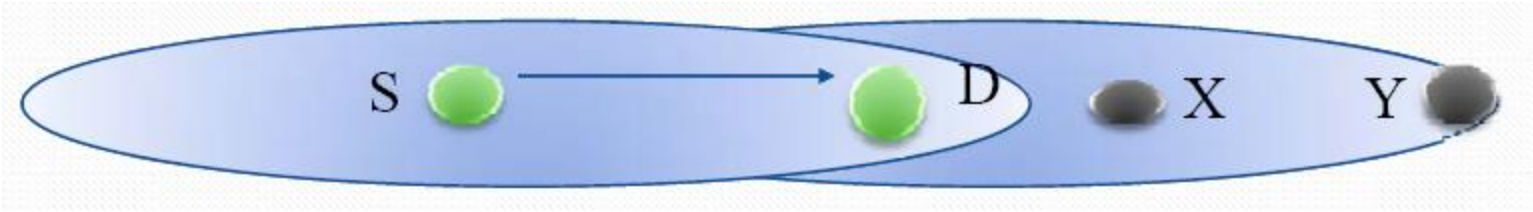
avoid data frame collisions completely using small reservation packets!

Collision Avoidance: RTS-CTS exchange



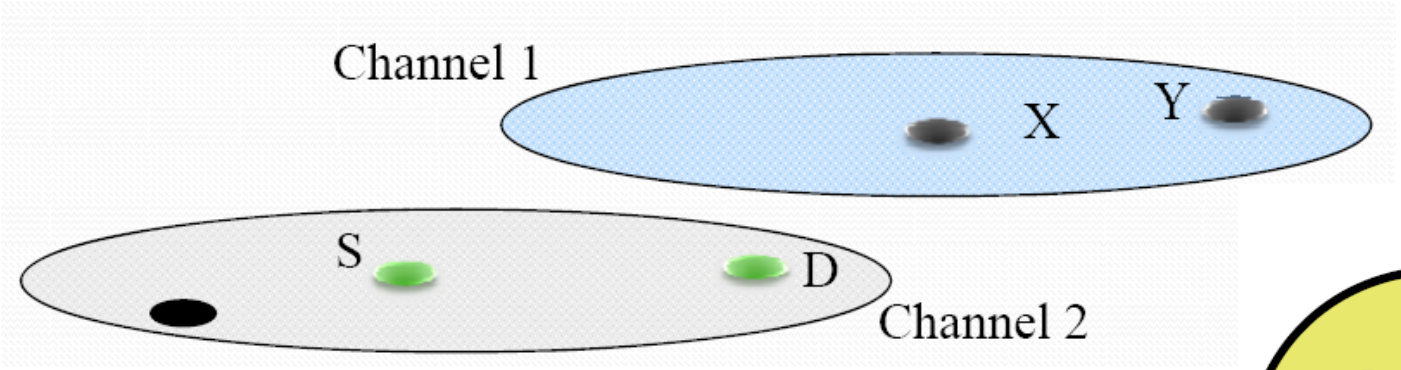
Problems with Single Channel

- Collisions happen to RTS and CTS too
- Bandwidth is limited
- Are there alternatives to avoid interference??

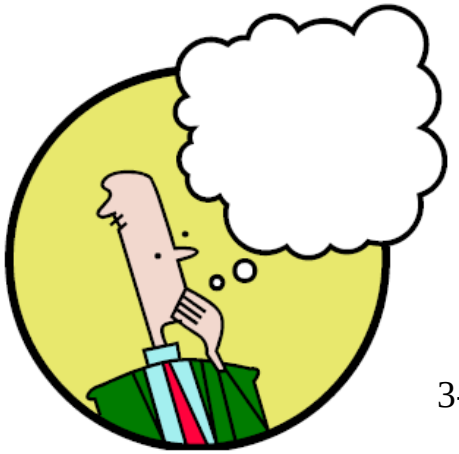


Multiple Channel Motivation

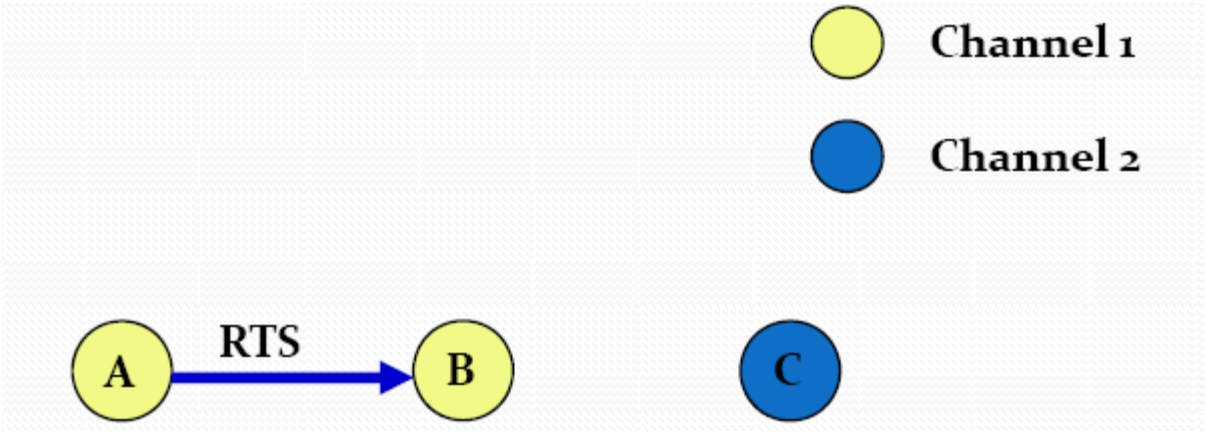
- Ways to avoid interference
  - Time
  - Space
  - Frequency/channel



How to coordinate among users which channel to use?

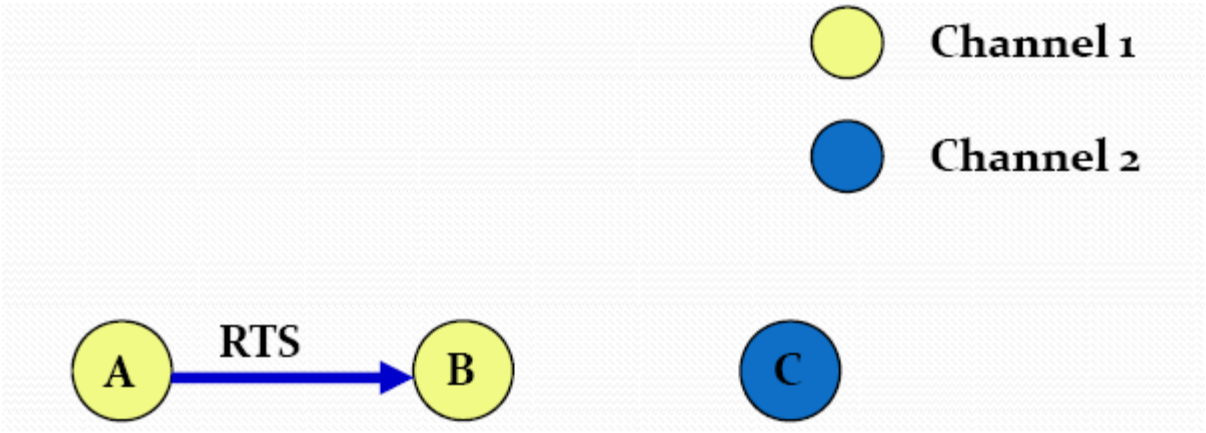


Multi-Channel Hidden Terminals



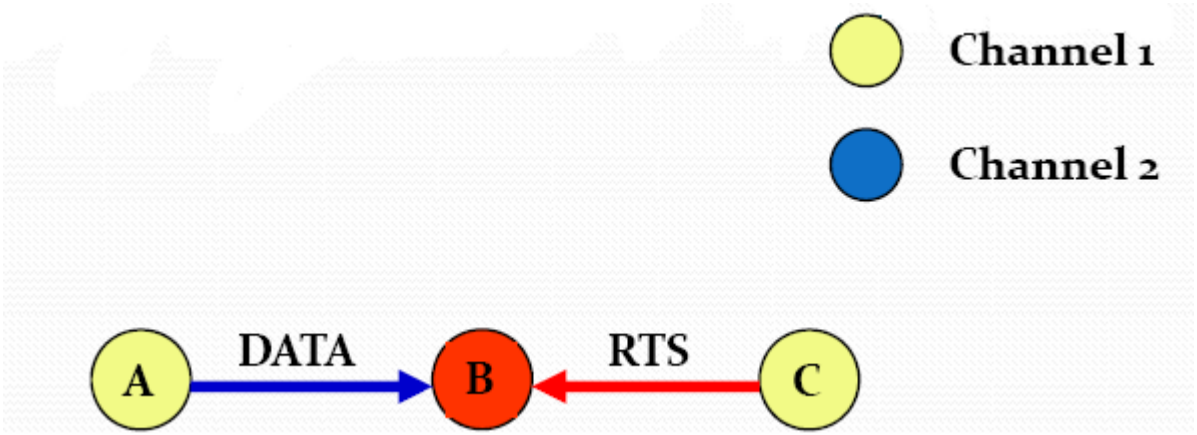
A sends RTS

Multi-Channel Hidden Terminals



B sends CTS
C does not hear CTS because C is listening on channel 2

Multi-Channel Hidden Terminals



C switches to channel 1 and transmits RTS
Collision occurs at B

How to coordinate the channel usage?

Solution 1: Add a Control Radio

- Each user has two radios
  - Radio 1: control radio; users exchange control information – which channel to use for their data radio
  - Radio 2: data radio; transmit packets
- Pro:
  - Simple; instantaneous coordination
- Con:
  - Need an extra radio; bandwidth wasted..

Wu's Protocol [Wu00ISPAN]

- Assumes 2 transceivers per host
  - One transceiver always listens on control channel
- Negotiate channels using RTS/CTS/RES
  - RTS/CTS/RES packets sent on control channel
  - Sender includes preferred channels in RTS
  - Receiver decides a channel and includes in CTS
  - Sender transmits RES (Reservation)
  - Sender sends DATA on the selected data channel

What if each user only has one radio????

Solution 2: Add a control slot

- Each user transmits in two phases
  - Phase I: users exchange control information – which channel to use for their data transmission
  - Phase II: transmit packets on the pre-determined channel
- Pro:
  - Only need one radio…
- Con:
  - Need synchronization;
  - Only periodic coordination

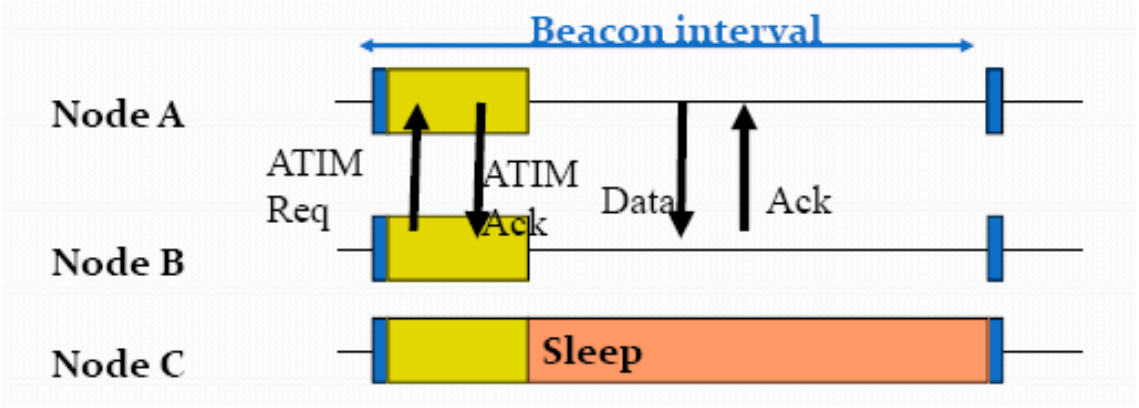
An example of Solution 2: MMAC

- Assumptions
  - Each node is equipped with a single transceiver
  - The transceiver is capable of switching channels
  - Channel switching delay is approximately 250us
    - Per-packet switching not recommended
    - Occasional channel switching not too expensive
  - Multi-hop synchronization is achieved by other means

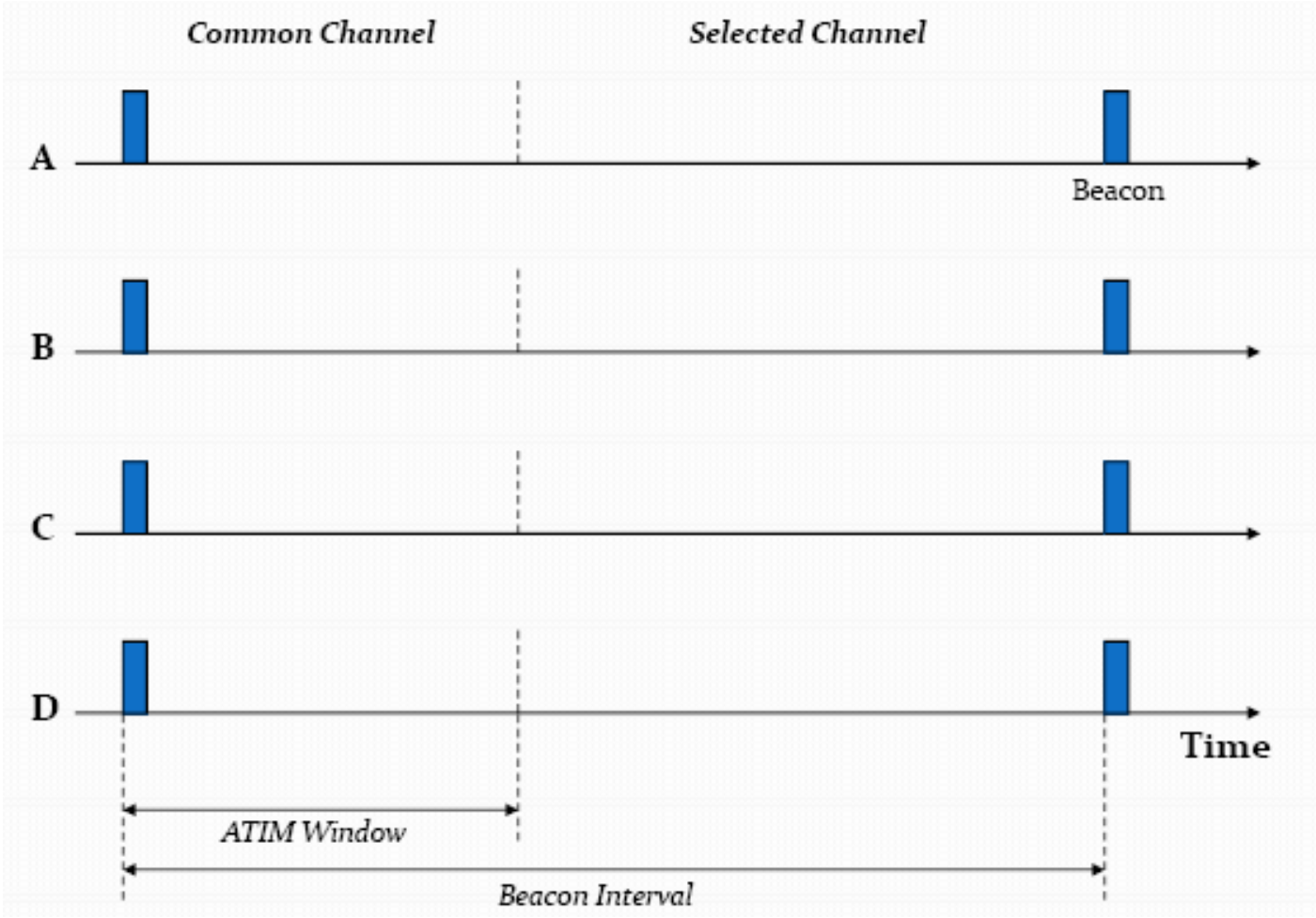
[so04] J. So and N. Vaidya, Multi-channel MAC for Ad Hoc Networks: Handling Multi-channel Hidden Terminals with a Single Transceiver, Mobihoc 2004.

Power Saving in 802.11 Ad hoc Mode

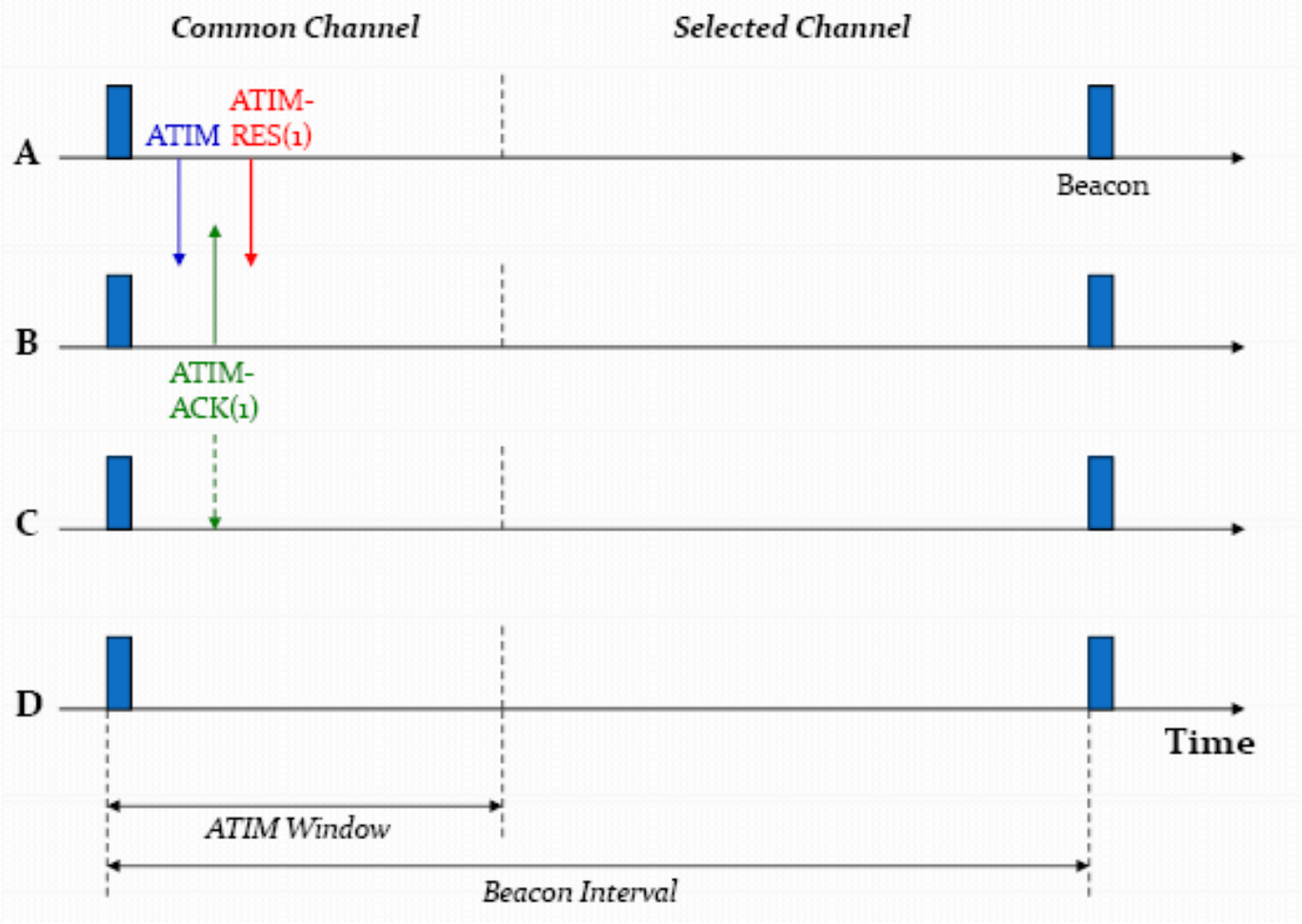
- Time is divided into beacon intervals
- Each beacon interval begins with an ATIM window
- If host A has a packet to transmit to B, A must send an ATIM Request to B during an ATIM Window
- If a host does not receive an ATIM Request during an ATIM window, and has no pending packets to transmit, it may sleep during rest of the beacon interval



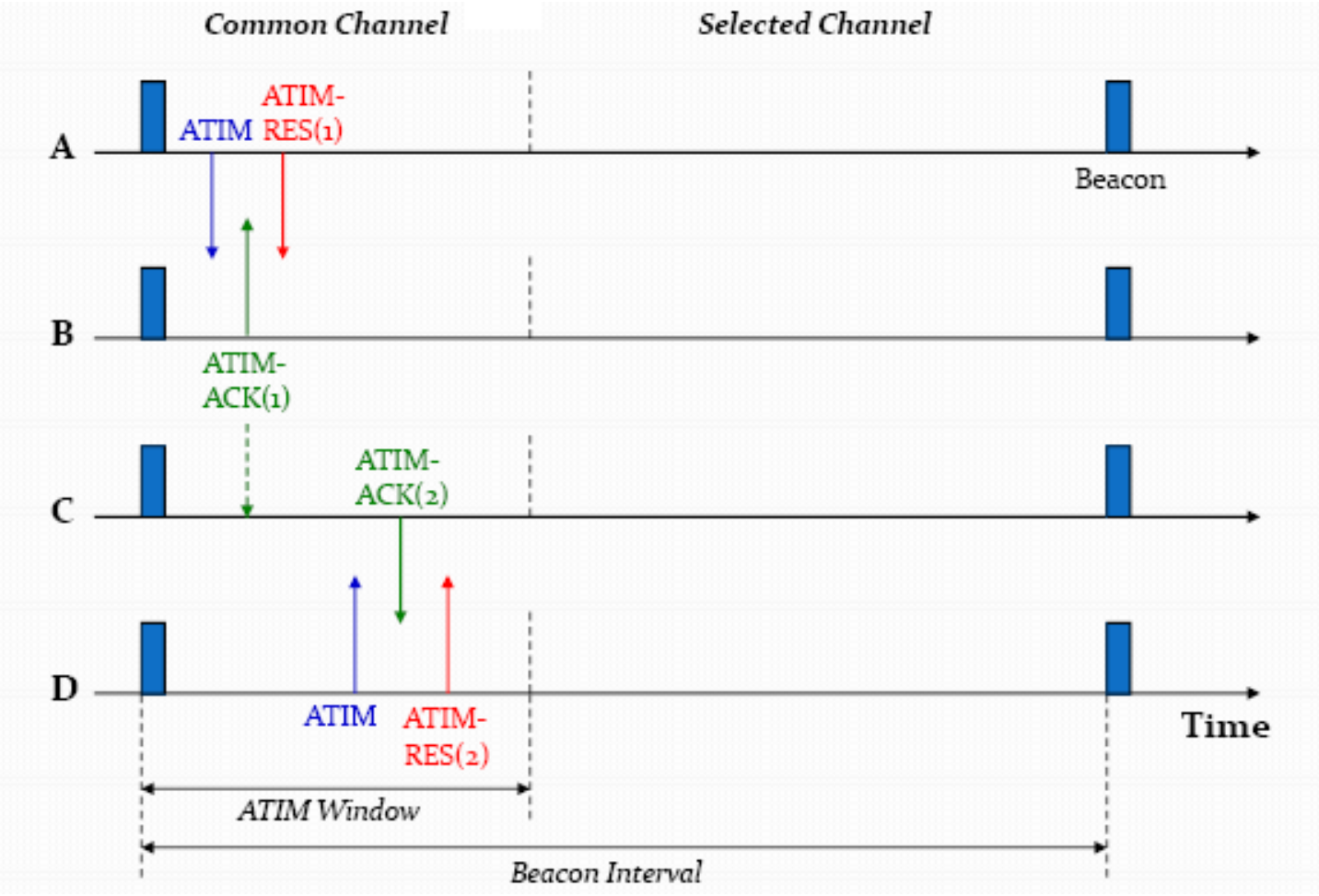
Channel Negotiation



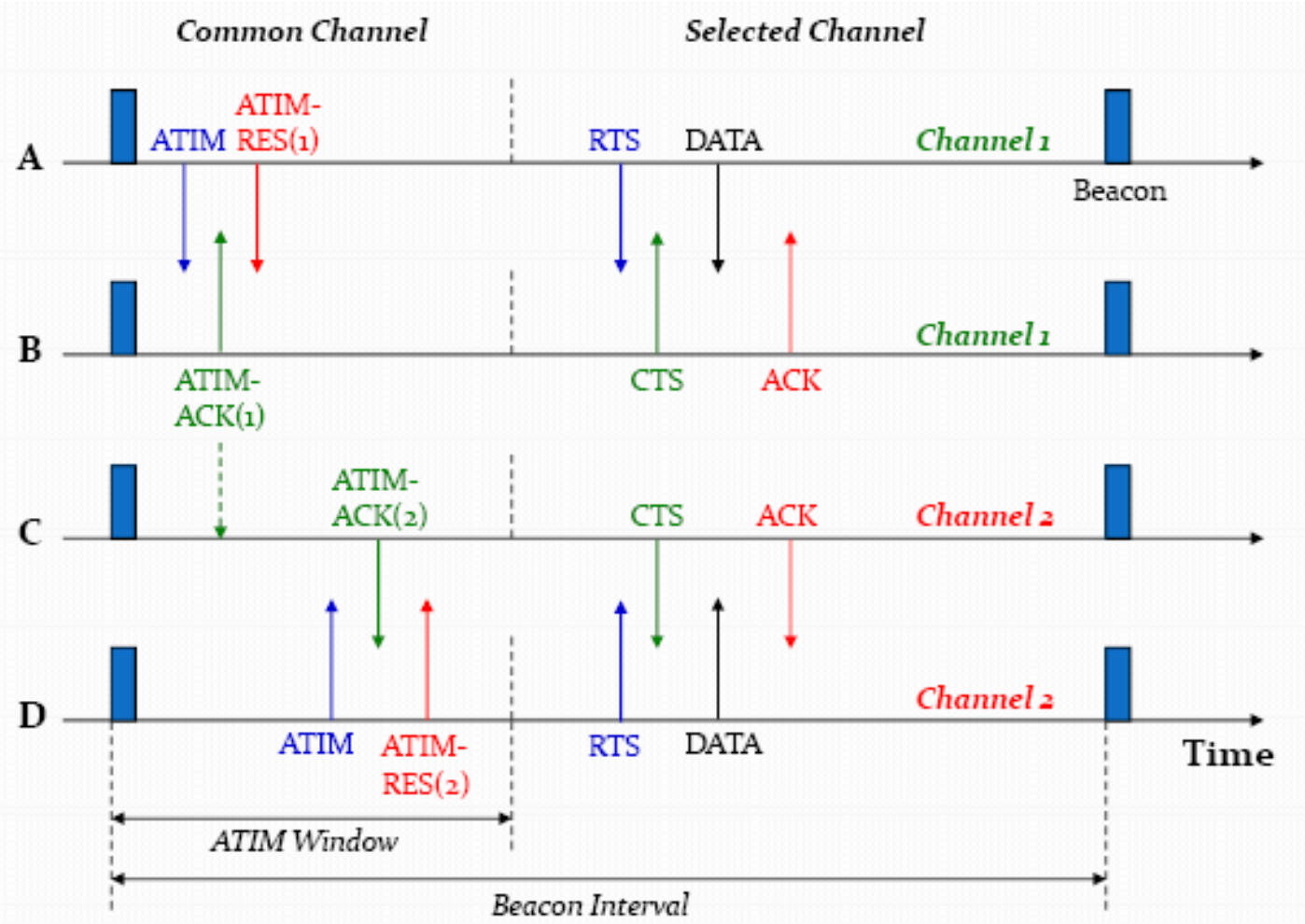
Channel Negotiation



Channel Negotiation



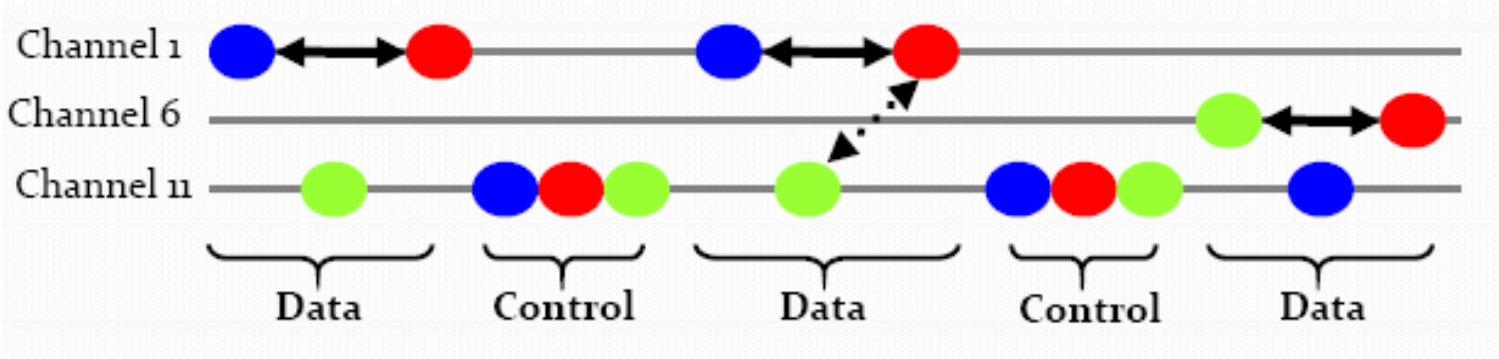
Channel Negotiation



QUESTION:
WHAT IS THE LIMITATION OF MMAC??

MMAC

MMAC Basic idea:
Periodically rendezvous on a fixed channel to decide the next channel



Issues

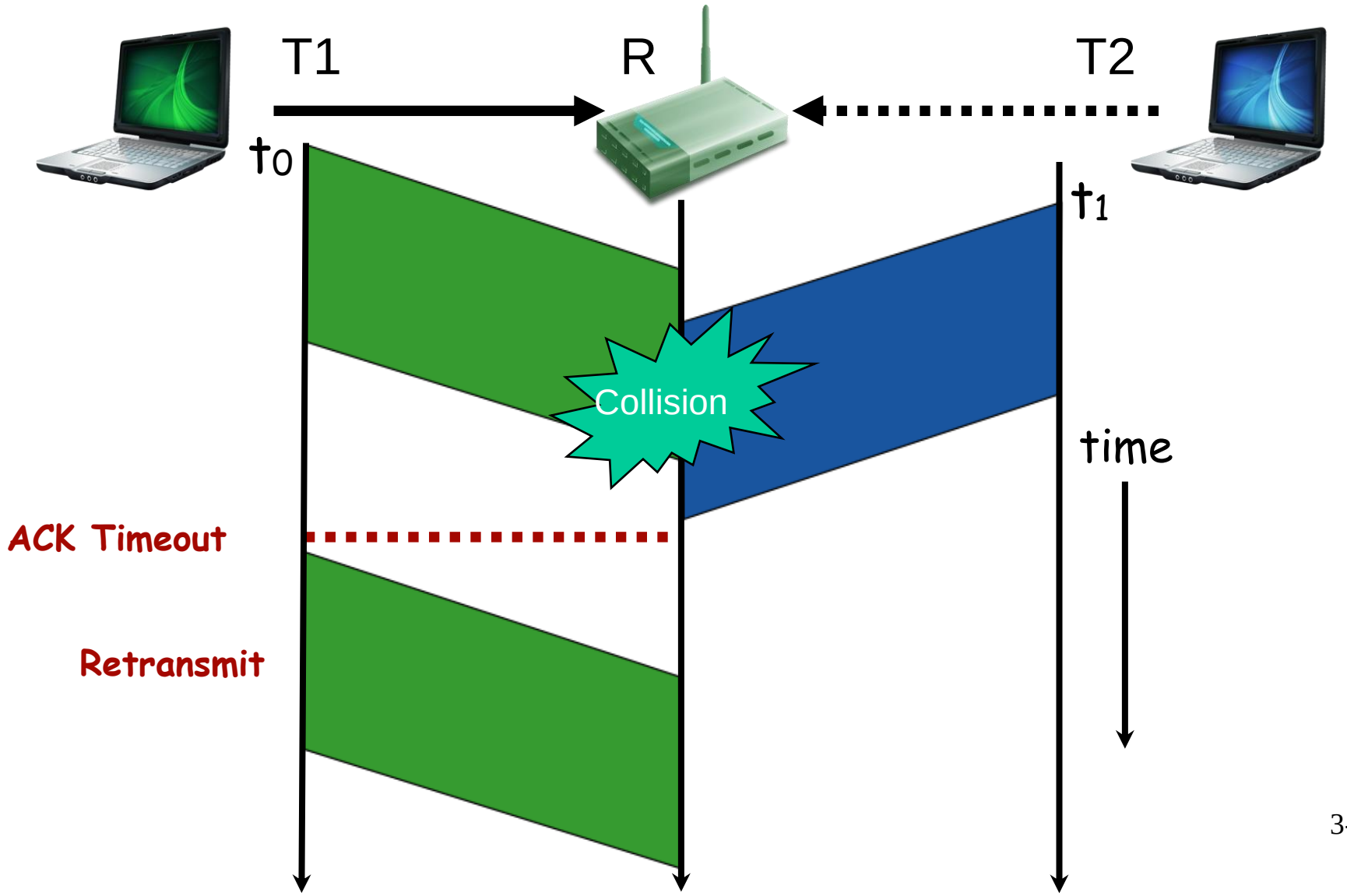
- Packets to multiple destinations ⇒ high delays
- Control channel congestion

CSMA/CN: Carrier Sense Multiple Access with Collision Notification

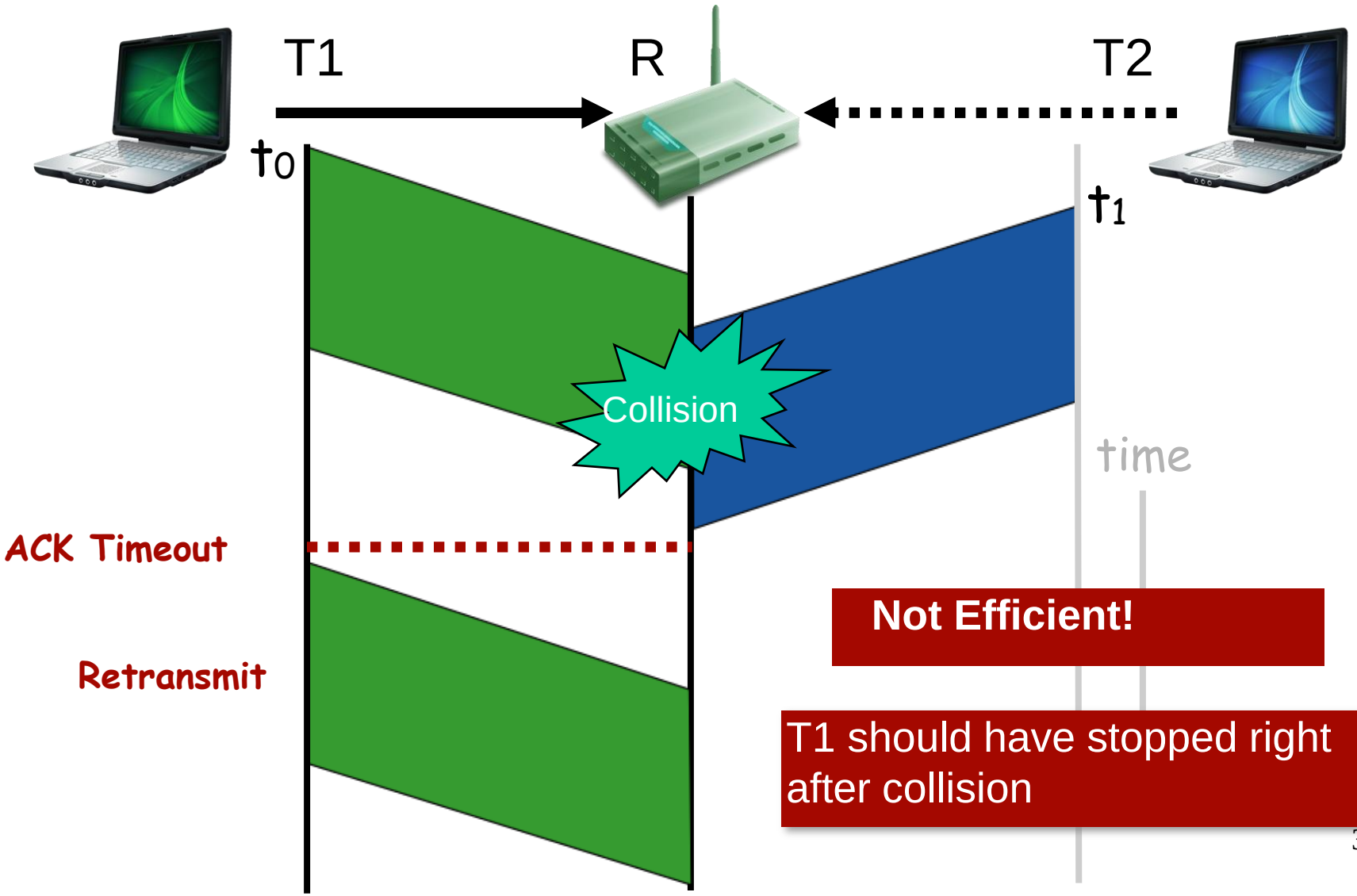
Souvik Sen,
Naveen Santhapuri, Romit Roy Choudhury, Srihari Nelakuditi

ACM Mobicom 2011

Collision in Wireless Networks



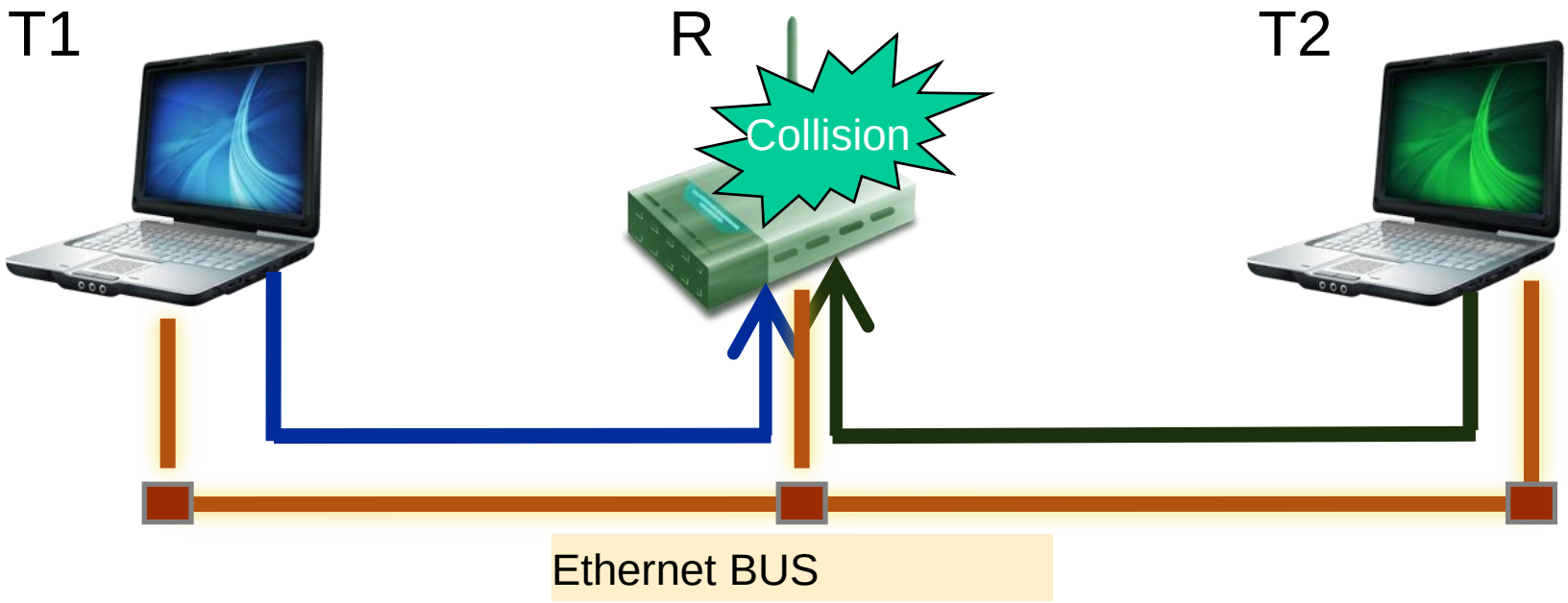
Collision in Wireless Networks



Not Efficient!

T1 should have stopped right after collision

Collision in Wired Networks



- Transmitter aborts transmission on collision
  - Transmitter senses the signal while transmitting
  - If **(sensed != transmitted)**, abort

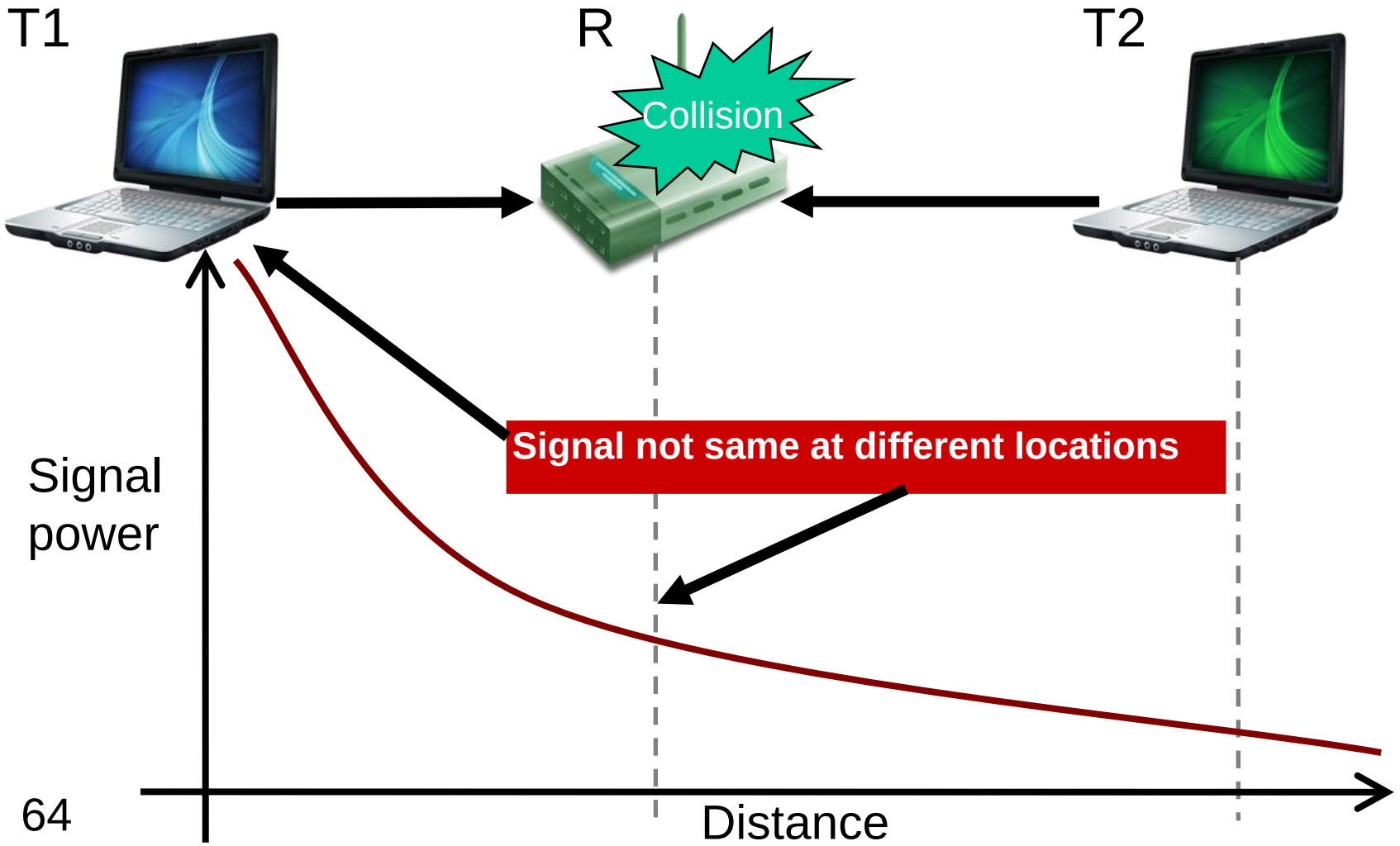
Collision Detection (CSMA/CD)

Can we do CSMA/CD in Wireless?

Seems hard because.....

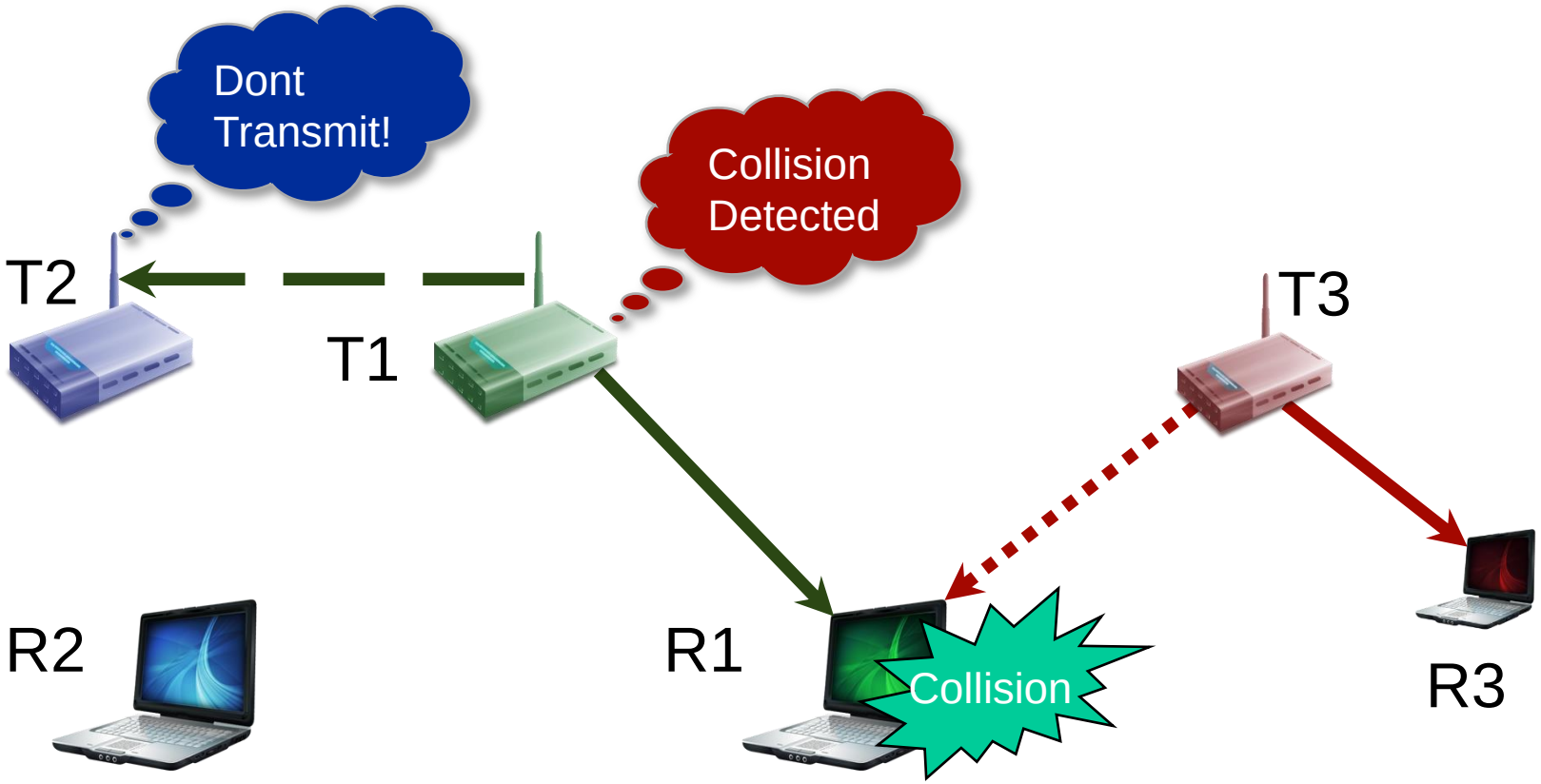
Wireless Signal Propagation

T1 cannot send and listen in parallel

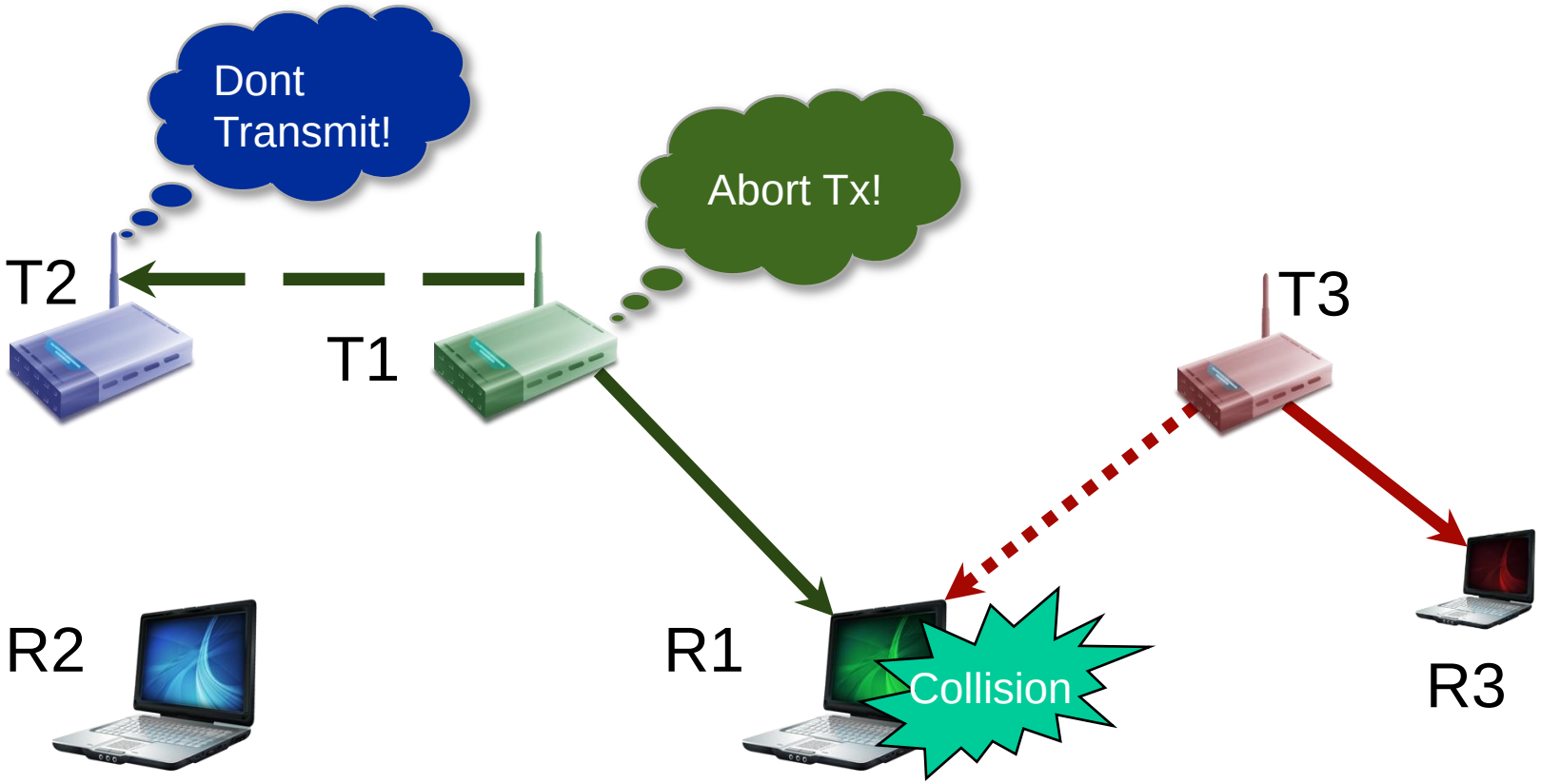


But what if we could do CSMA/CD in wireless?

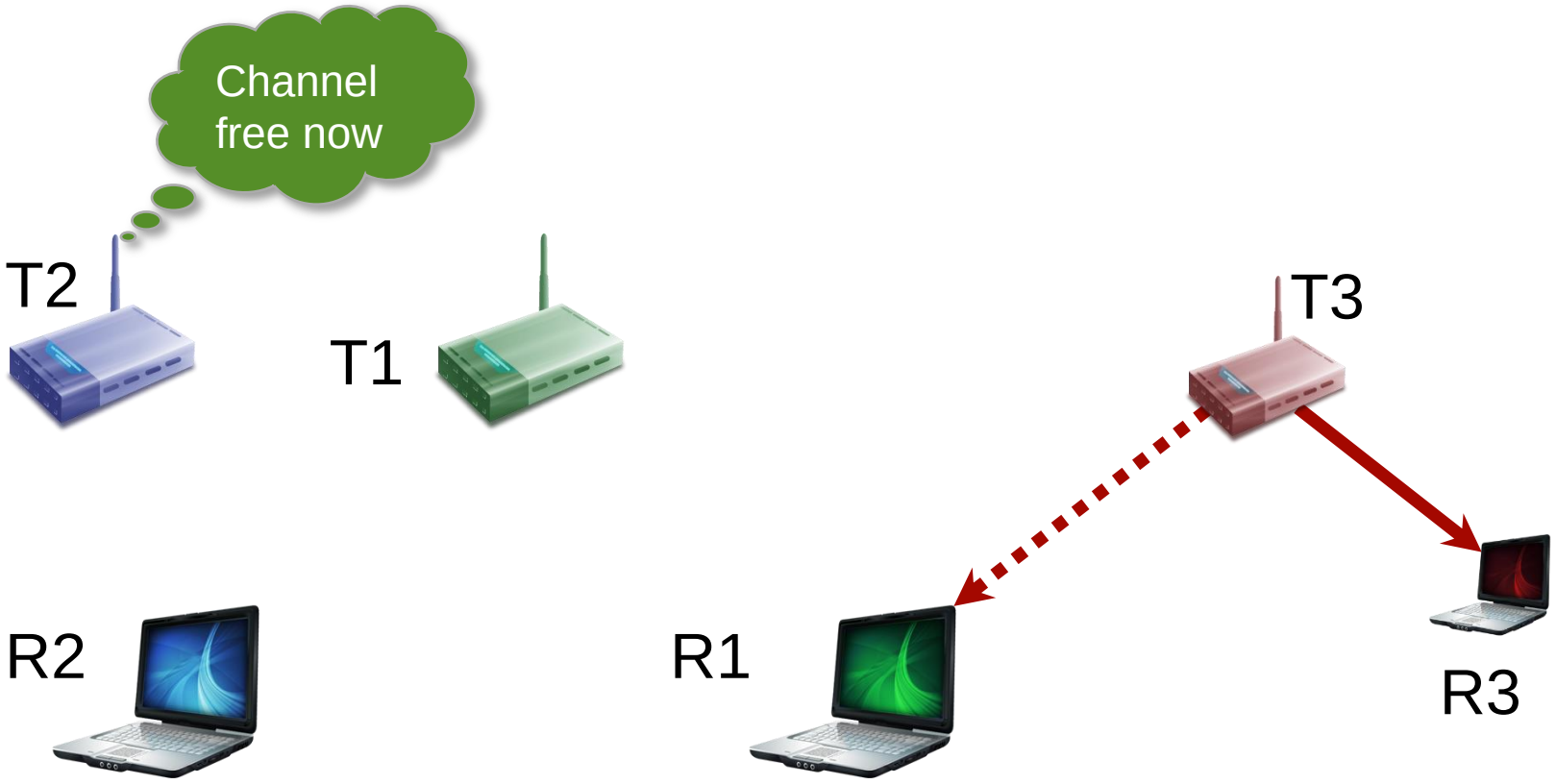
Is CSMA/CD Beneficial in Wireless?



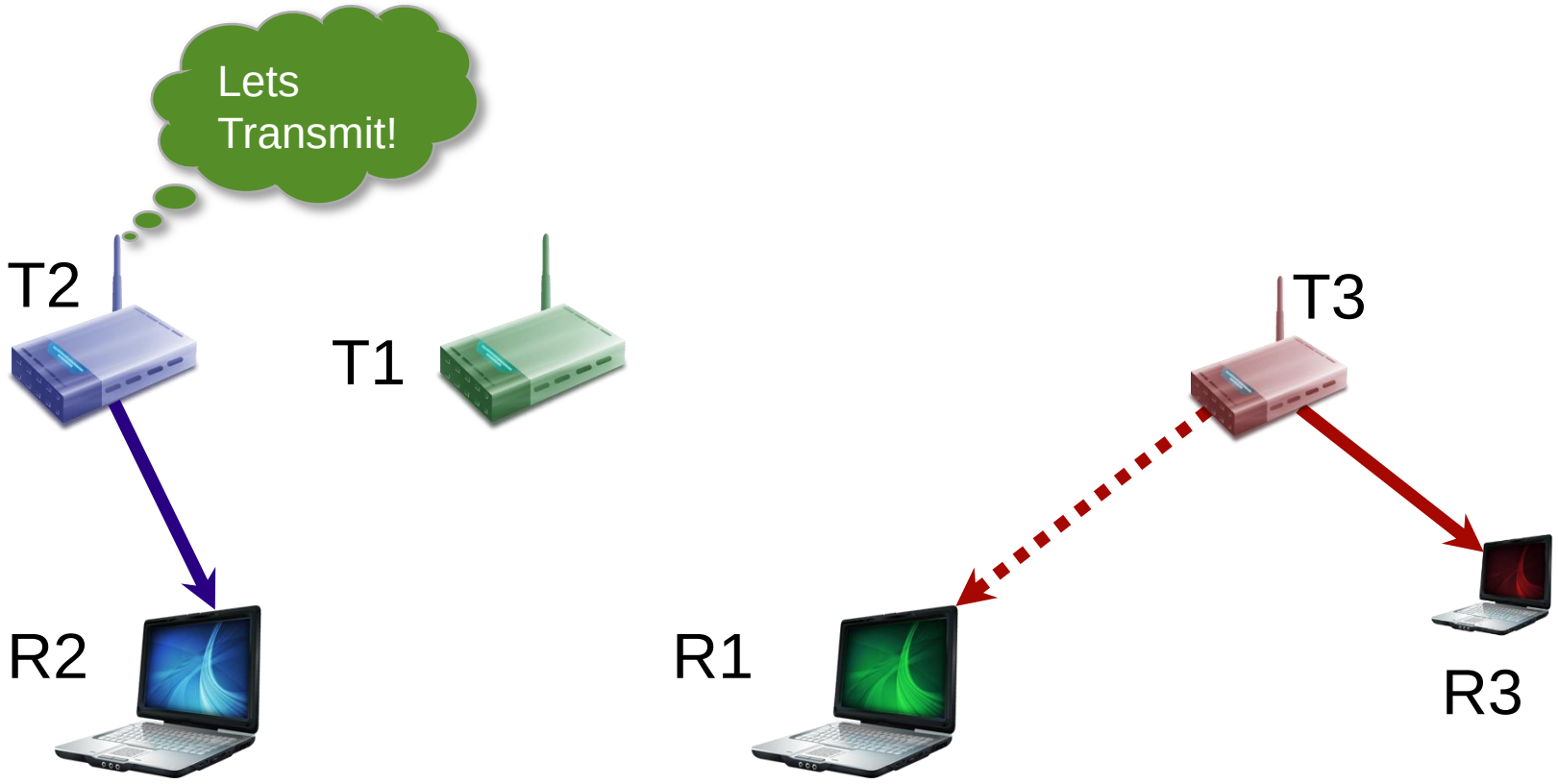
Is CSMA/CD Beneficial in Wireless?



Is CSMA/CD Beneficial in Wireless?



Is CSMA/CD Beneficial in Wireless?

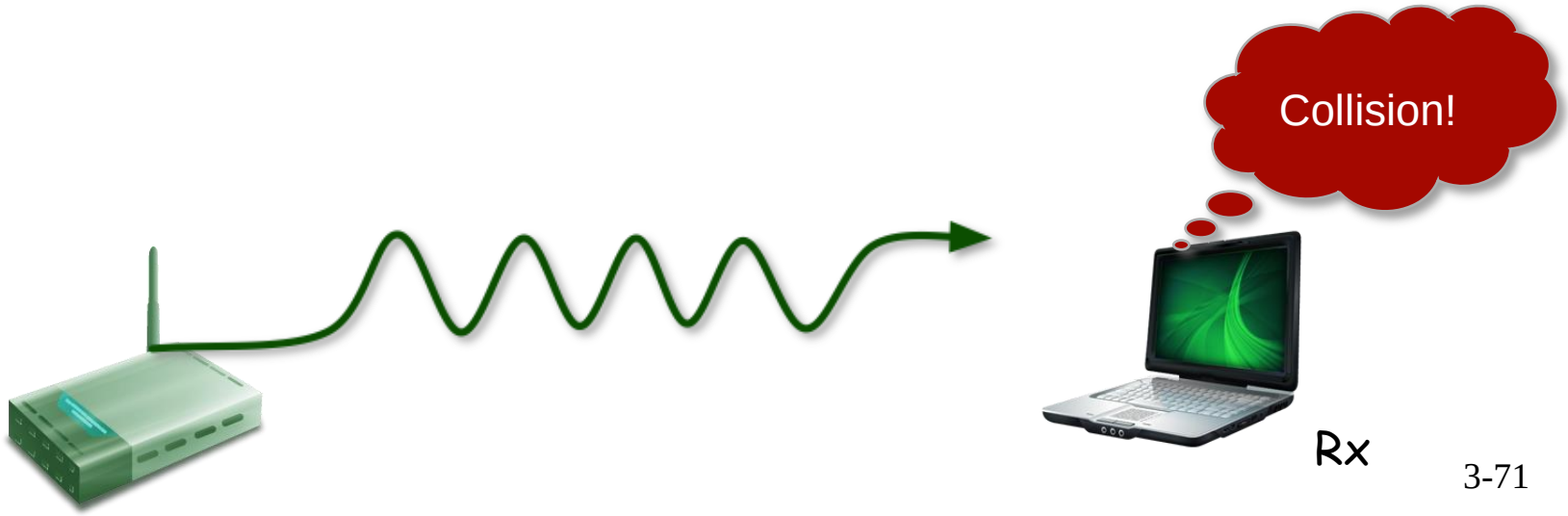


CSMA/CD frees the channel for other transmissions

Can we imitate CSMA/CD on Wireless?

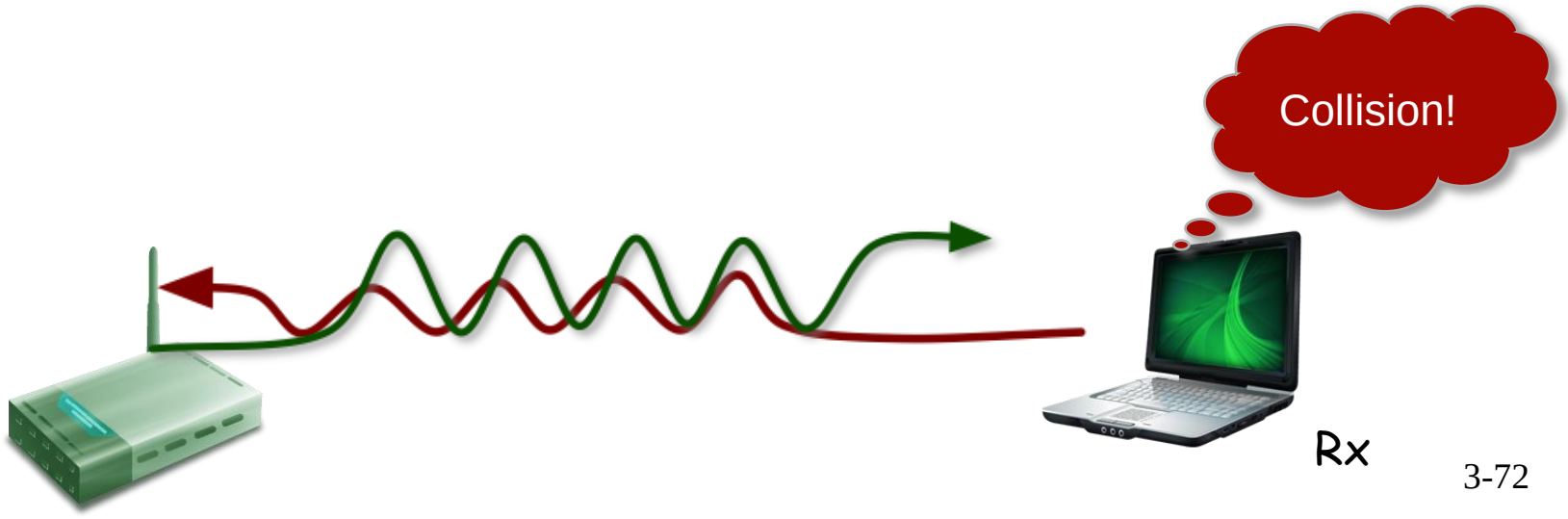
Practical Requirements?

1. Transmitter cannot detect collision
   - Receiver needs to detect it



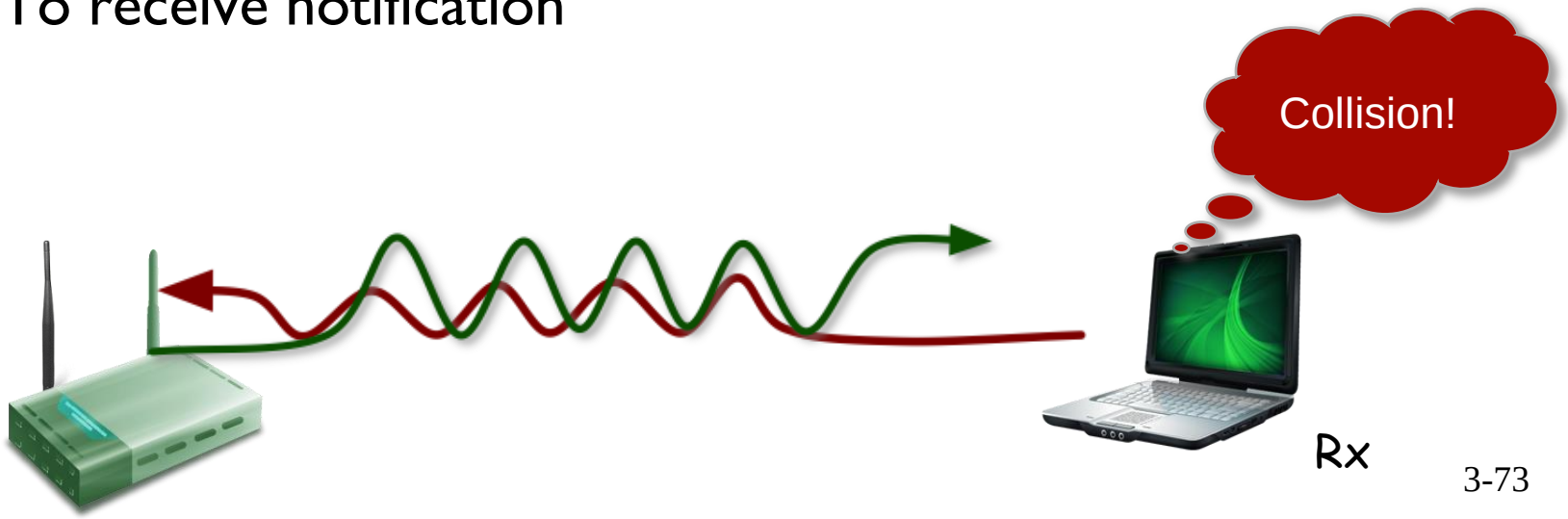
Practical Requirements?

1. Transmitter cannot detect collision
   - ❖ Receiver needs to detect it
2. Receiver needs to convey
   - ❖ collision notification to the transmitter



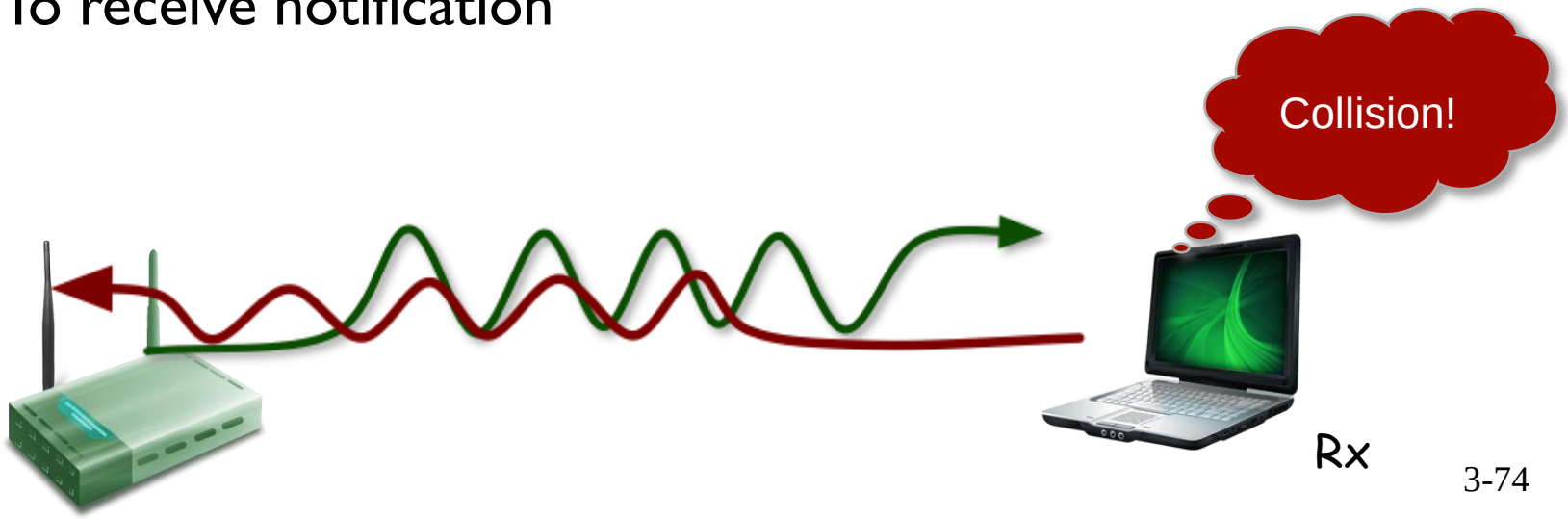
Practical Requirements?

1. Transmitter cannot detect collision
   - Receiver needs to detect it
2. Receiver needs to convey
   - collision notification to the transmitter
3. Transmitter needs an additional antenna
   - To receive notification

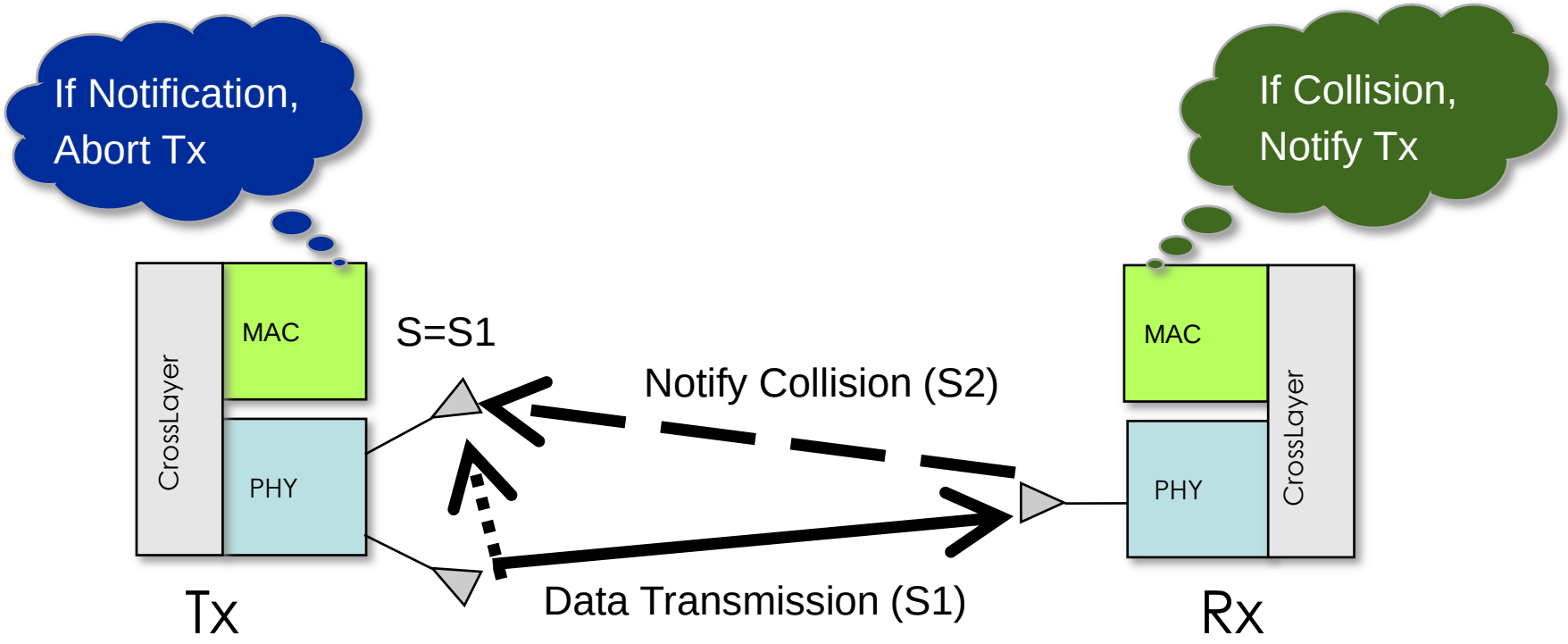


Practical Requirements?

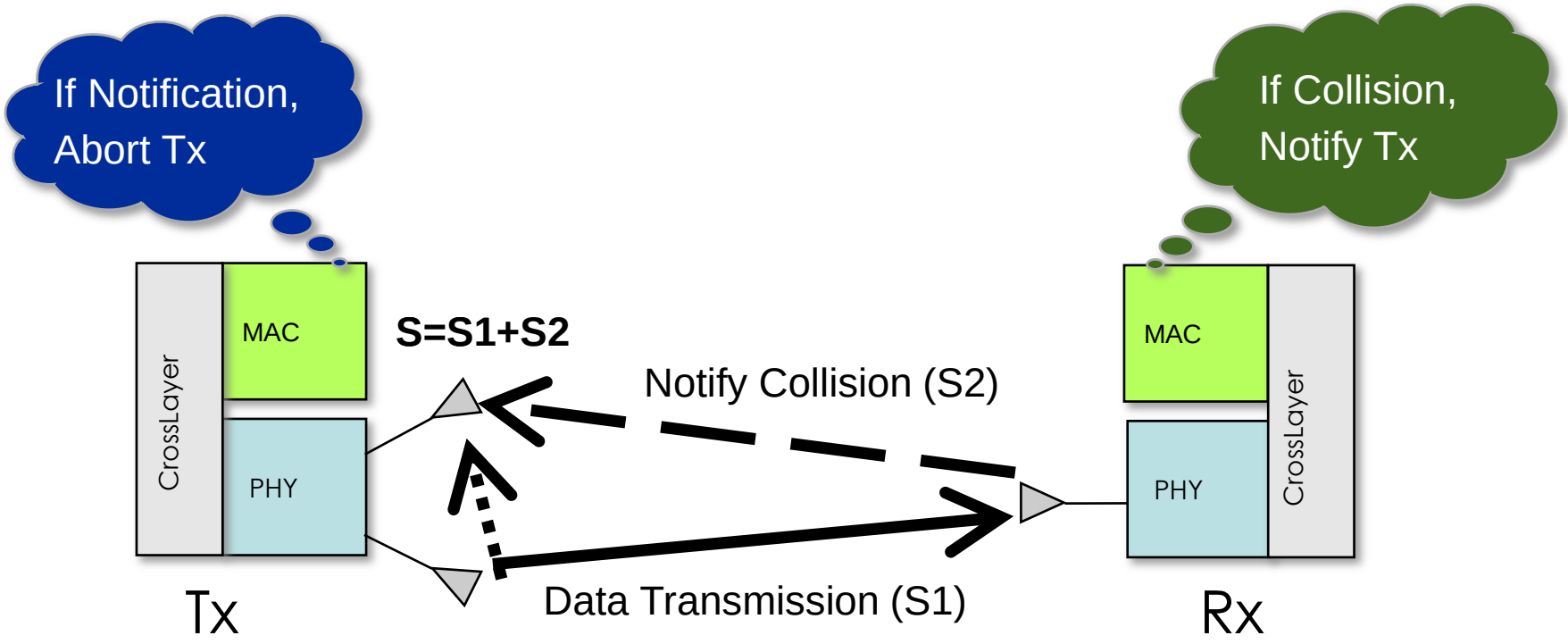
1. Transmitter cannot detect collision
   - ❖ Receiver needs to detect it
2. Receiver needs to convey
   - ❖ collision notification to the transmitter
3. Transmitter needs an additional antenna
   - ❖ To receive notification



Overview


If Notification, Abort Tx
If Collision, Notify Tx
MAC
CrossLayer
PHY
S=S1
Notify Collision (S2)
Data Transmission (S1)
MAC
PHY
CrossLayer
Tx
Rx

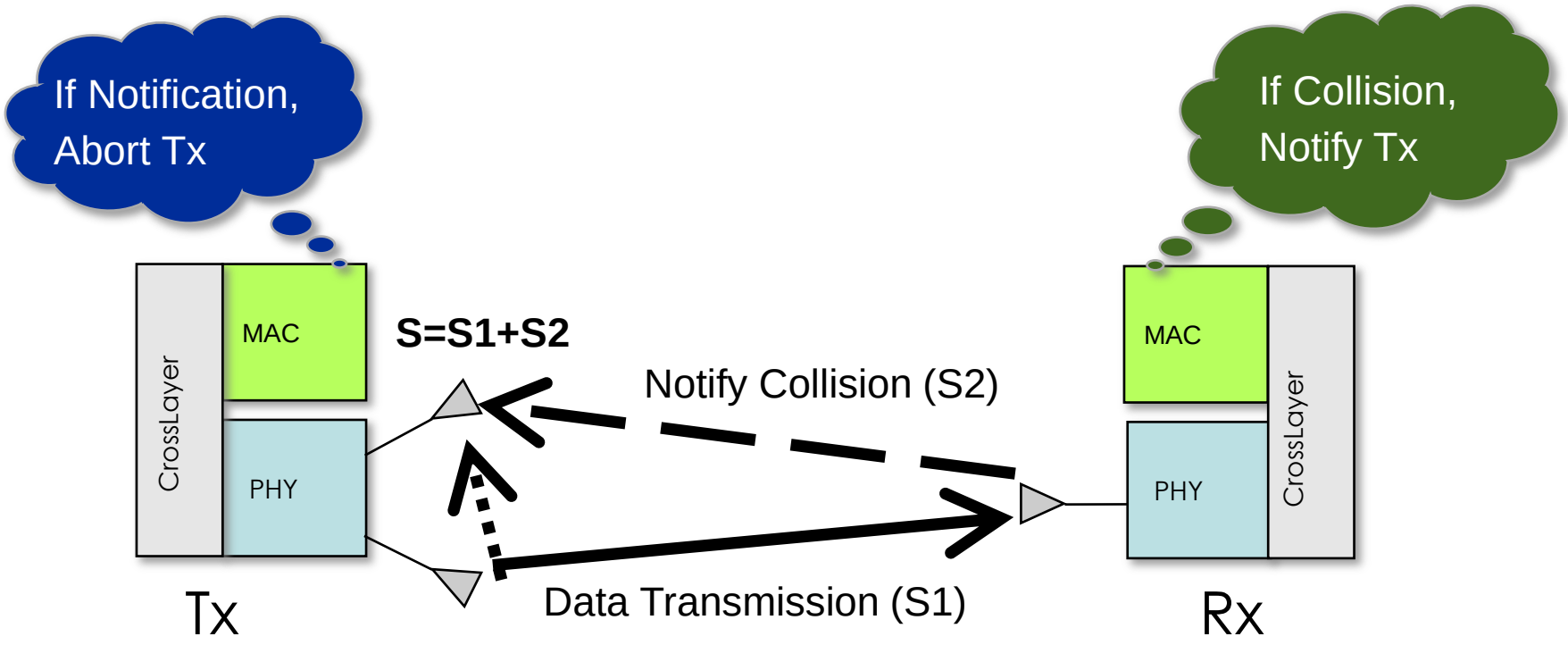
Overview


If Notification, Abort Tx
If Collision, Notify Tx
MAC
PHY
CrossLayer
S=S1+S2
Notify Collision (S2)
Data Transmission (S1)
MAC
PHY
CrossLayer
Tx
Rx

Two Key Challenges

1. Find Notification on Listening Antenna

2. Detect Collision in real time



1. Find Notification on Listening Antenna

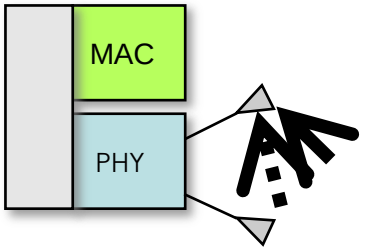
2. Detect Collision in real time

We propose CSMA/CN

Our key idea: Correlation

Challenge 1: Detecting Notification

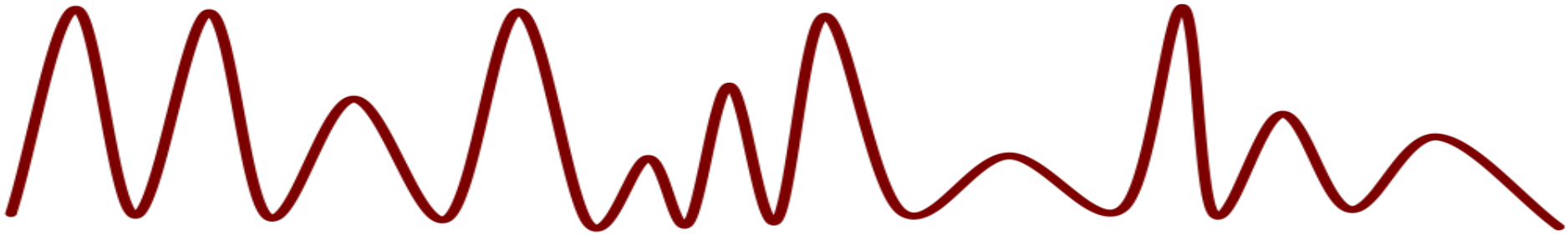
- Hard to decode notification on same channel
  - Self-signal too strong



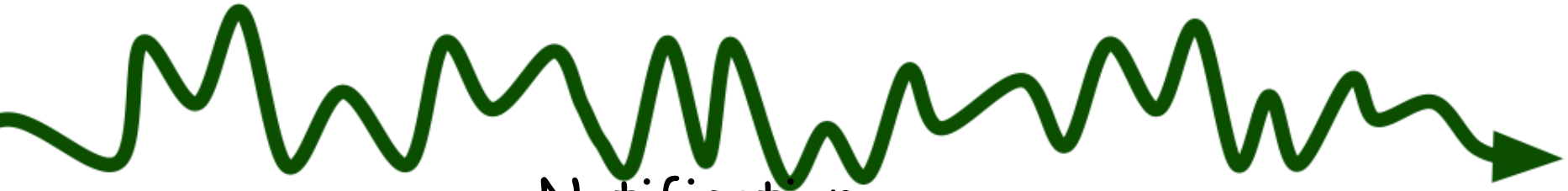
- Let Tx and Rx share a unique signature
- Tx correlates with shared signature
  - Detects collision notification, aborts

Observe: No decoding, just correlate

Challenge 1: Detecting Notification

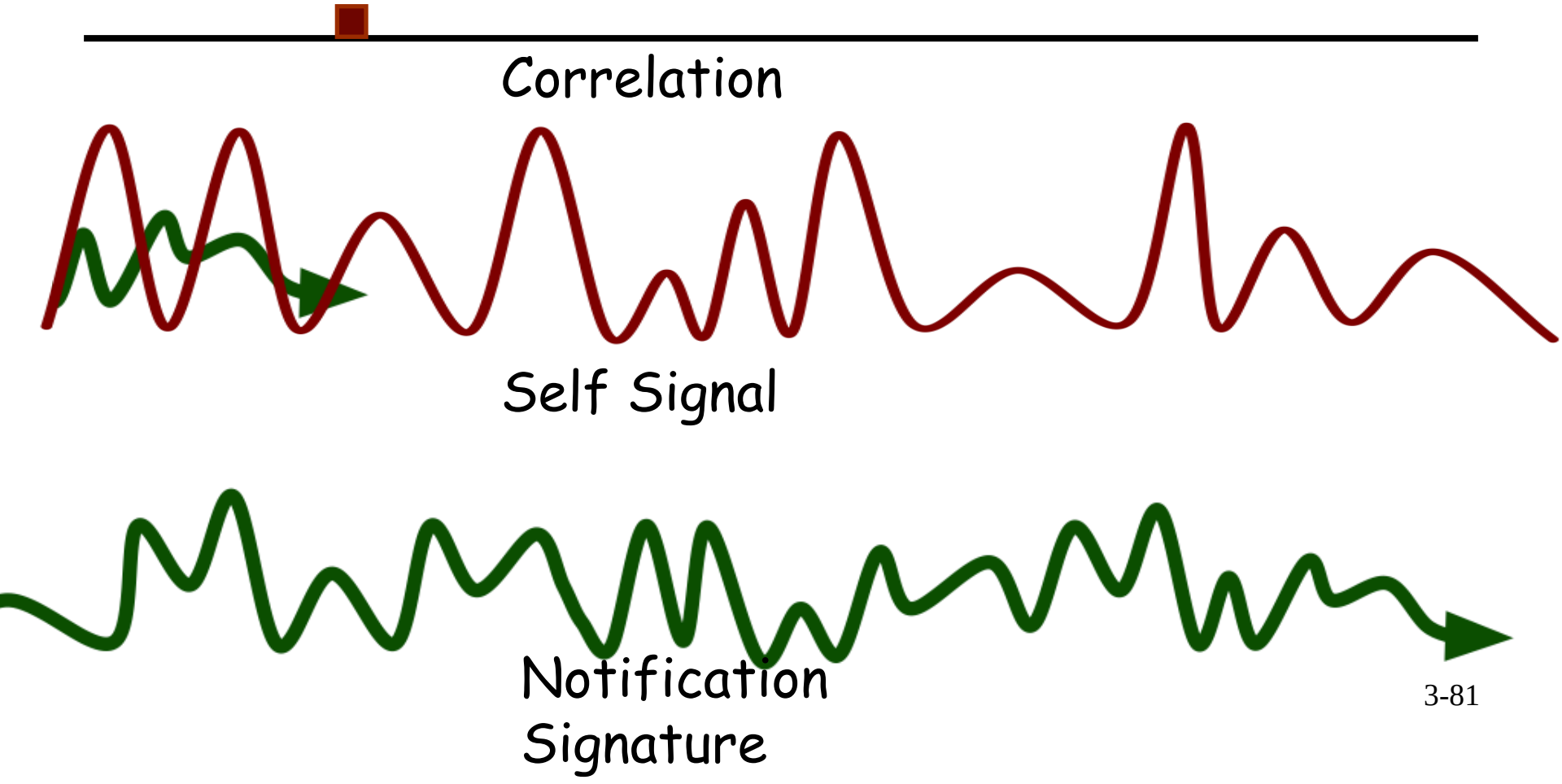


Self Signal



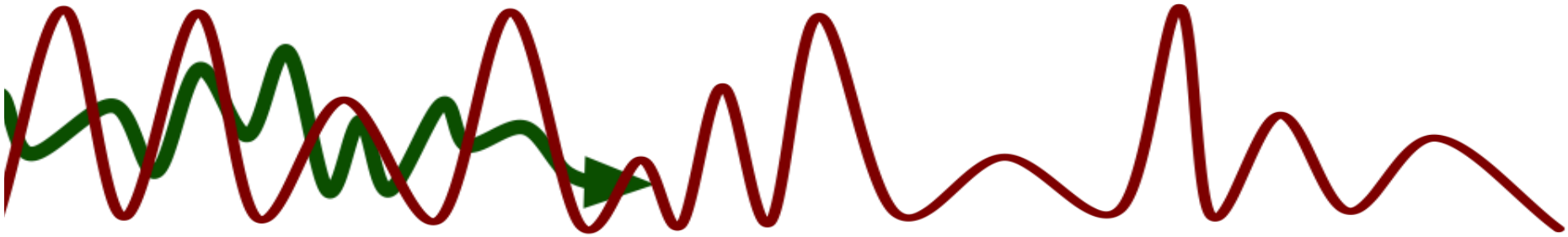
Notification
Signature

Challenge 1: Detecting Notification

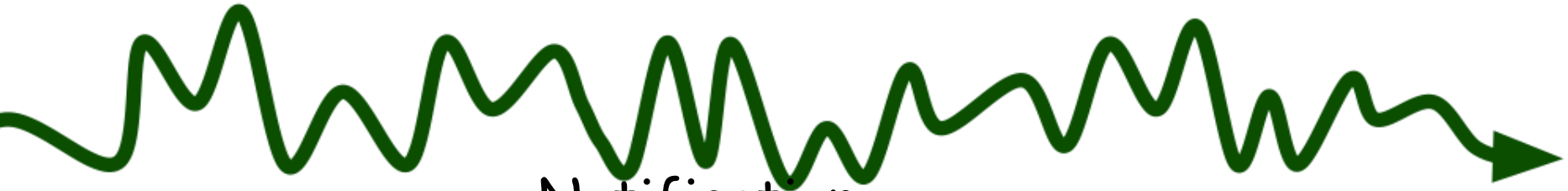


Challenge 1: Detecting Notification

Correlation



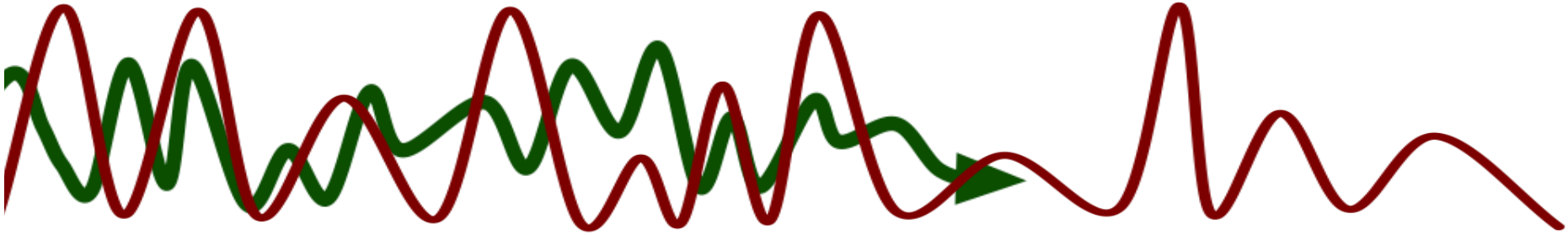
Self Signal



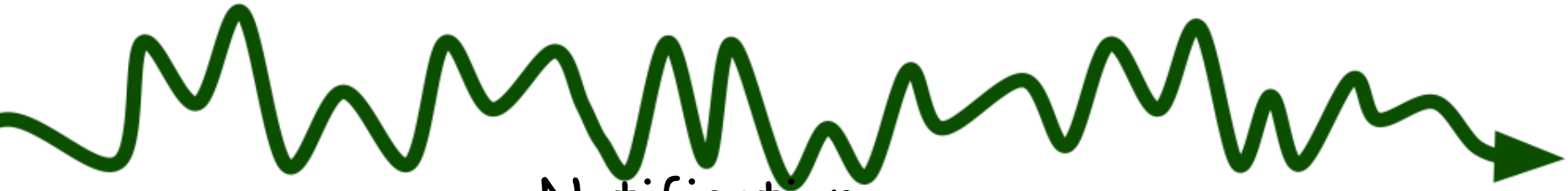
Notification Signature

Challenge 1: Detecting Notification

Correlation



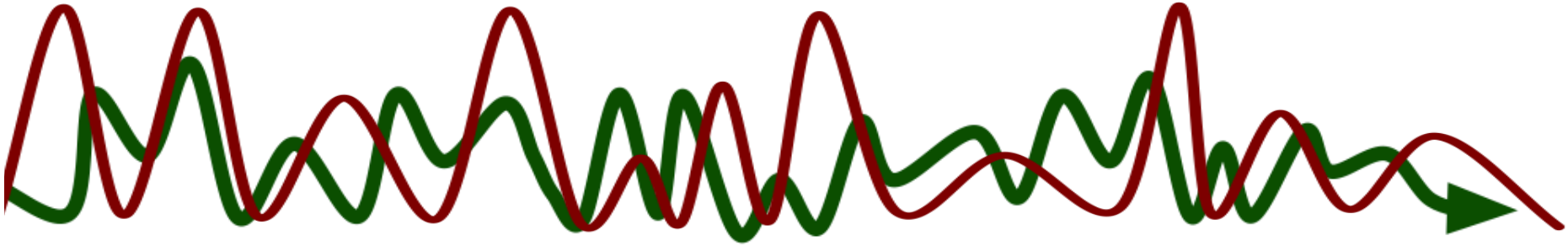
Self Signal



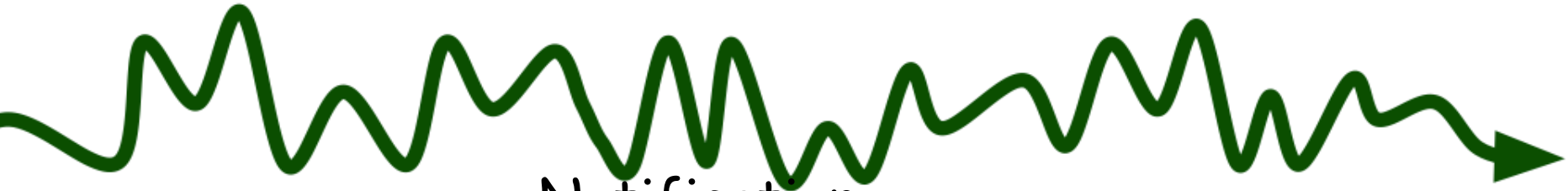
Notification Signature

Challenge 1: Detecting Notification

Correlation

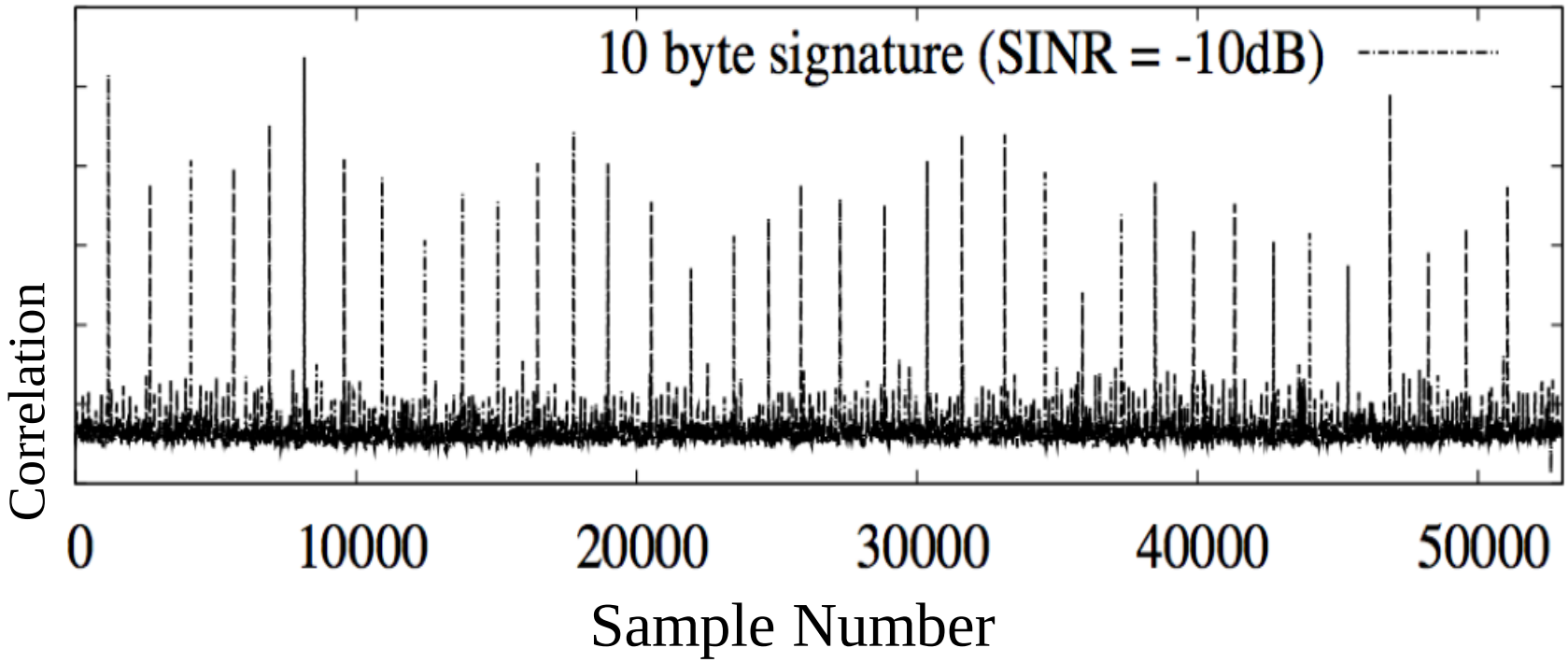


Self Signal



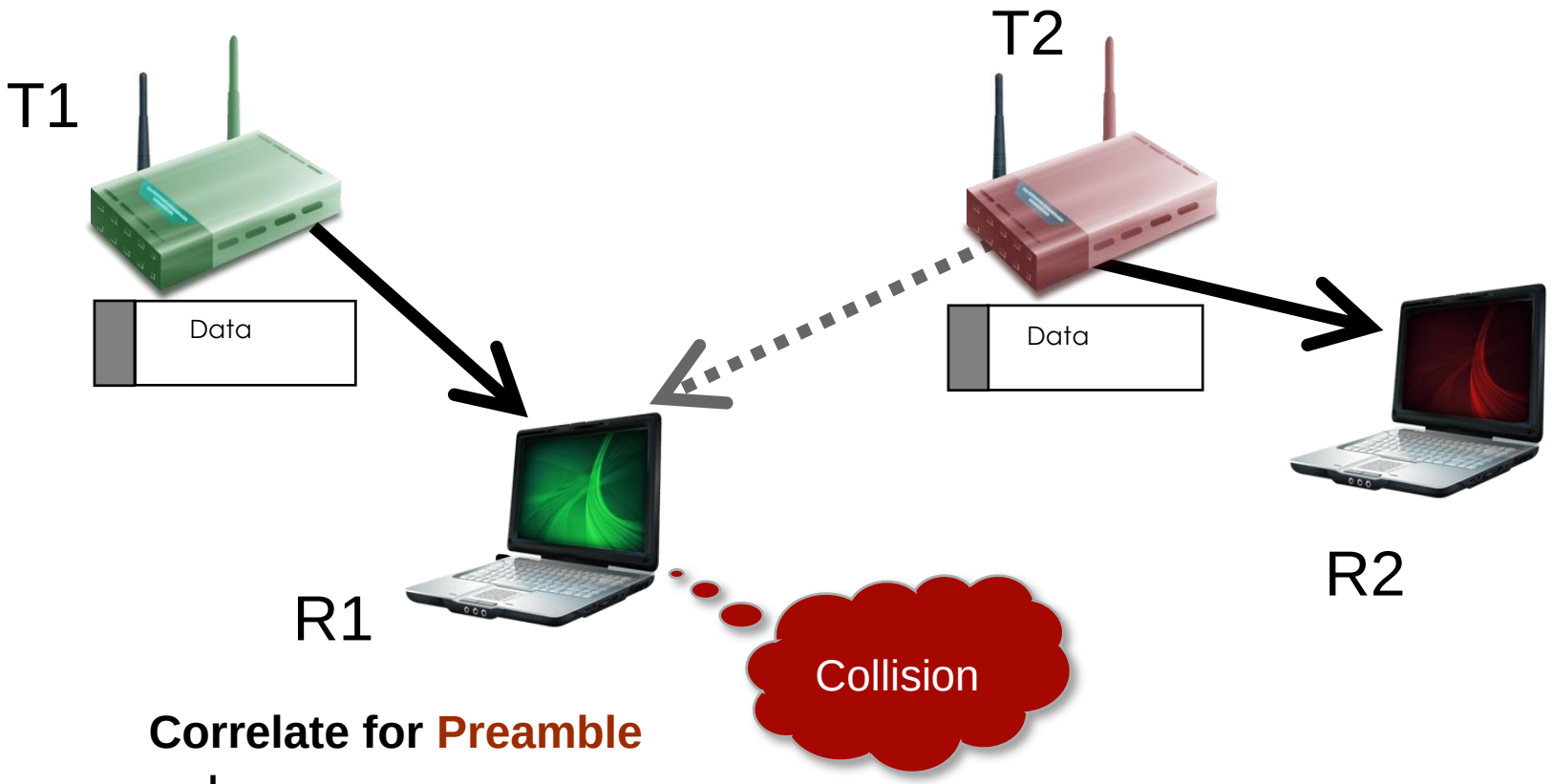
Notification Signature

Challenge 1: Detecting Notification



Whenever there is a notification, there is a jump in correlation

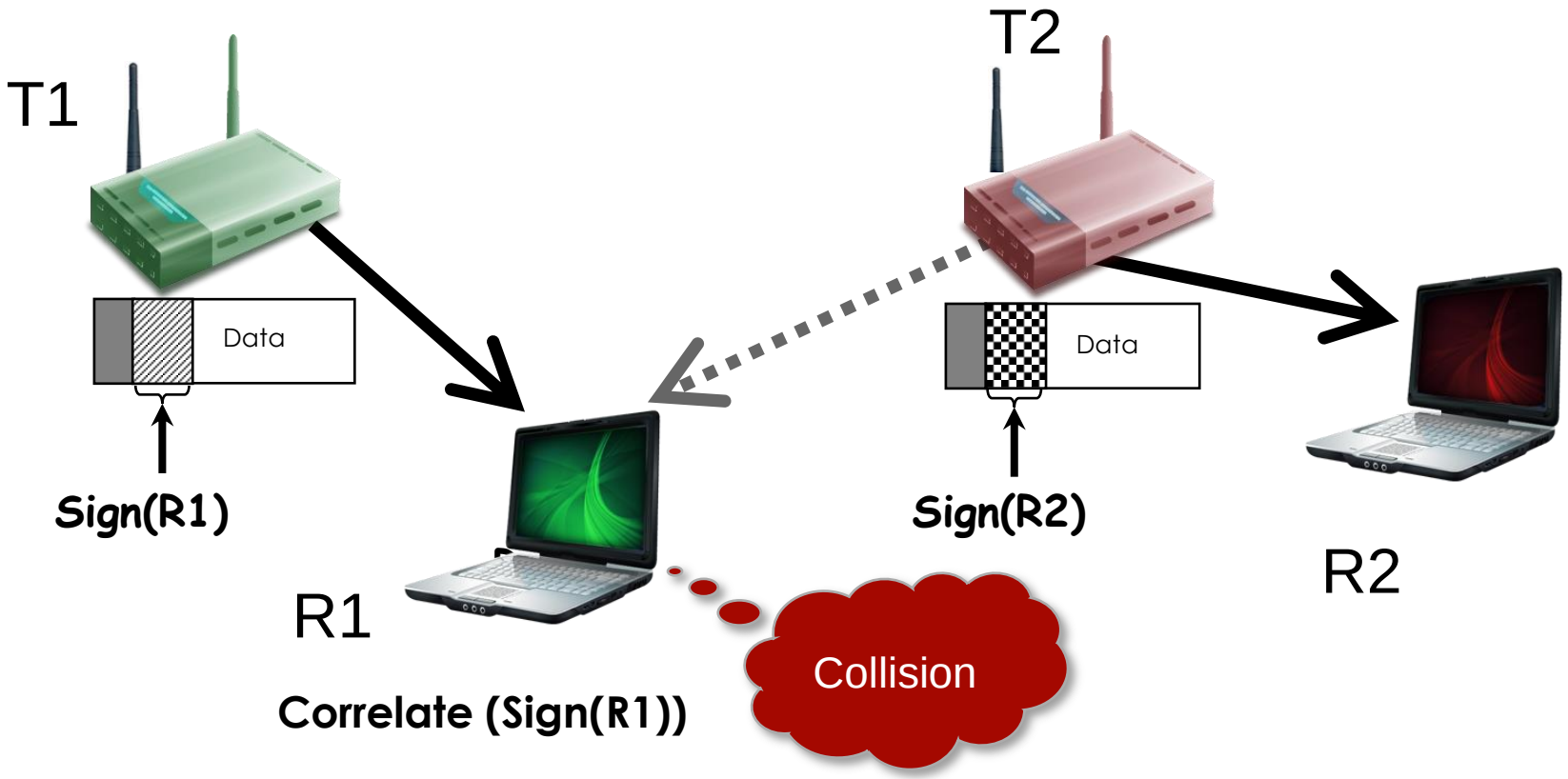
Challenge 2: Interference Detection



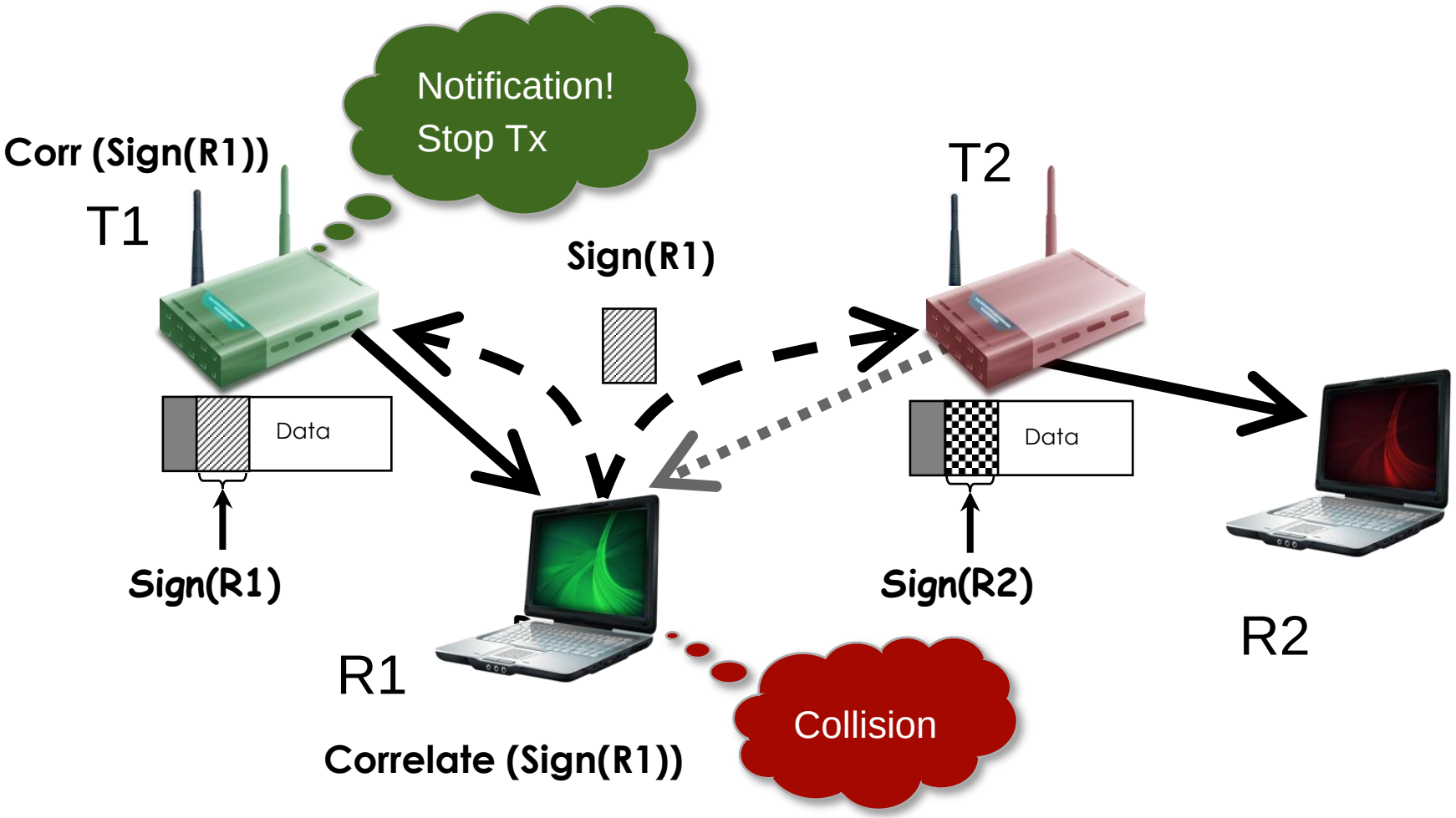
Correlate for Preamble
+
SoftPHY

What if transmitter starts second?

SOI starts after interference



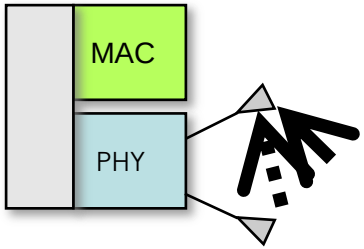
Signal Correlation and Abort



Performance Evaluation

- 7 node USRP testbed
- Zigbee CC2420 PHY
- Max data rate: 250Kbps
- Signature size: 5 bytes
- Compare with 802.11-like and PPR
  - PPR detects interfered portion of received packet
    - Transmitter sends only the interfered portion

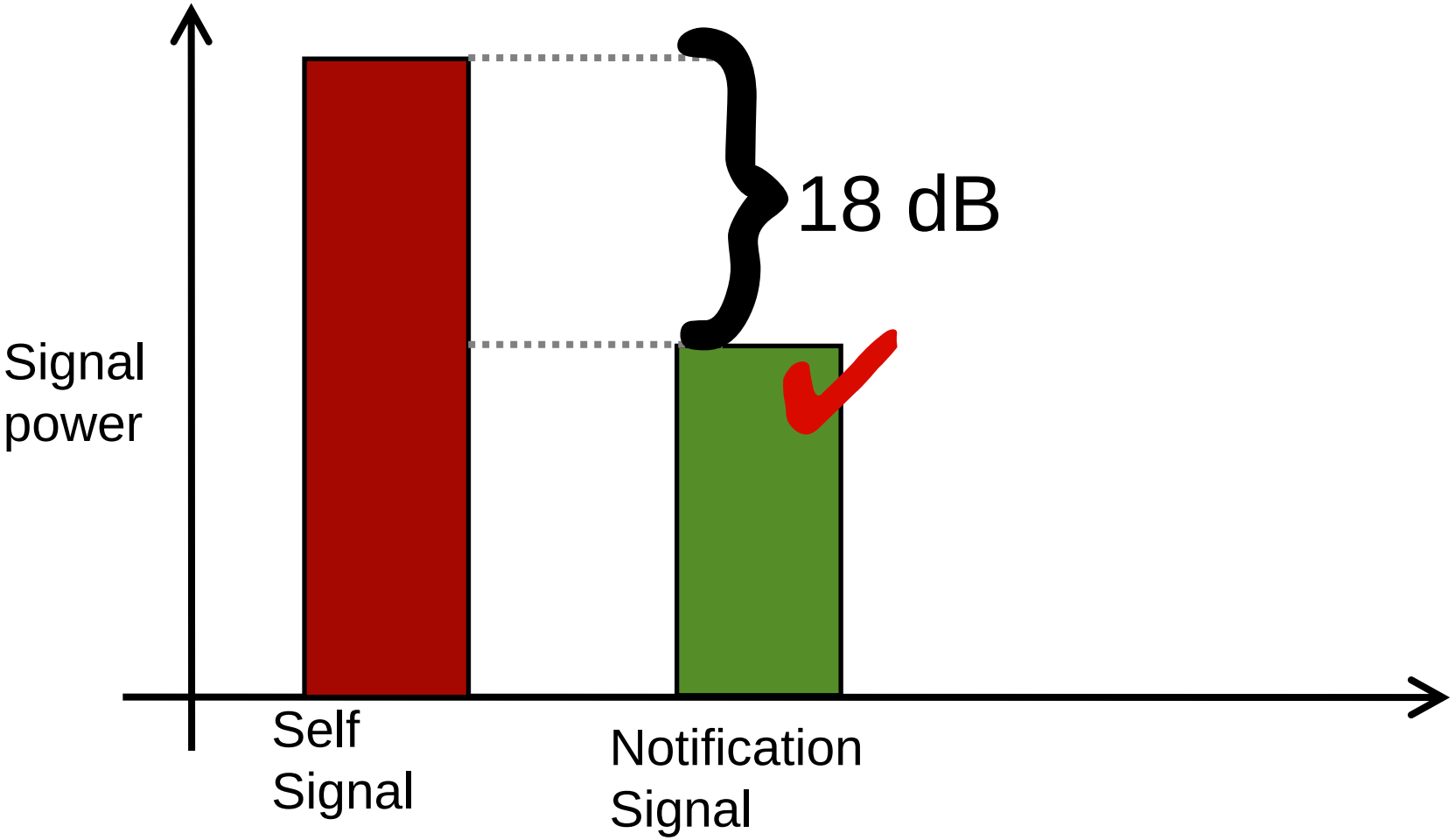
Notification Detection at Tx



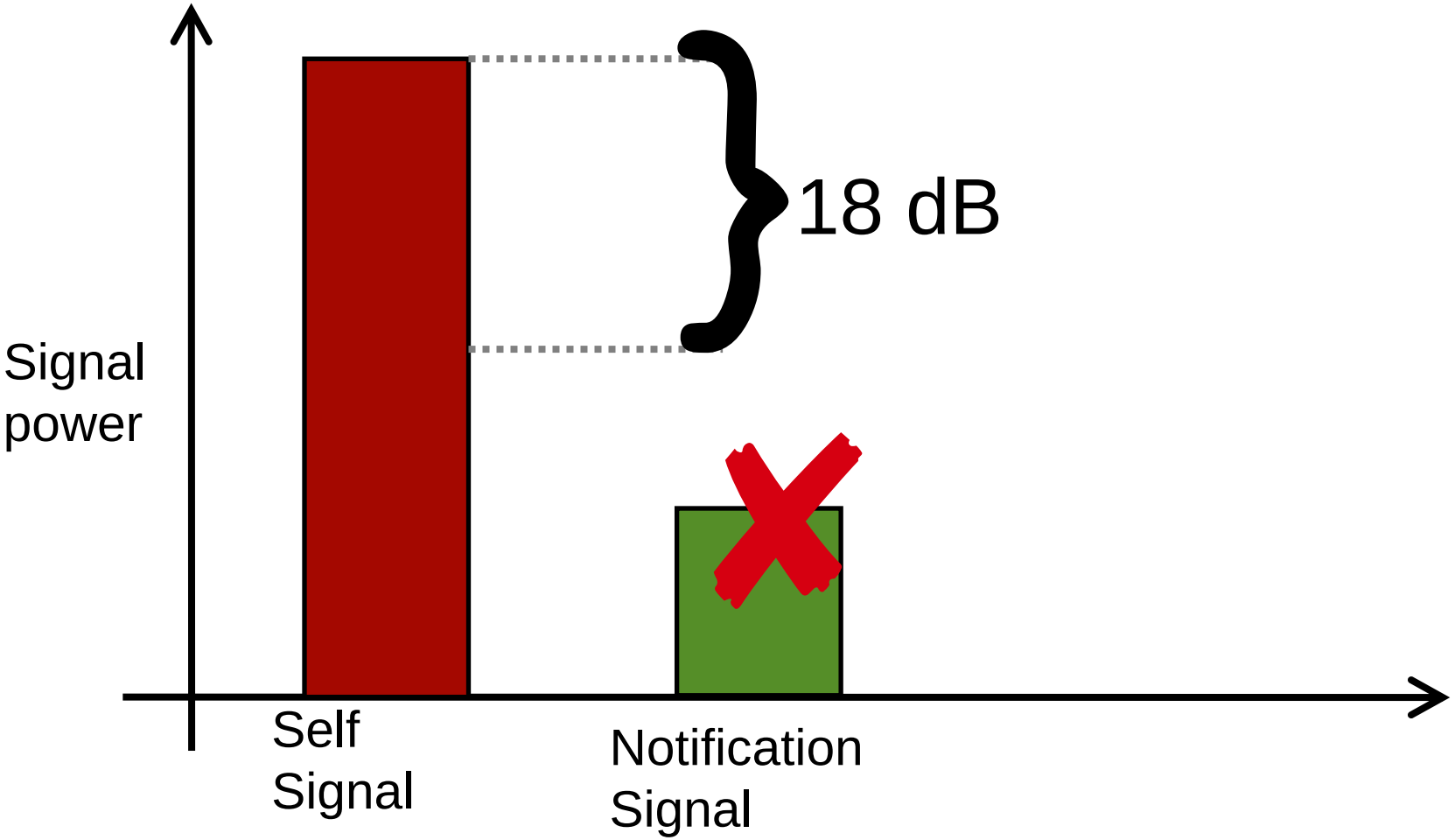
Notification Signal << Self Signal

How weak can the notification signal be?

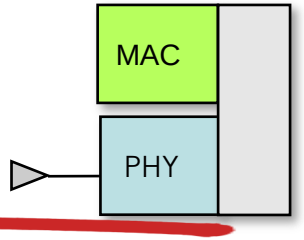
How weak the notification signal be?



How weak the notification signal be?

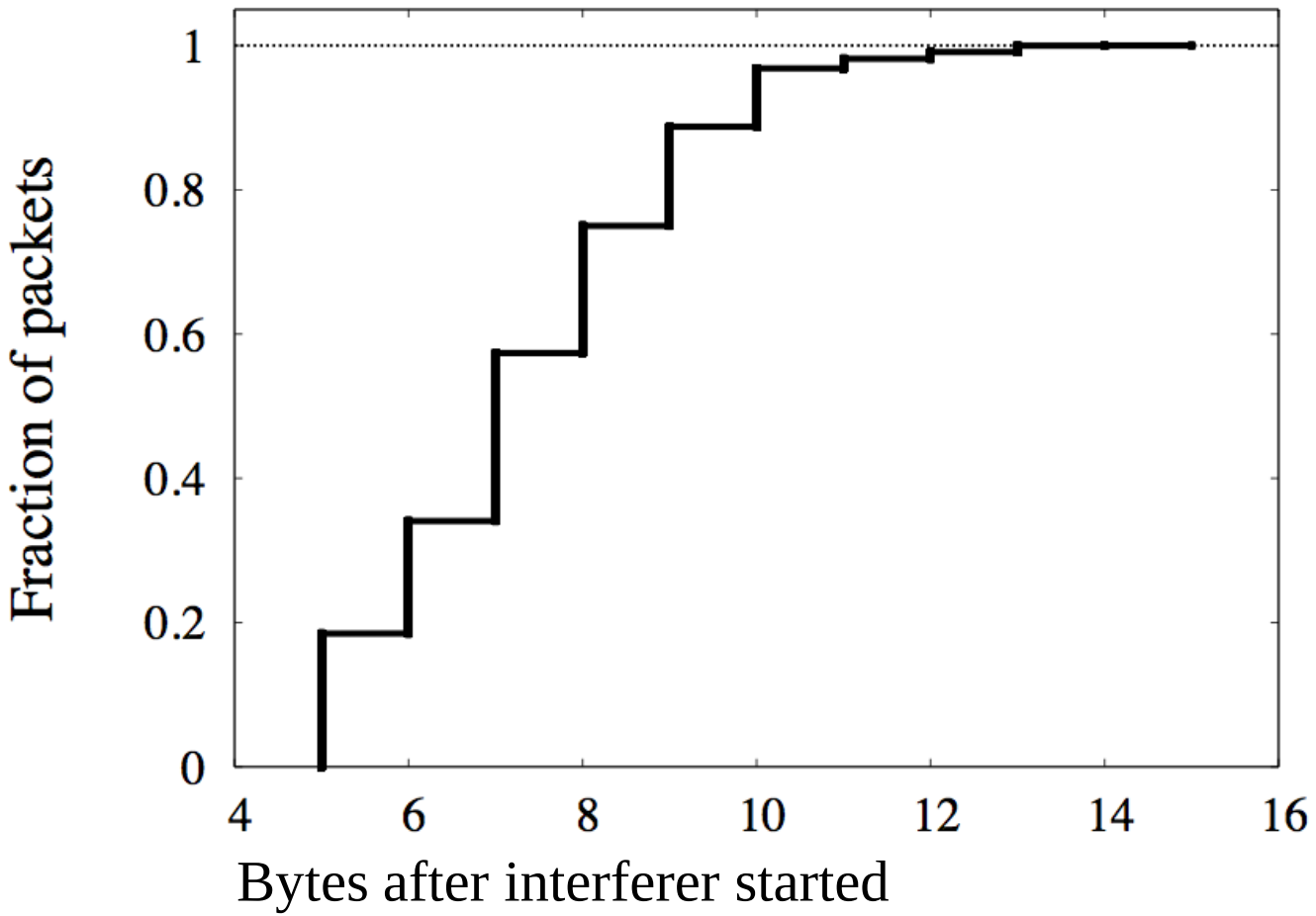


Interference Detection at Rx



- Interference detection accuracy of 93%
- Receiver should detect interference quickly
- Quicker detection → Faster Tx abortion

Interference Detection: Speed

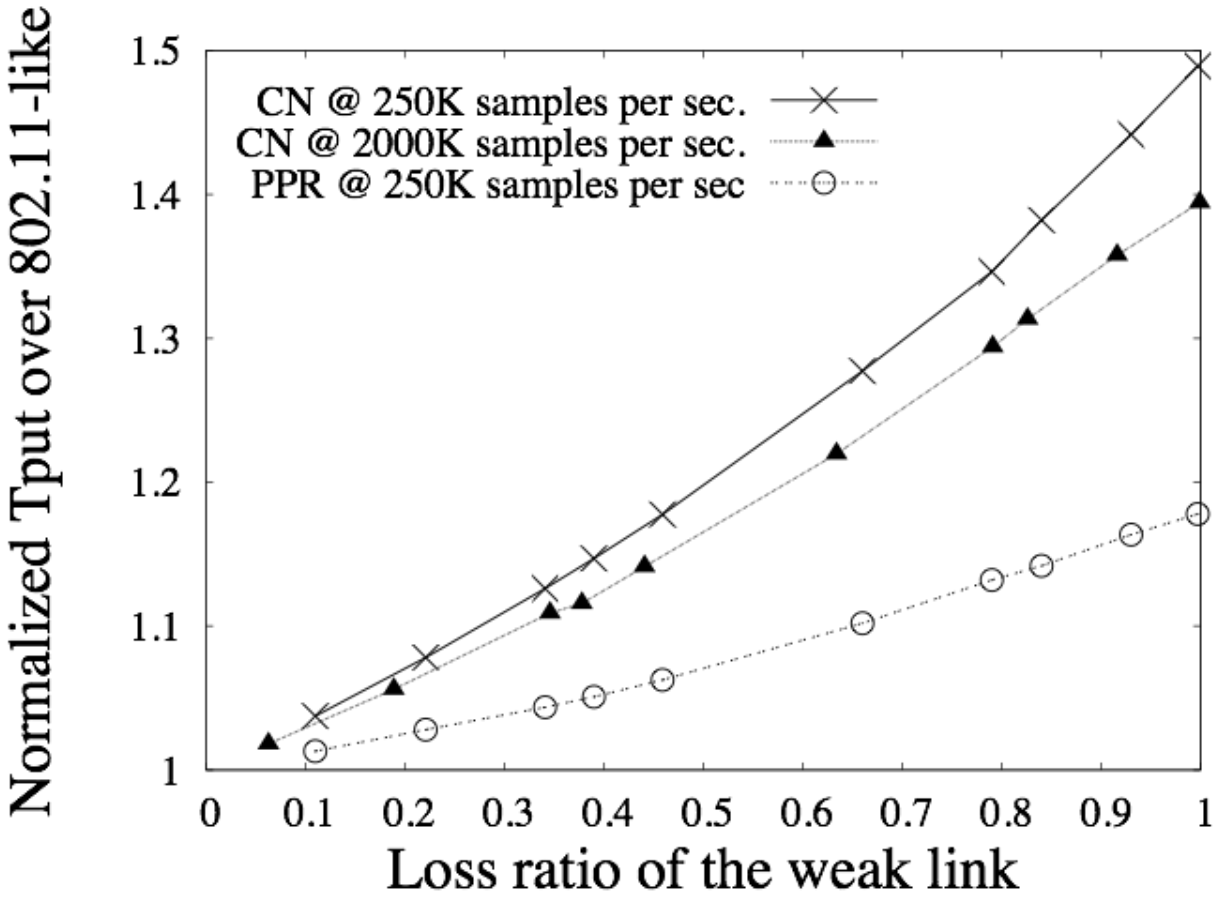


CSMA/CN predicts collision within 7 bytes

Testbed Experimentation

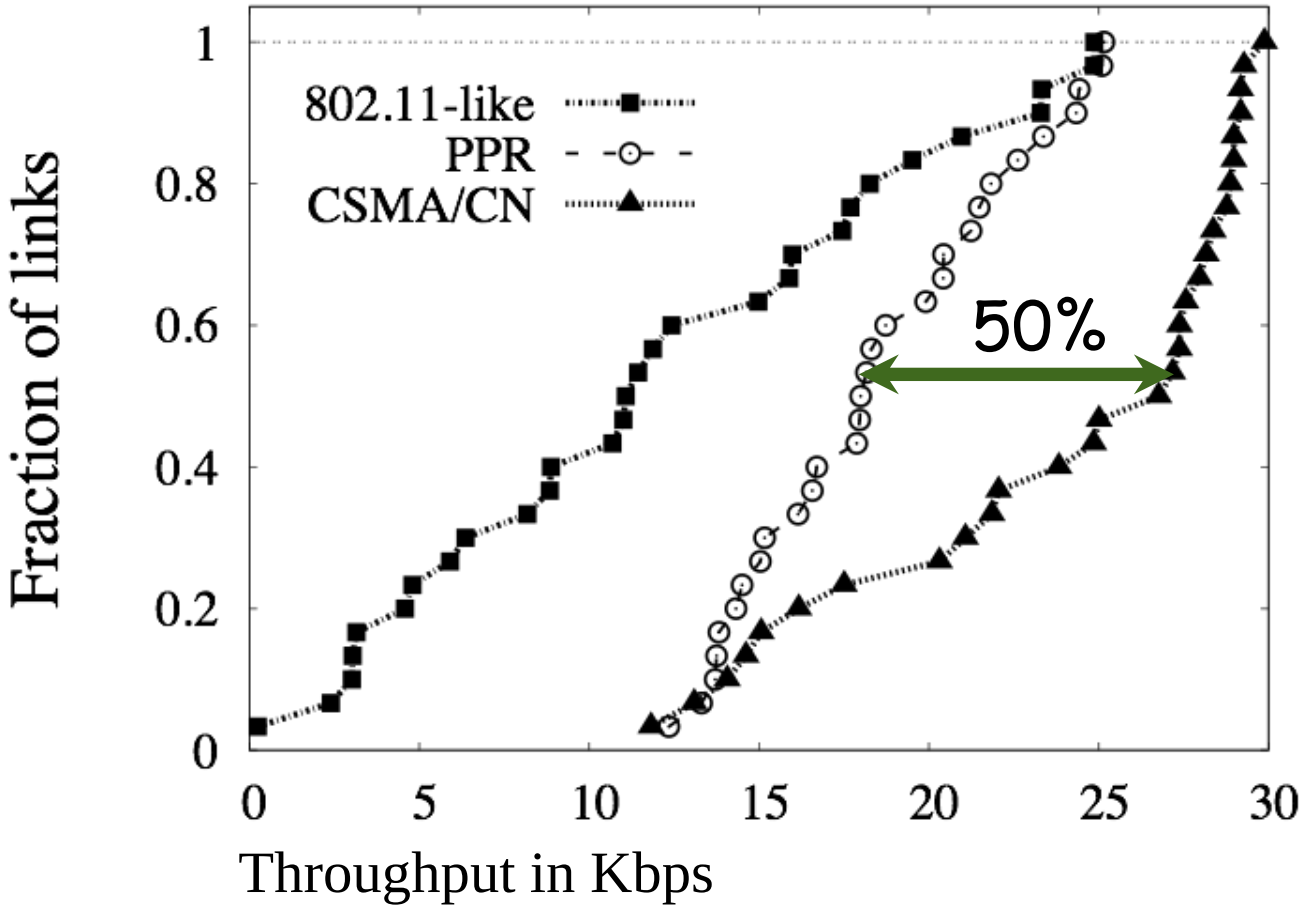
- One link doing CSMA/CN
- CSMA/CN link has an exposed and hidden terminal
- Whenever CSMA/CN link fails due to interference
  - CSMA/CN link stops
  - Exposed terminal transmits reducing channel wastage

Testbed Throughput



PPR continues to transmit under collision, worse than CSMA/CN

Traced Based Evaluation



Up to 50% gain in per link throughput

Summary

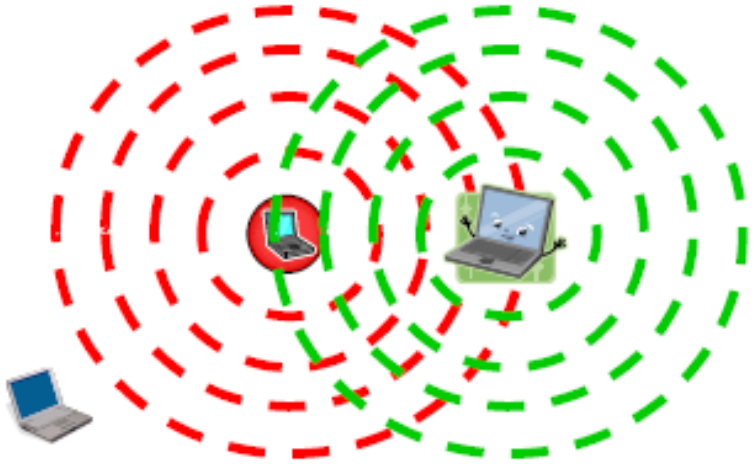
- CSMA/CN imitates CSMA/CD in wireless
- Rx uses correlation to detect interference
- Tx uses correlation to detect notification
- Others can utilize freed-up channel

Outline

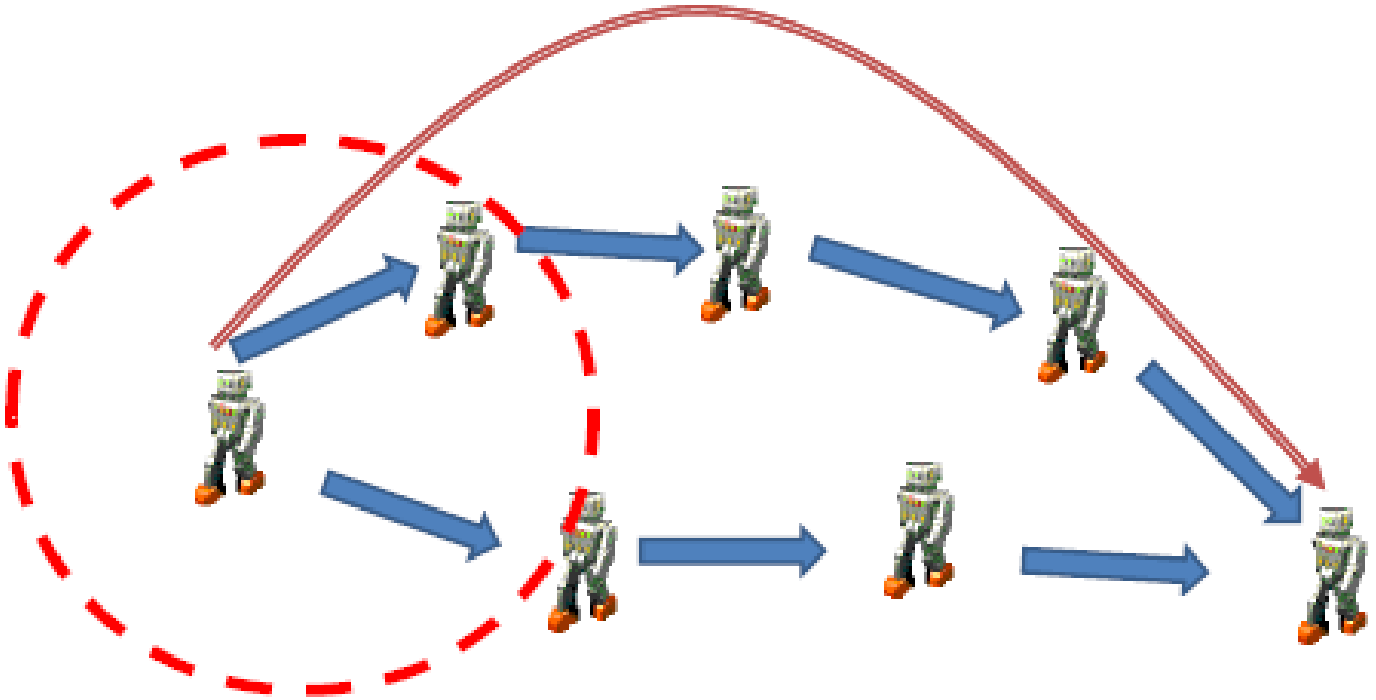
- Overview
- MAC
- **Routing**
- Wireless in real world
- Leverage broadcasting nature
- Explore the characteristic of wireless signal

Assumptions of Wireless Routing

- Inherent mobility
  - Nodes are not static
- Transmission properties
  - Classically assumed as unit-disc model
- All or nothing range R
  - Symmetric reception

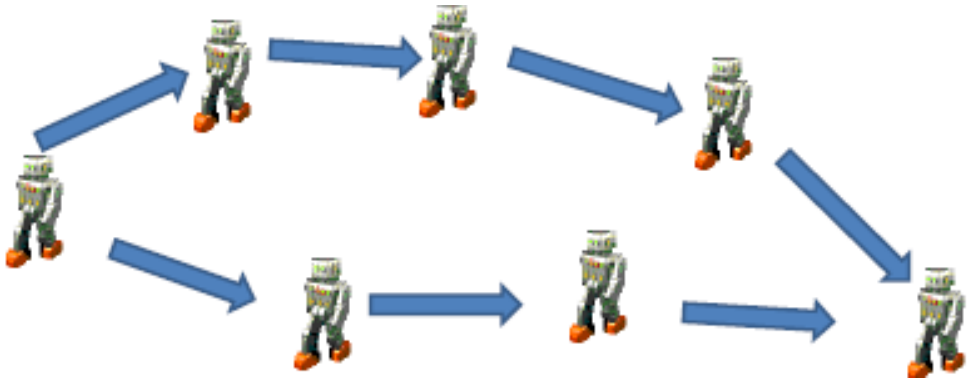


Scenarios



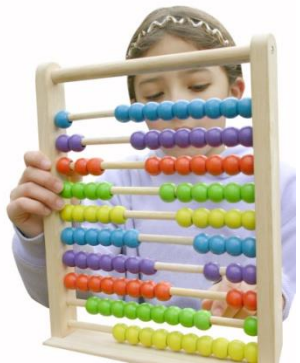
GOAL

- Minimize control overhead
- Minimize processing overhead
- Multi-hop path routing capability
- Dynamic topology maintenance
- No routing loops
- Self-starting



Brief Review of Internet Routing

- Intra-AS routing
  - Link-state
  - Distance vector
- Distance vector
  - Neighbors periodically exchange routing information with neighbors
    - <destination IP addr, hop count>
  - Nodes iteratively learn network routing info compute routes to all destinations
  - Suffer from problems like *counting-to-infinity*



Review Cont.

- Link State
  - Nodes flood neighbor routing information to all nodes in network
    - <neighbor IP Addr, cost>
  - Once each node knows all links in network, can individually compute routing paths
    - Use Dijkstra for example
    - Minimize routing "cost"
  - Supports metrics other than hop count, but is more complex

Review Cont.

- Examples of routing protocols
  - Distance vector: RIP
  - Link state: OSPF
- What do these have in common?
  - Both maintain routes to all nodes in network

Approaches to Wireless Routing

- Proactive Routing
  - Based on traditional distance-vector and link-state protocols
  - Nodes *proactively maintains route to each other*
  - Periodic and/or event triggered routing update exchange
  - Higher overhead in most scenarios
  - Longer route convergence time
  - Examples: DSDV, TBRPF, OLSR

Approaches Cont.

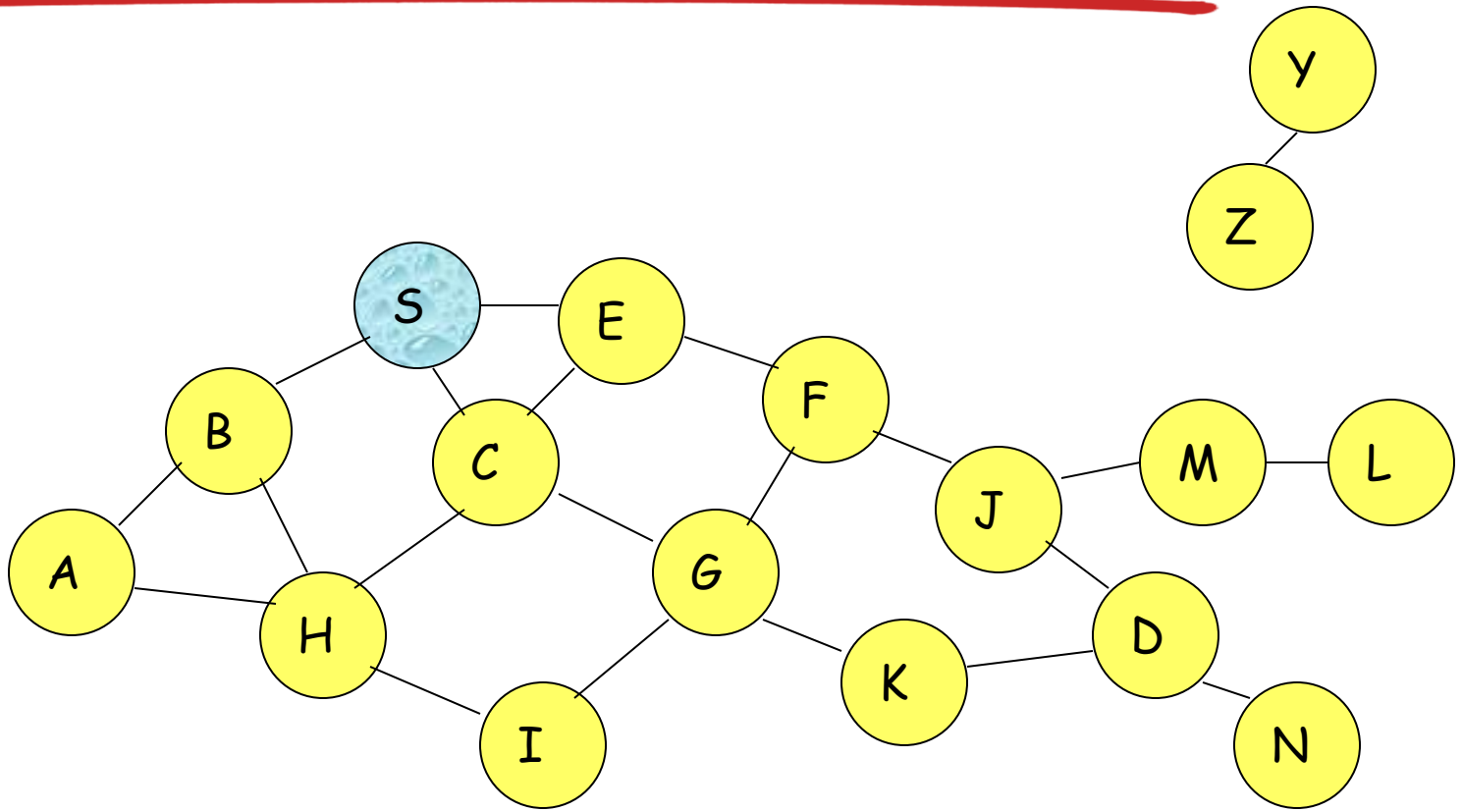
- Reactive (on-demand) Routing
  - Source build routes on-demand by "flooding"
  - Maintain only active routes
  - Route discovery cycle
  - Typically, less control overhead, better scaling properties
  - Drawback??
    - Route acquisition latency
  - Example: AODV, DSR

WIRELESS ROUTING PROTOCOLS (1): REACTIVE PROTOCOLS

Dynamic Source Routing (DSR) [Johnson96]

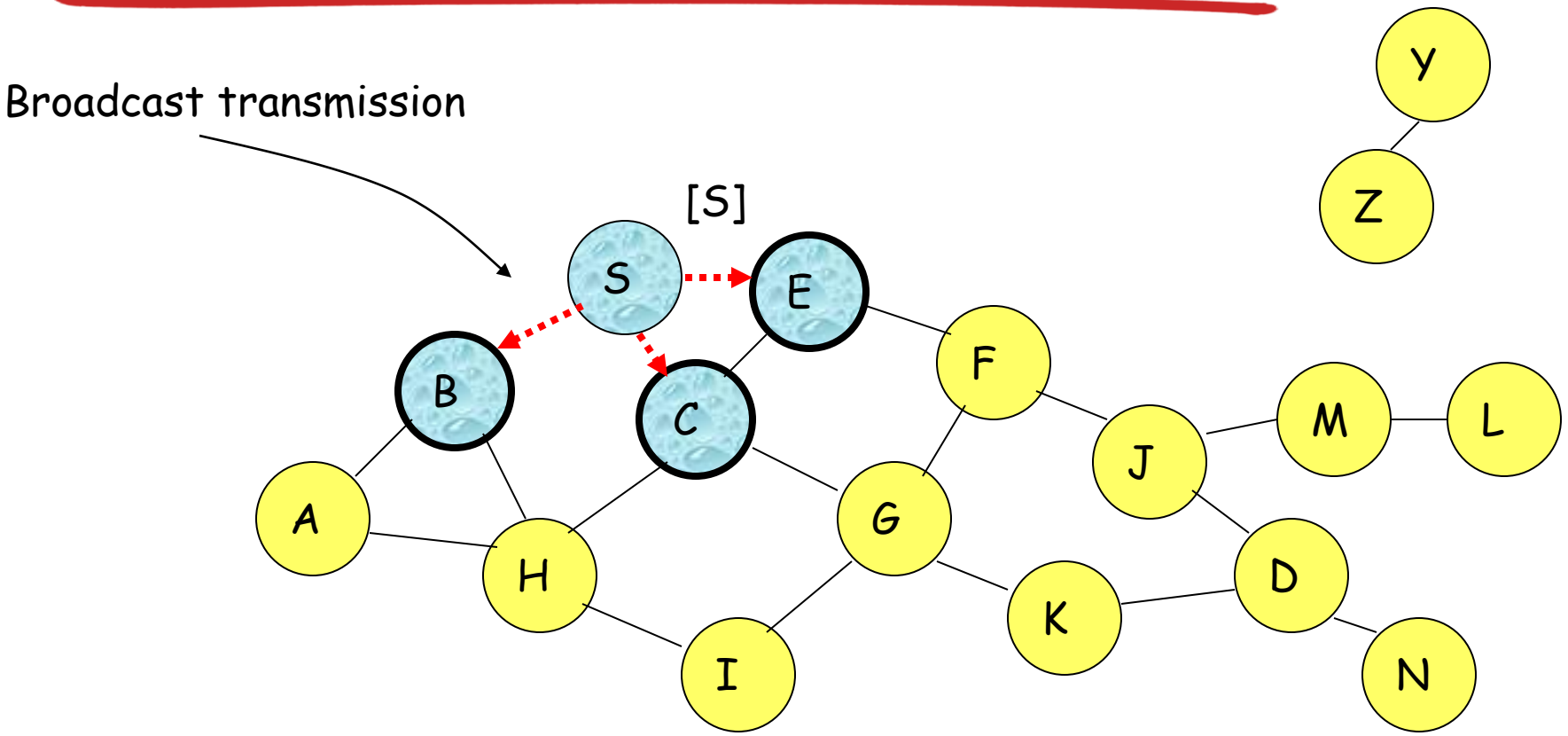
- When node S wants to send a packet to node D, but does not know a route to D, node S initiates a route discovery
- Source node S floods Route Request (RREQ)
- Each node appends own identifier when forwarding RREQ

Route Discovery in DSR



Represents a node that has received RREQ for D from S

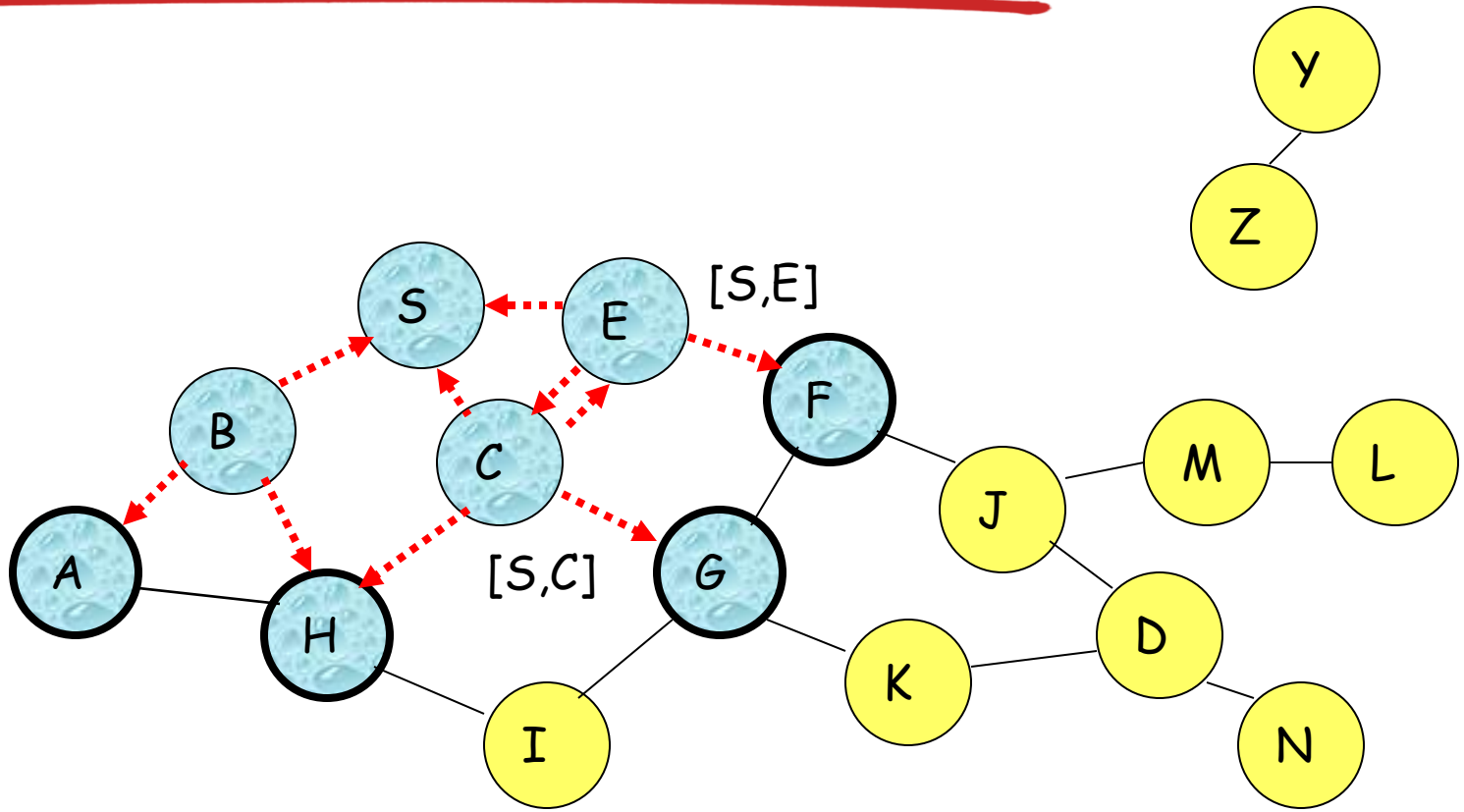
Route Discovery in DSR



Represents transmission of RREQ

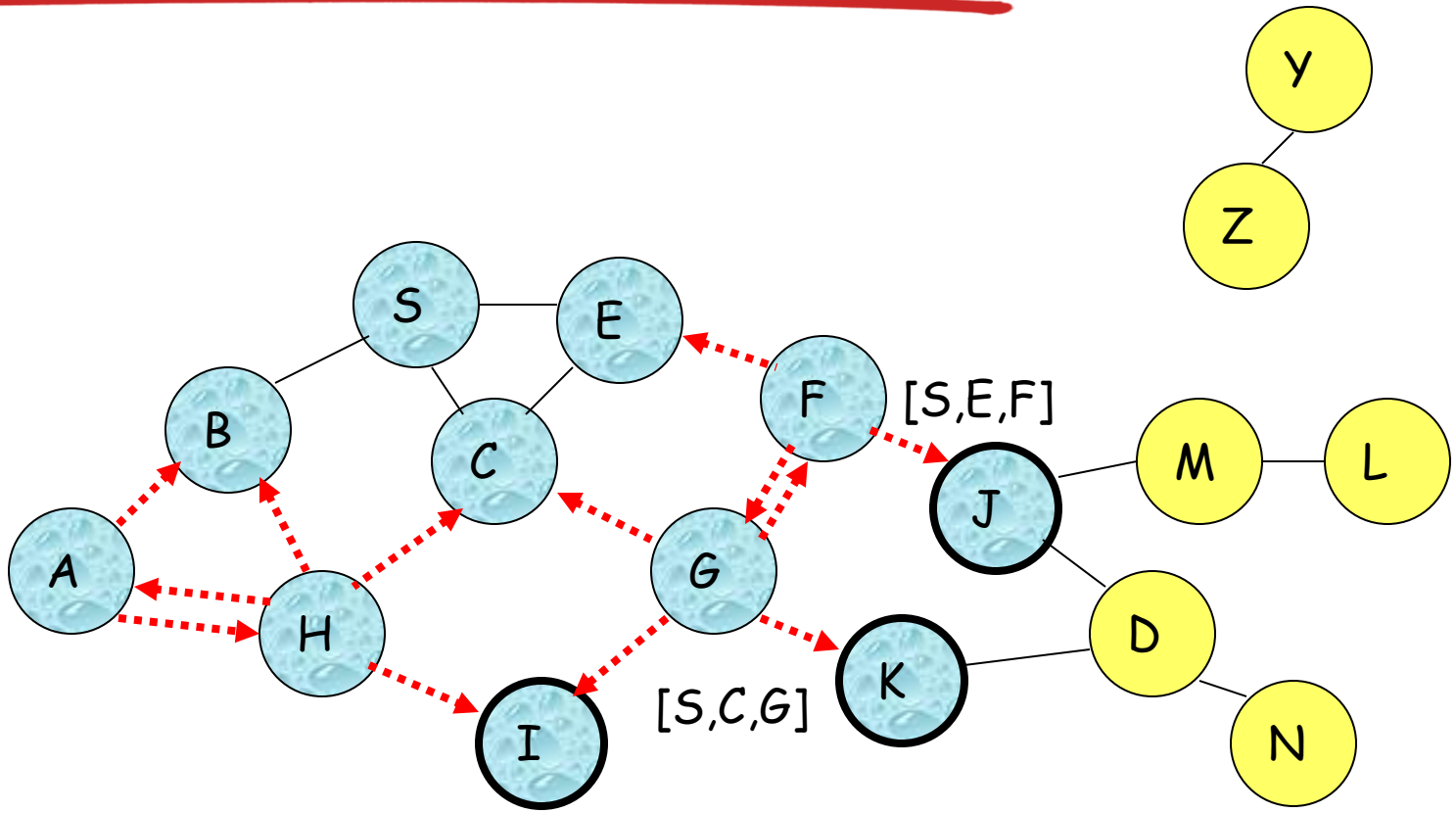
[X,Y] Represents list of identifiers appended to RREQ

Route Discovery in DSR



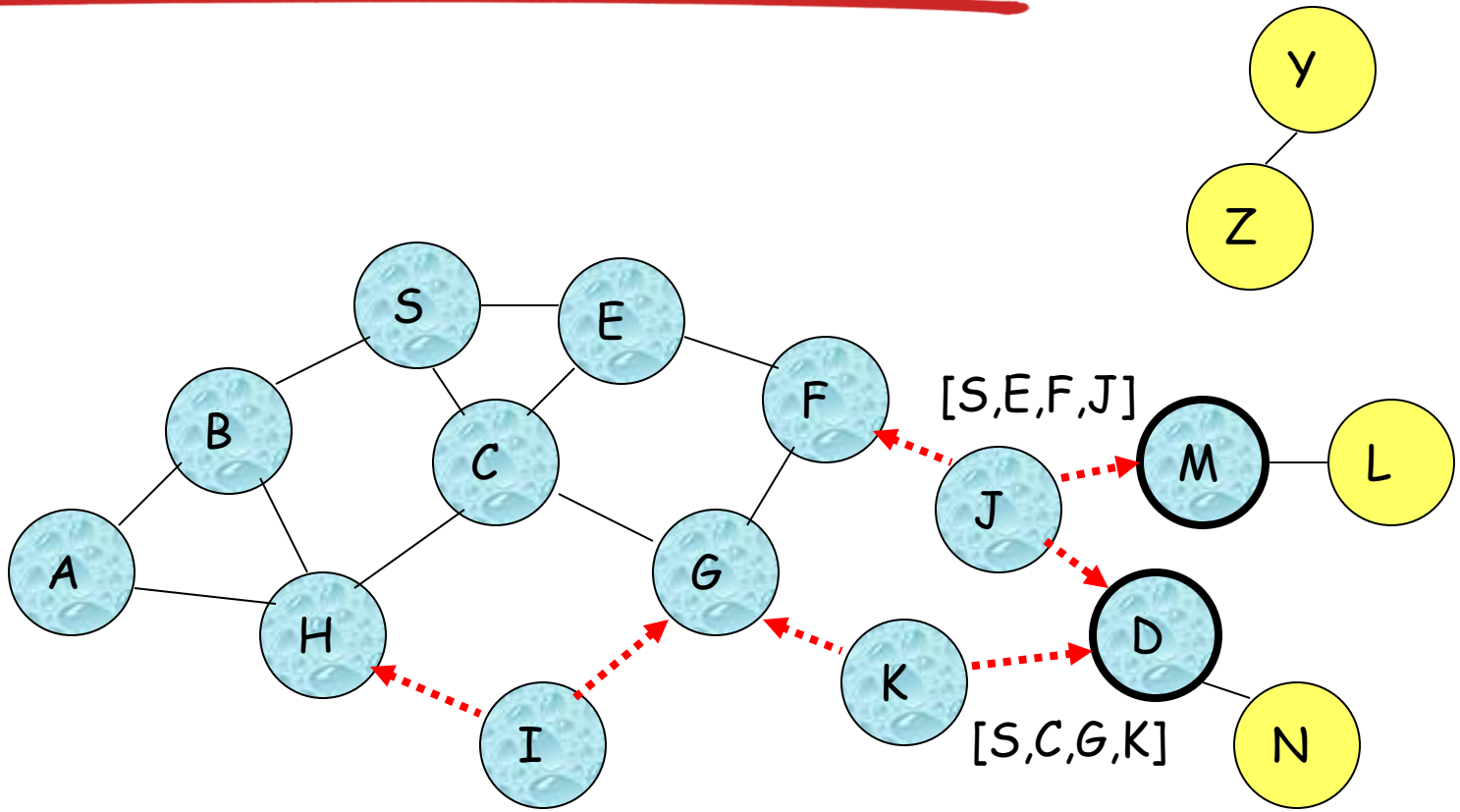
- Node H receives packet RREQ from two neighbors:
  potential for collision

Route Discovery in DSR



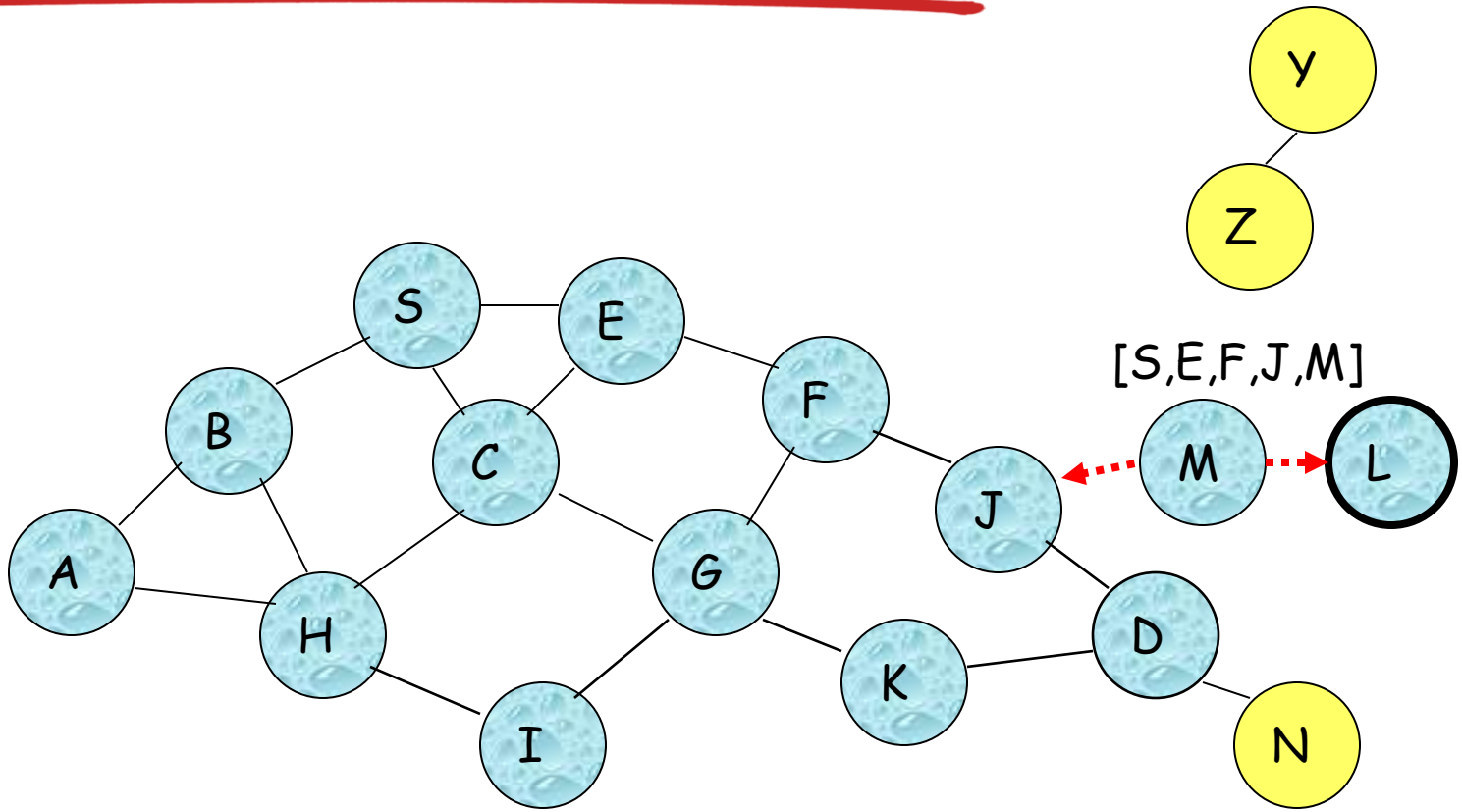
- Node C receives RREQ from G and H, but does not forward it again, because node C has already forwarded RREQ once

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

Route Discovery in DSR

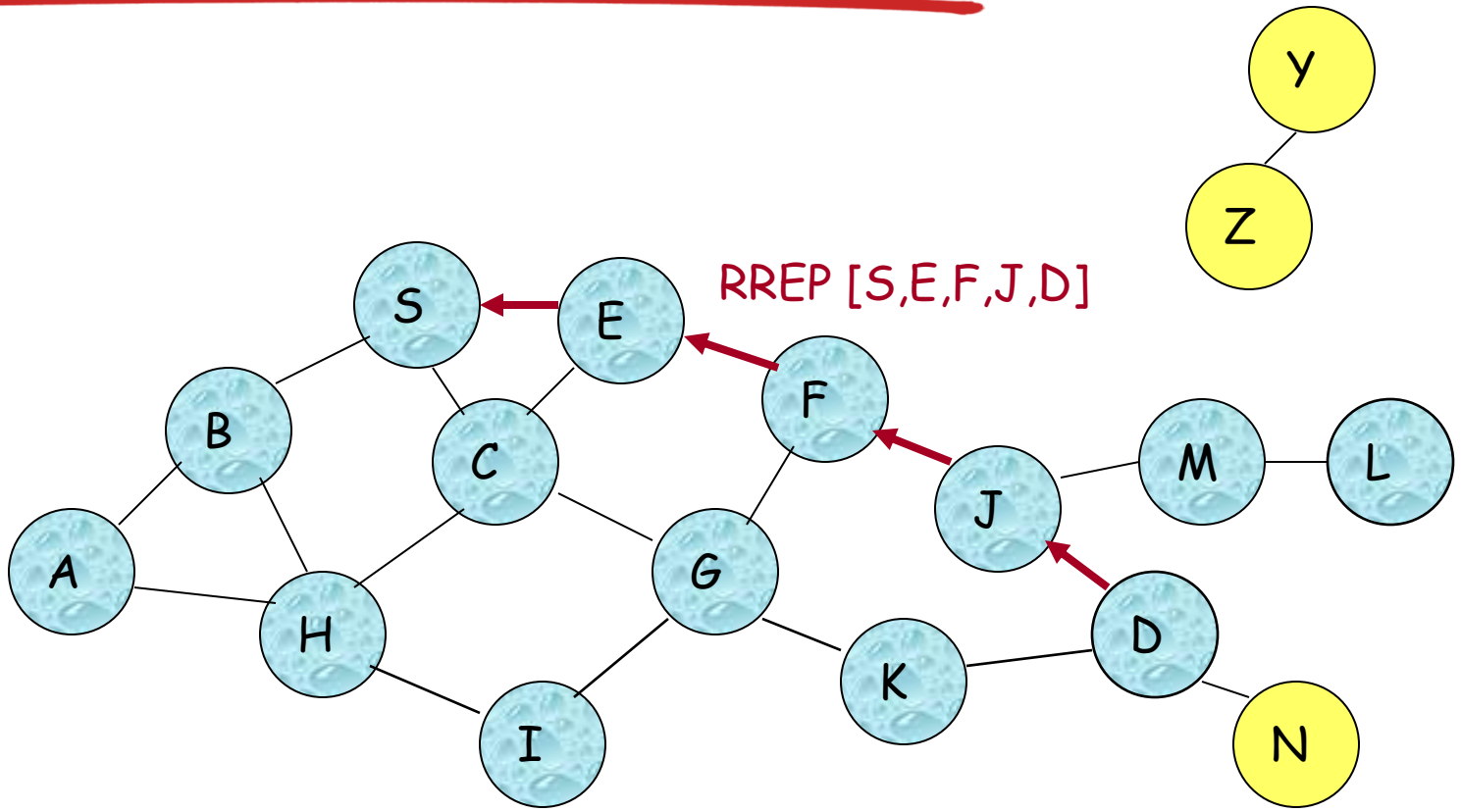


- Node D does not forward RREQ, because node D is the intended target of the route discovery

Route Discovery in DSR

- 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

Route Reply in DSR



Represents RREP control message

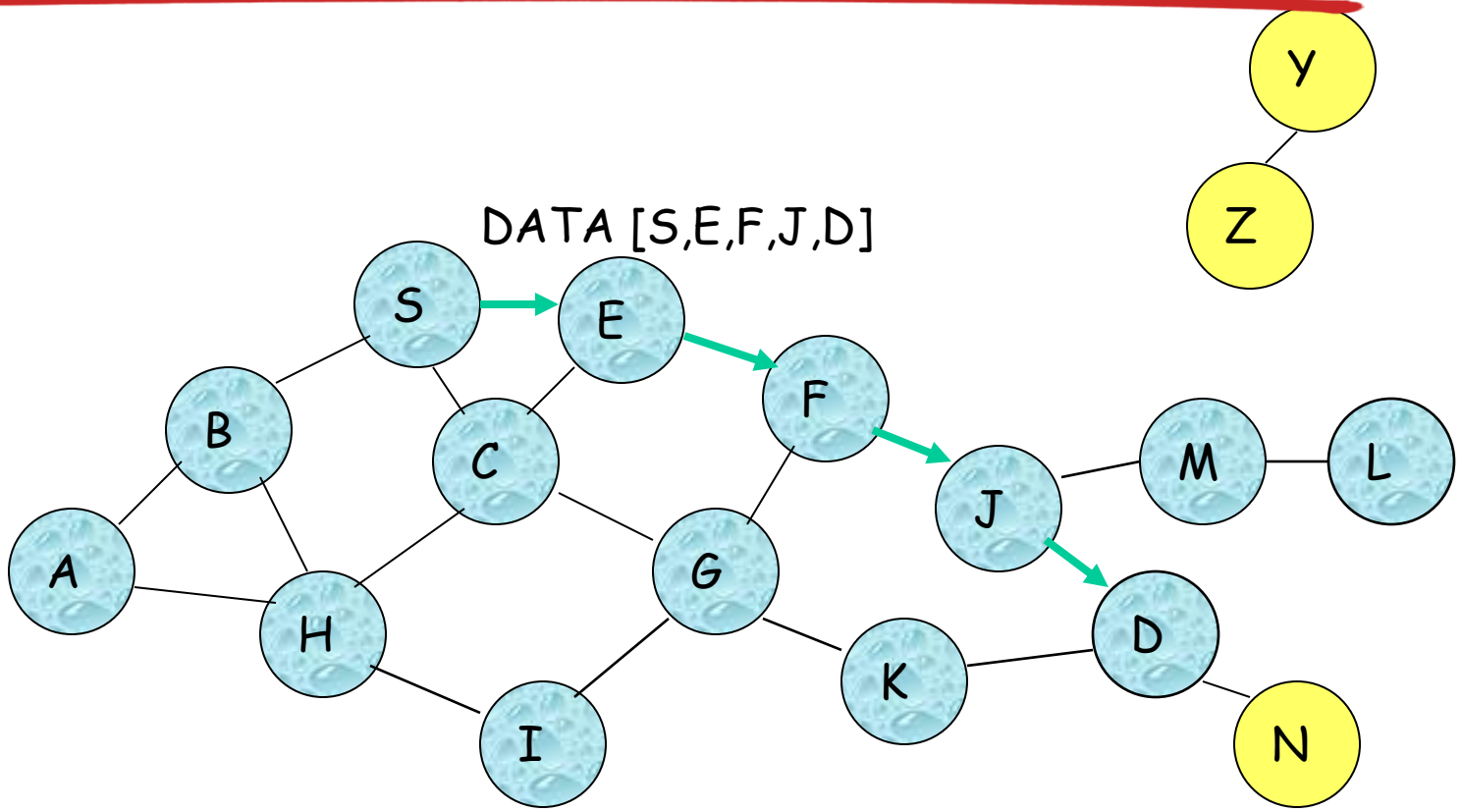
Route Reply in DSR

- Route Reply can be sent by reversing the route in Route Request (RREQ) only if links are guaranteed to be bi-directional
  - To ensure this, RREQ should be forwarded only if it received on a link that is known to be bi-directional
- If unidirectional (asymmetric) links are allowed, then RREP may need a route discovery for S from node D
  - Unless node D already knows a route to node S
  - If a route discovery is initiated by D for a route to S, then the Route Reply is piggybacked on the Route Request from D.
- If IEEE 802.11 MAC is used to send data, then links have to be bi-directional (since Ack is used)

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

Data Delivery in DSR



Packet header size grows with route length

When to Perform a Route Discovery

- When node S wants to send data to node D, but does not know a valid route node D

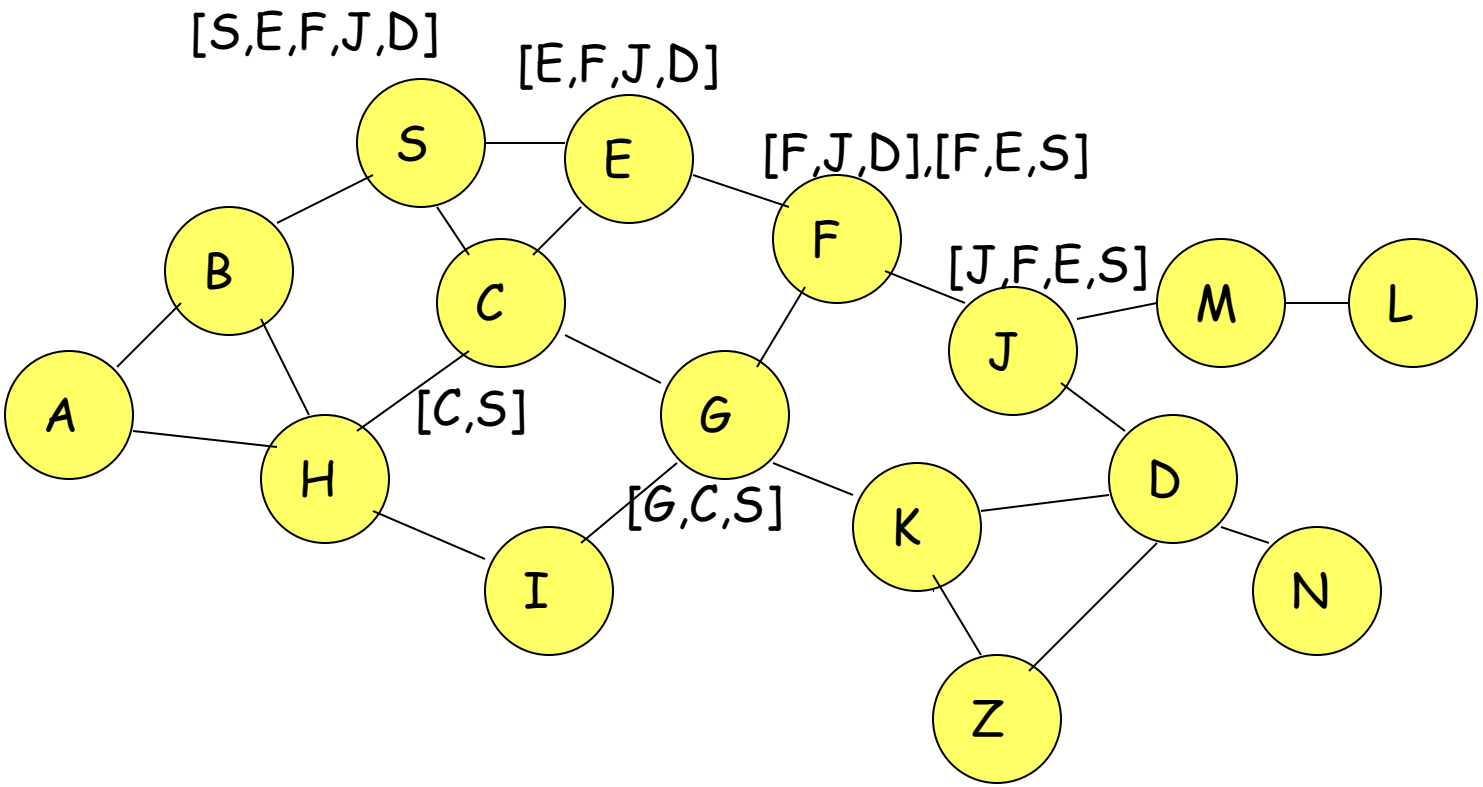
DSR Optimization: Route Caching

- 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, 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 packets

Use of Route Caching

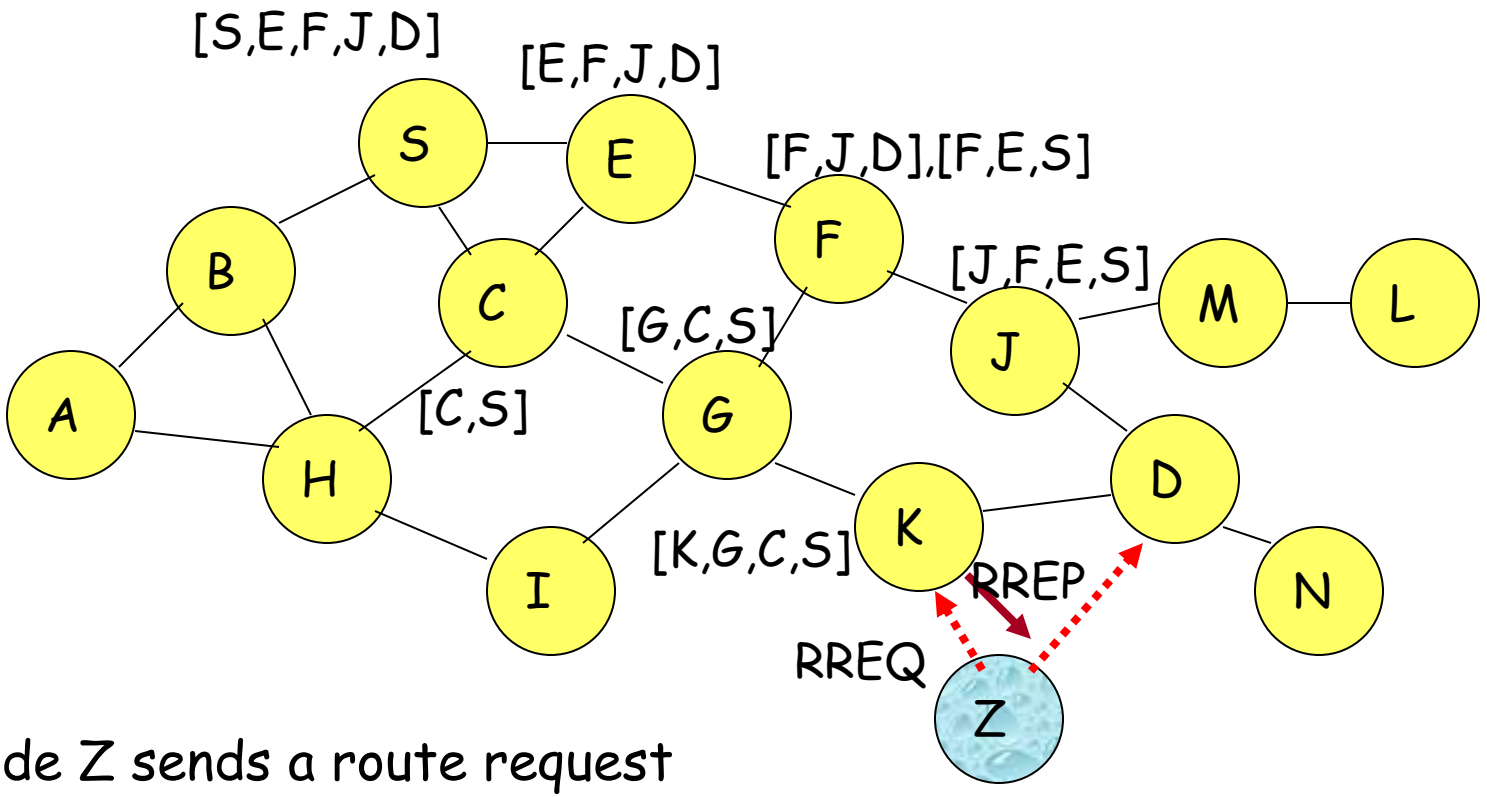
- When node S learns that a route to node D is broken, it uses another route from its local cache, if such a route to D exists in its cache. Otherwise, node S initiates route discovery by sending a route request
- Node X on receiving a Route Request for some node D can send a Route Reply if node X knows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

Use of Route Caching



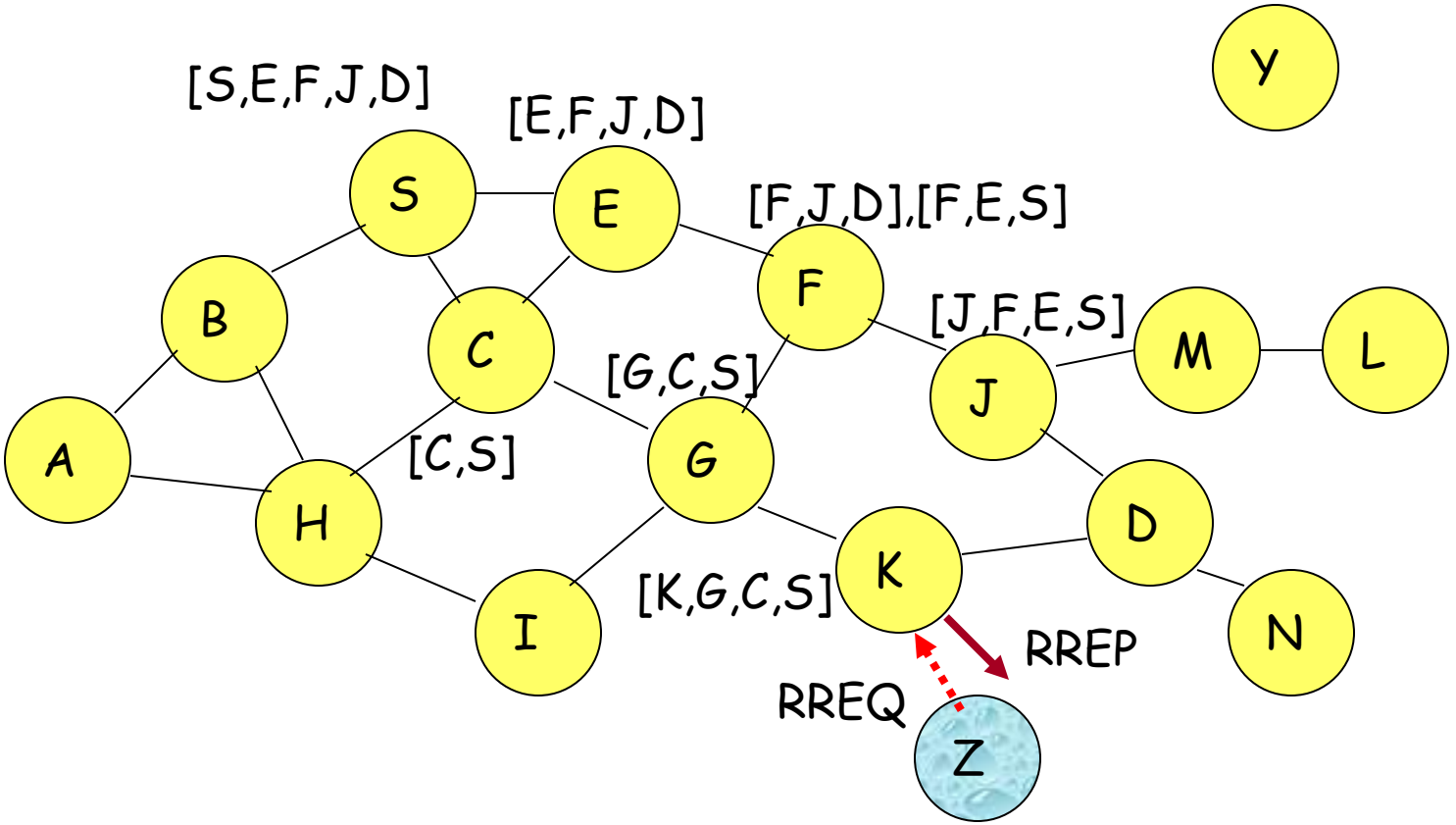
[P,Q,R] Represents cached route at a node
(DSR maintains the cached routes in a tree format)

Use of Route Caching: Can Speed up Route Discovery



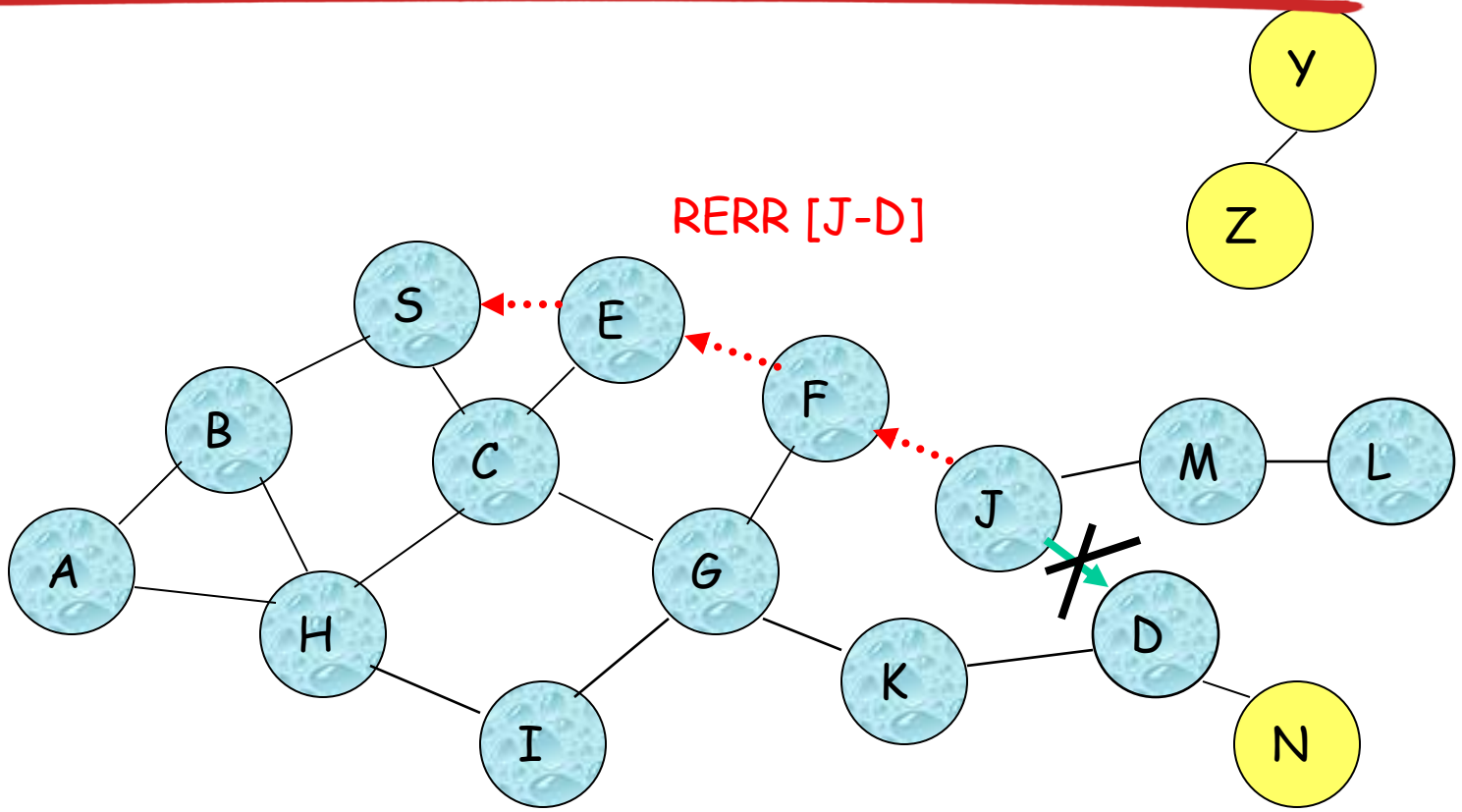
When node Z sends a route request for node C, node K sends back a route reply [Z,K,G,C] to node Z using a locally cached route

Use of Route Caching:
Can Reduce Propagation of Route Requests



Assume that there is no link between D and Z.
Route Reply (RREP) from node K limits flooding of RREQ.
In general, the reduction may be less dramatic.

Route Error (RERR)



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

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

Route Caching: Beware!

- Stale caches can adversely affect performance
- With passage of time and host mobility, cached routes may become invalid
- A sender host may try several stale routes (obtained from local cache, or replied from cache by other nodes), before finding a good route
- An illustration of the adverse impact on TCP will be discussed later in the tutorial [Holland99]

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

Dynamic Source Routing: Disadvantages

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

Dynamic Source Routing: Disadvantages

- An intermediate node may send Route Reply using a stale cached route, thus polluting other caches
- This problem can be eased if some mechanism to purge (potentially) invalid cached routes is incorporated.
- For some proposals for cache invalidation, see [Hu00Mobicom]
  - Static timeouts
  - Adaptive timeouts based on link stability

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]

Location-Aided Routing (LAR) [Ko98Mobicom]

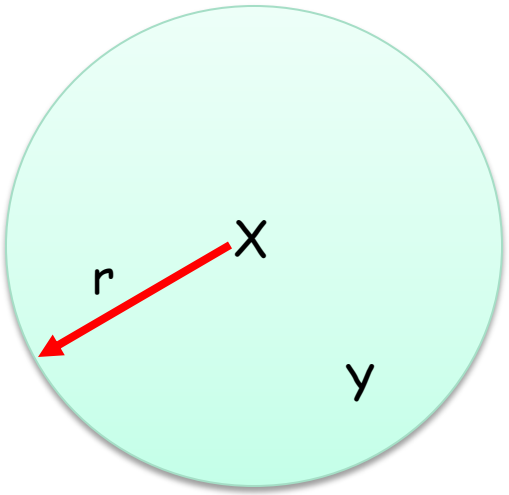
- Exploits location information to limit scope of route request flood
  - Location information may be obtained using GPS
- *Expected Zone* is determined as a region that is expected to hold the current location of the destination
  - Expected region determined based on potentially old location information, 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

Expected Zone in LAR

X = last known location of node D, at time t0

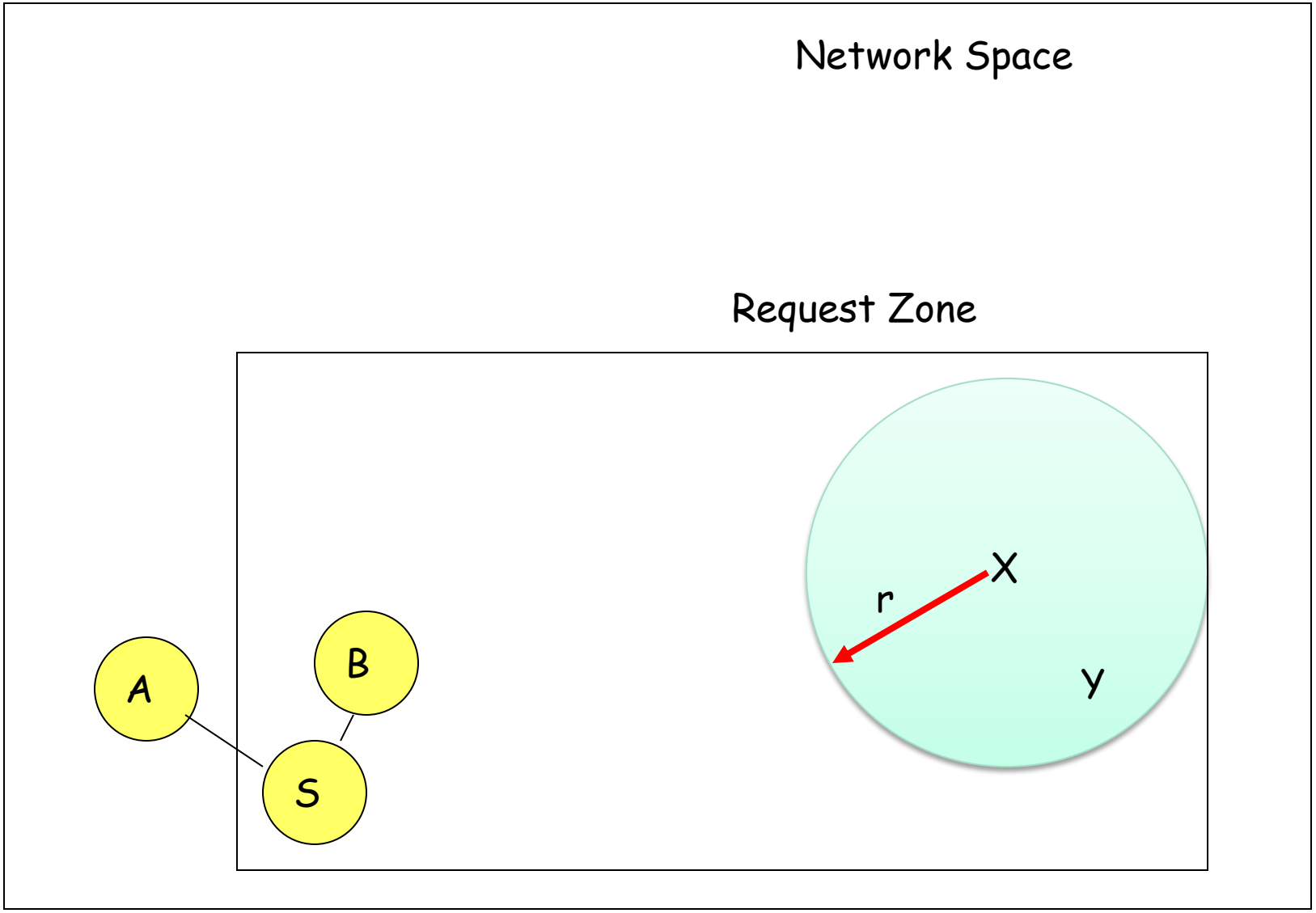
Y = location of node D at current time t1, unknown to node S

r = (t1 - t0) * estimate of D's speed



Expected Zone

Request Zone in LAR



LAR

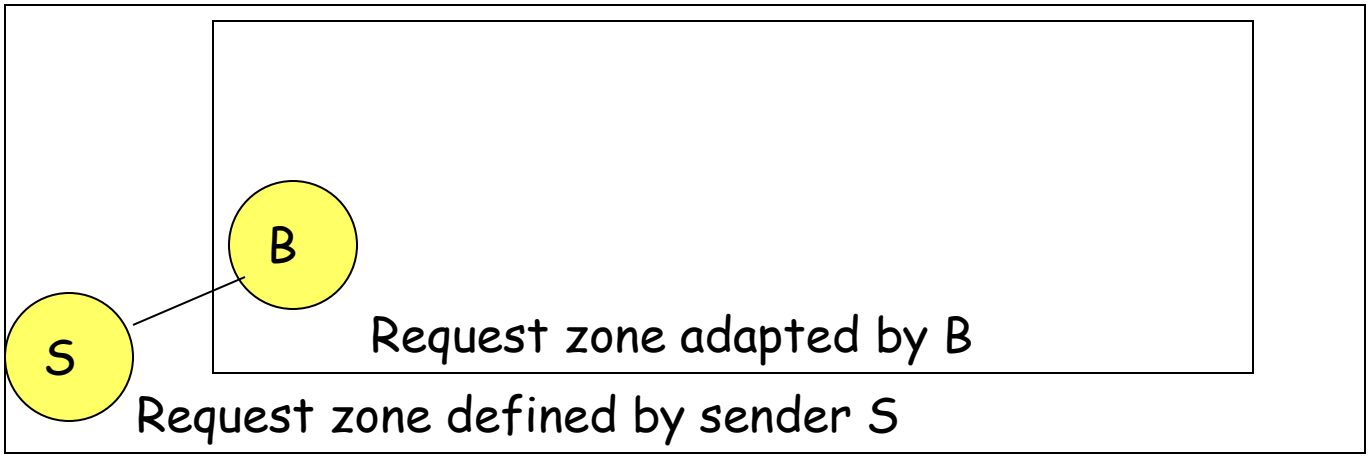
- Only nodes within the request zone forward route requests
  - Node A does not forward RREQ, but node B does (see previous slide)
- Request zone explicitly specified in the route request
- Each node must know its physical location to determine whether it is within the request zone

LAR

- Only nodes within the request zone forward route requests
- If route discovery using the smaller request zone fails to find a route, the sender initiates another route discovery (after a timeout) using a larger request zone
  - the larger request zone may be the entire network
- Rest of route discovery protocol similar to DSR

LAR Variations: Adaptive Request Zone

- Each node may modify the request zone included in the forwarded request
- Modified request zone may be determined using more recent/accurate information, and may be smaller than the original request zone



LAR Variations: Implicit Request Zone

- In the previous scheme, a route request explicitly specified a request zone
- Alternative approach: A node X forwards a route request received from Y if node X is deemed to be closer to the expected zone as compared to Y
- The motivation is to attempt to bring the route request physically closer to the destination node after each forwarding

Location-Aided Routing

- The basic proposal assumes that, *initially,* location information for node X becomes known to Y only during a route discovery
- This location information is used for a future route discovery
  - Each route discovery yields more updated information which is used for the next discovery

Variations

- Location information can also be piggybacked on any message from Y to X
- Y may also proactively distribute its location information
  - Similar to other protocols discussed later (e.g., DREAM, GLS)

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

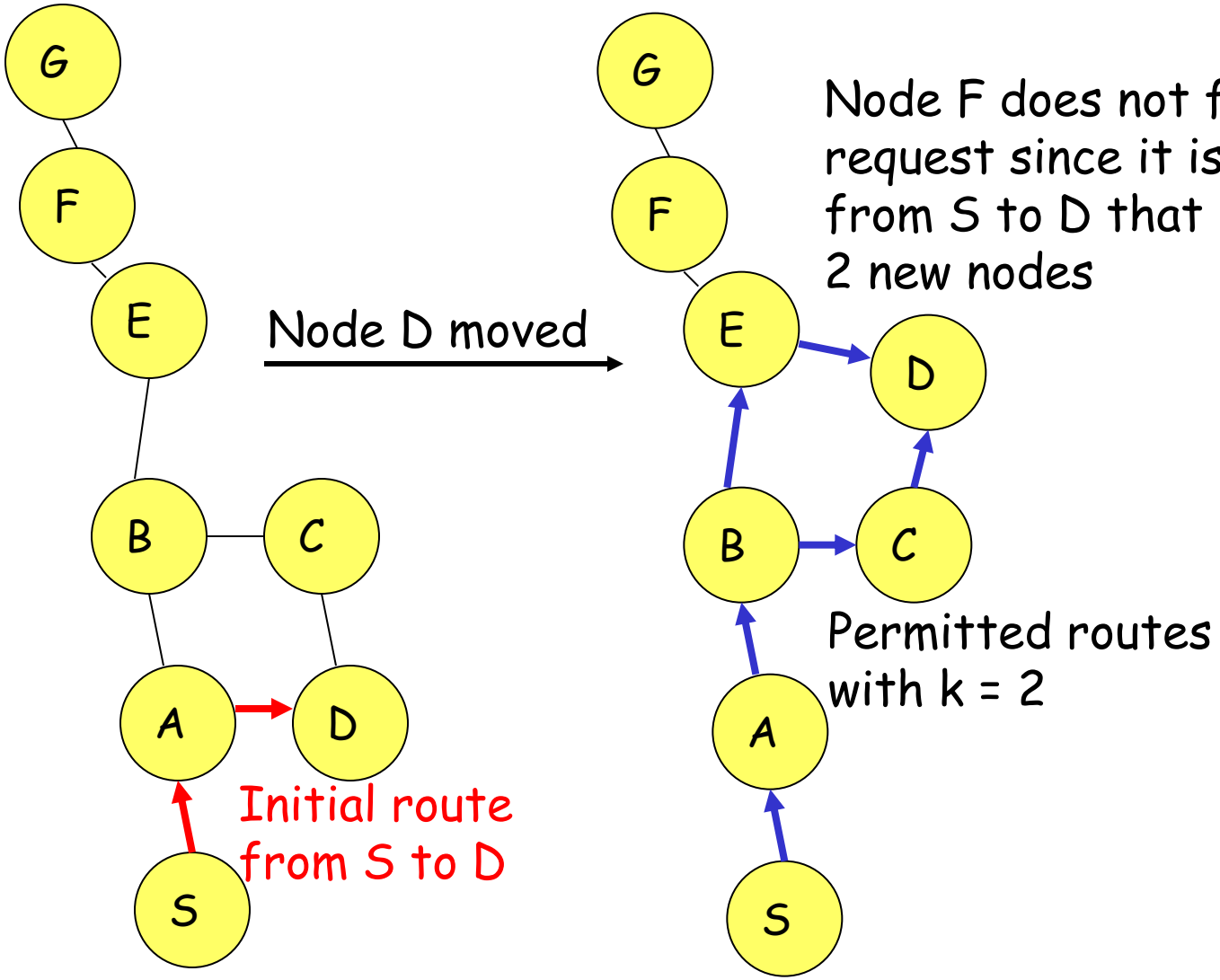
Query Localization [Castaneda99Mobicom]

- Limits route request flood without using physical information
- Route requests are propagated only along paths that are *close* to the previously known route
- The *closeness* property is defined without using physical location information

Query Localization

- Path locality heuristic: Look for a new path that contains at most *k* nodes that were not present in the previously known route
- Old route is piggybacked on a Route Request
- Route Request is forwarded only if the accumulated route in the Route Request contains at most *k* new nodes that were absent in the old route
  - this limits propagation of the route request

Query Localization: Example



Query Localization

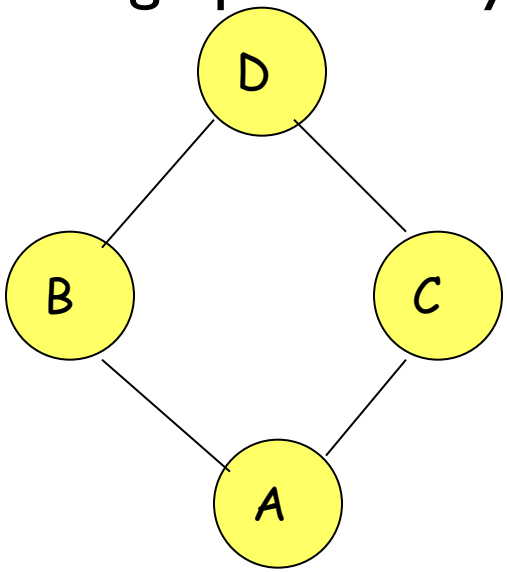
- Advantages:
  - Reduces overhead of route discovery without using physical location information
  - Can perform better in presence of obstructions by searching for new routes in the *vicinity* of old routes

- Disadvantage:
  - May yield routes longer than LAR

    (Shortest route may contain more than k new nodes)

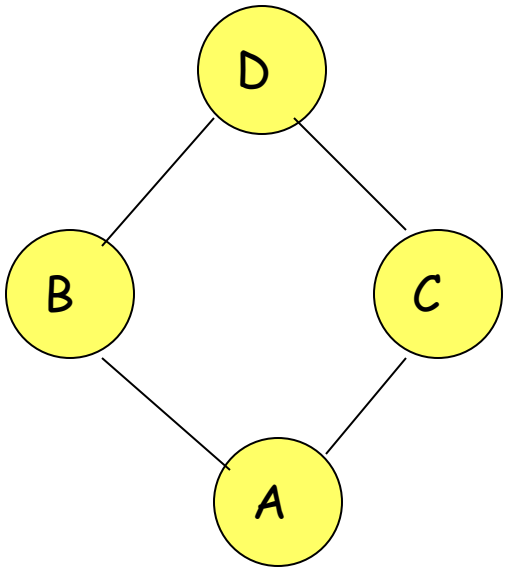
Broadcast Storm Problem [Ni99Mobicom]

- 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

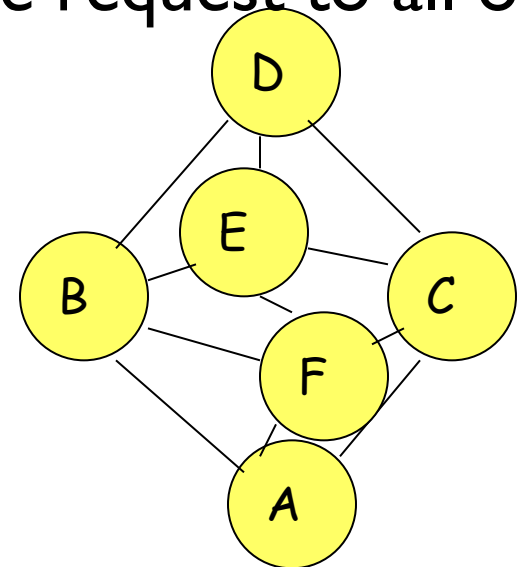


Solutions for Broadcast Storm

- 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

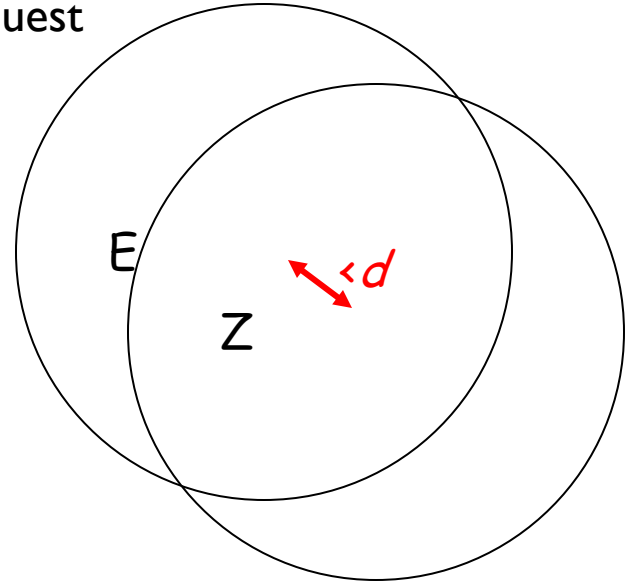
Solutions for Broadcast Storms

- 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



Solutions for Broadcast Storms

- Distance-Based Scheme: If node E hears RREQ broadcasted by some node Z within physical distance *d*, then E will not re-broadcast the request
- Intuition: Z and E are too close, so transmission areas covered by Z and E are not very different
  - if E re-broadcasts the request, not many nodes who have not already heard the request from Z will hear the request



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

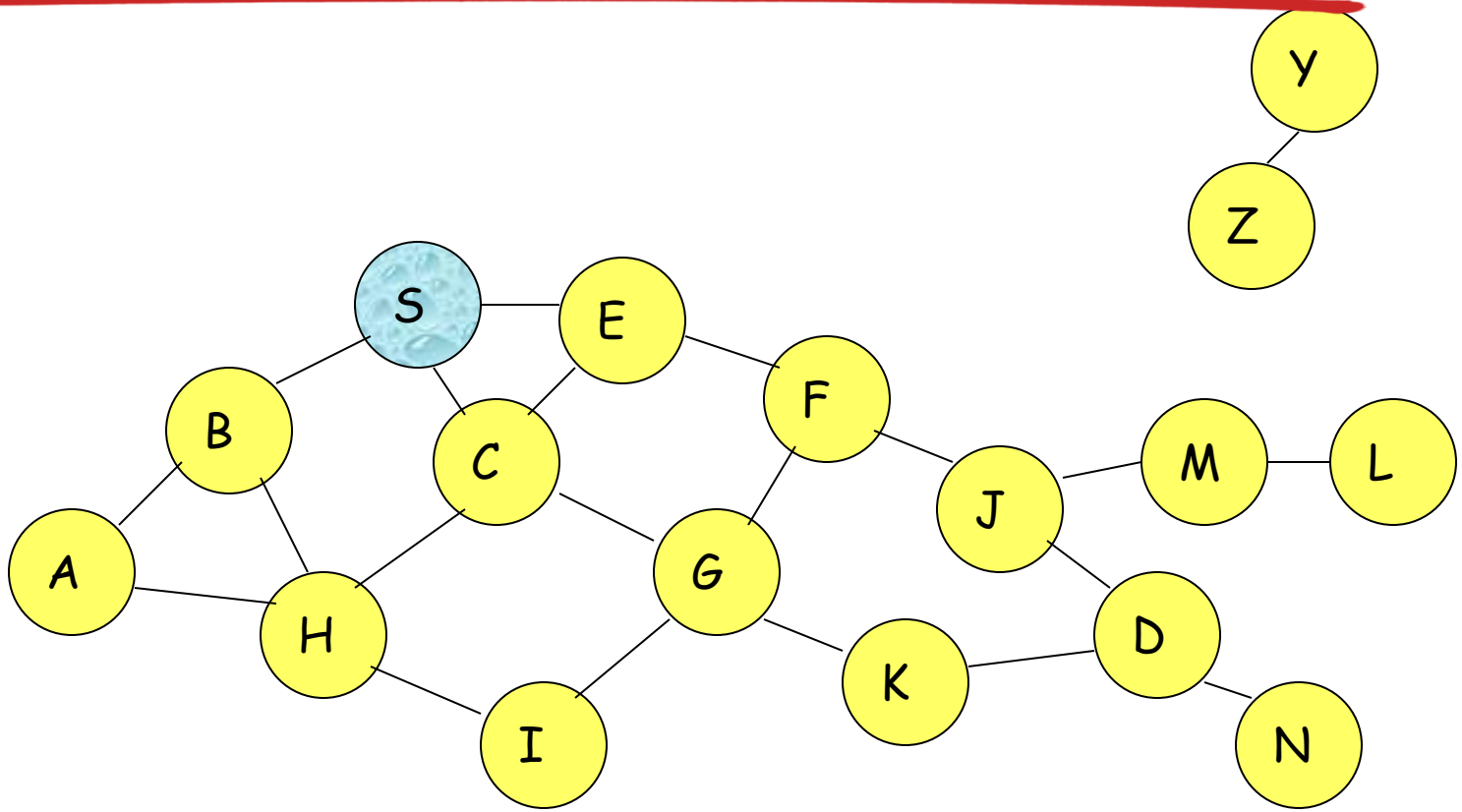
Ad Hoc On-Demand Distance Vector Routing (AODV) [Perkins99Wmcsa]

- 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

AODV

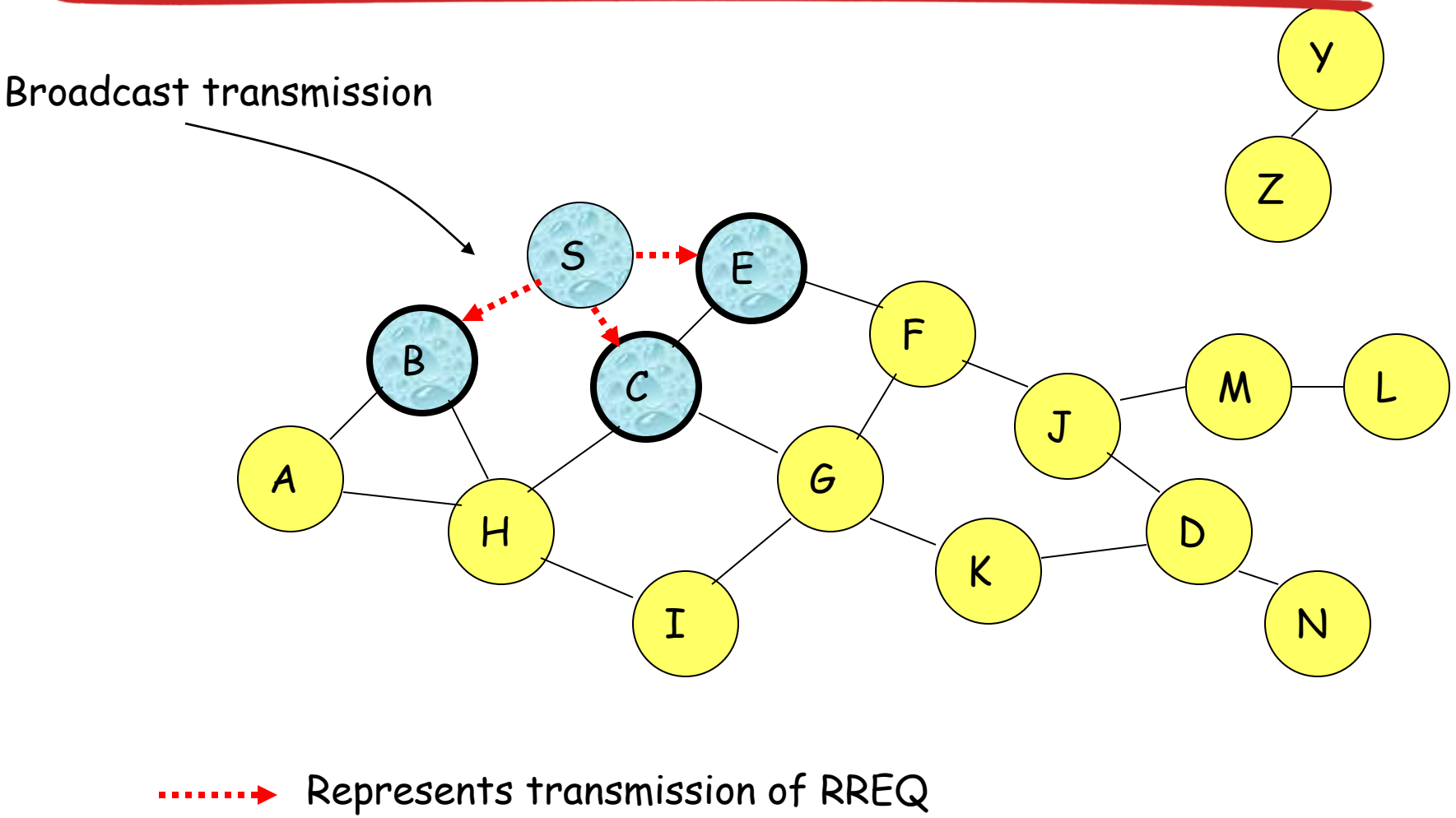
- Route Requests (RREQ) are forwarded in a manner similar to DSR
- When a node re-broadcasts a Route Request, it sets up a reverse path pointing towards the source
  - AODV assumes symmetric (bi-directional) links
- When the intended destination receives a Route Request, it replies by sending a Route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

Route Requests in AODV

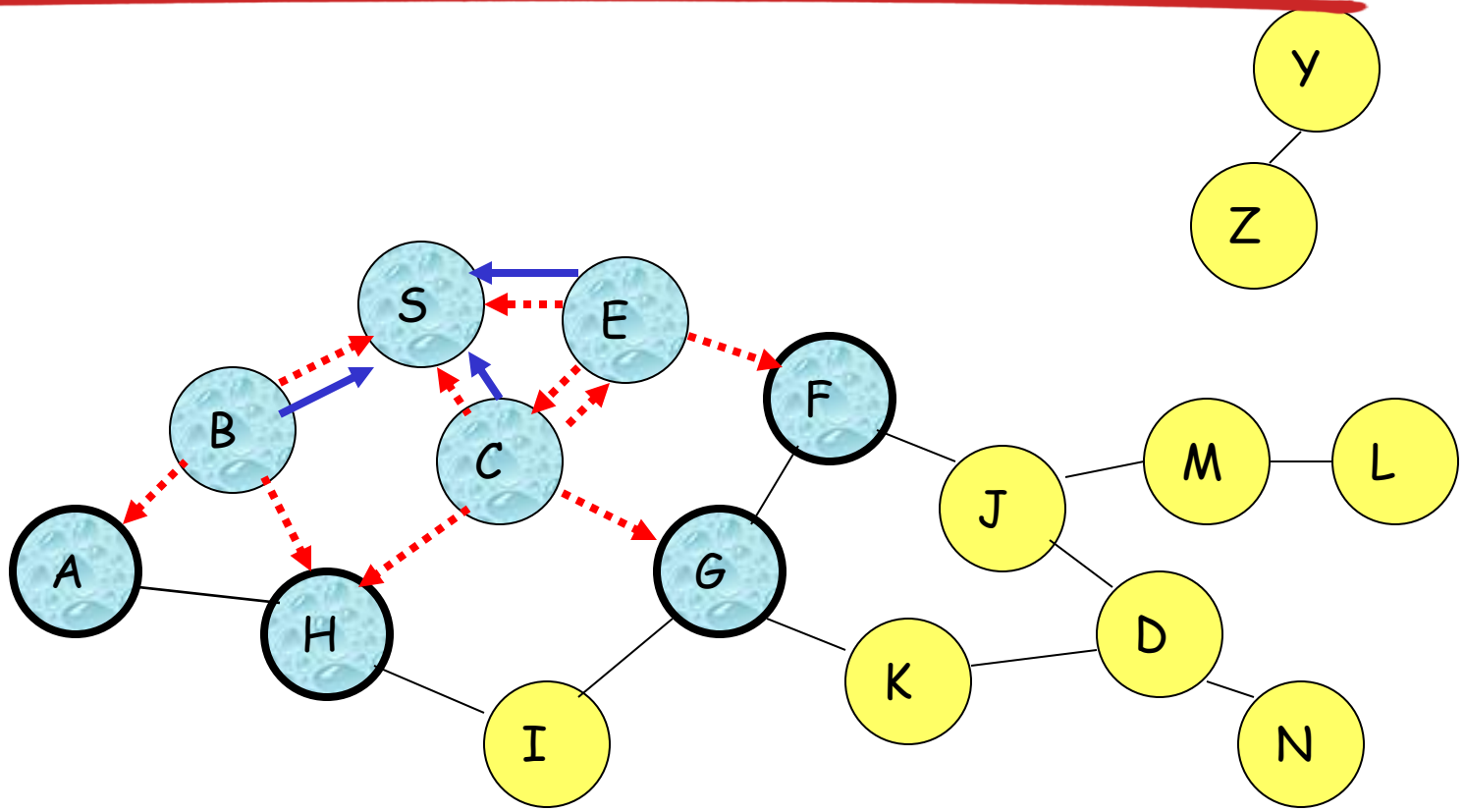


Represents a node that has received RREQ for D from S

Route Requests in AODV

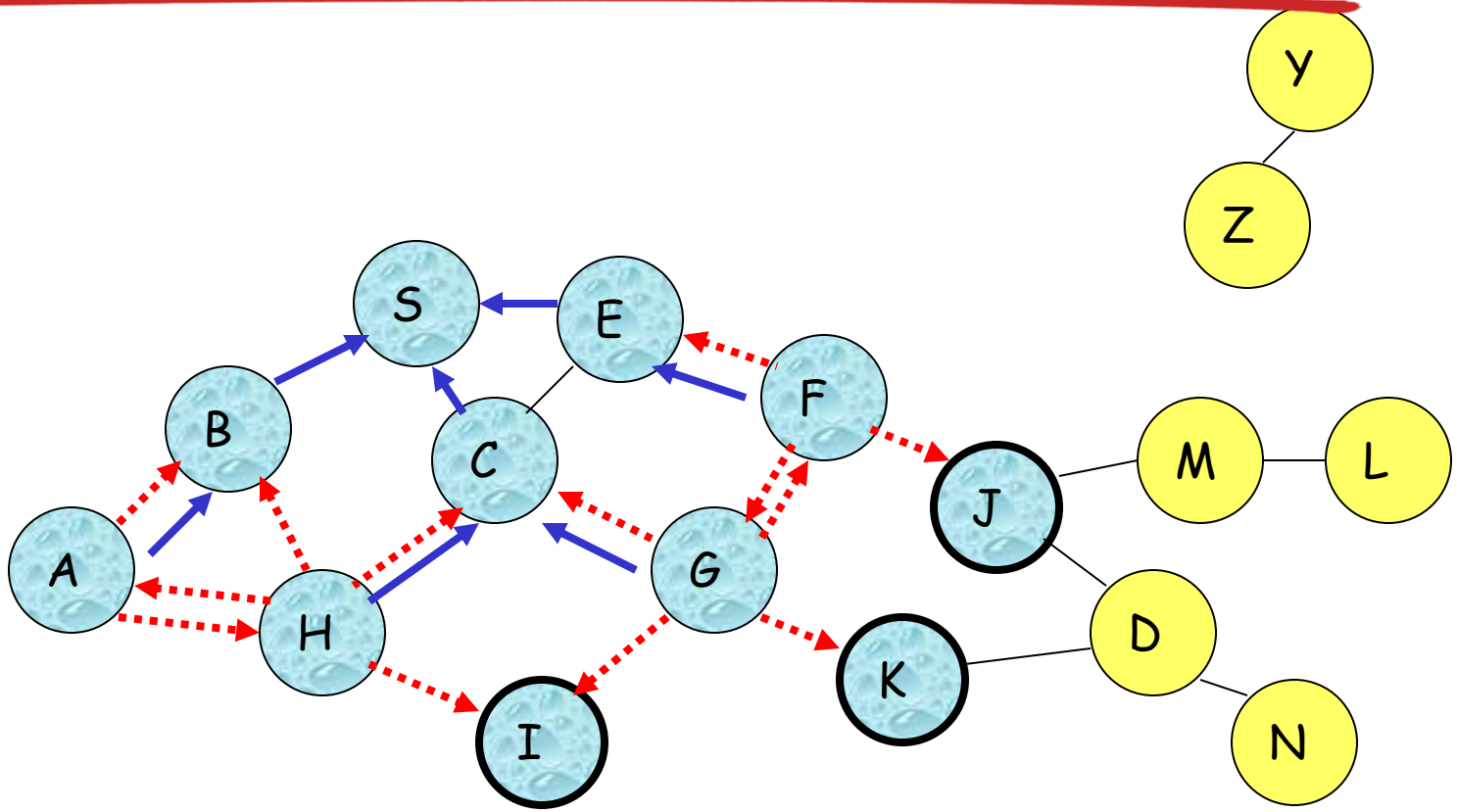


Route Requests in AODV



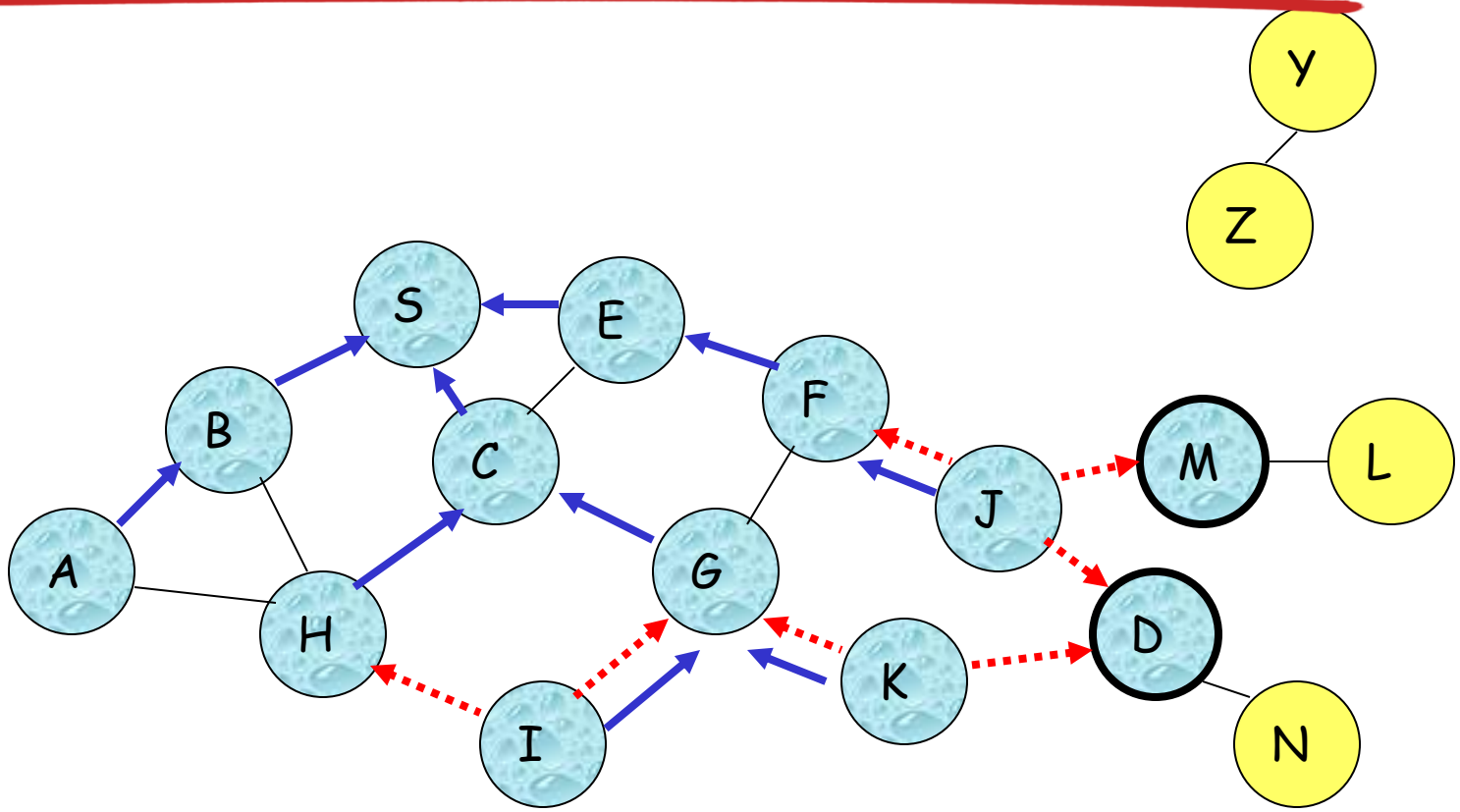
Represents links on Reverse Path

Reverse Path Setup in AODV

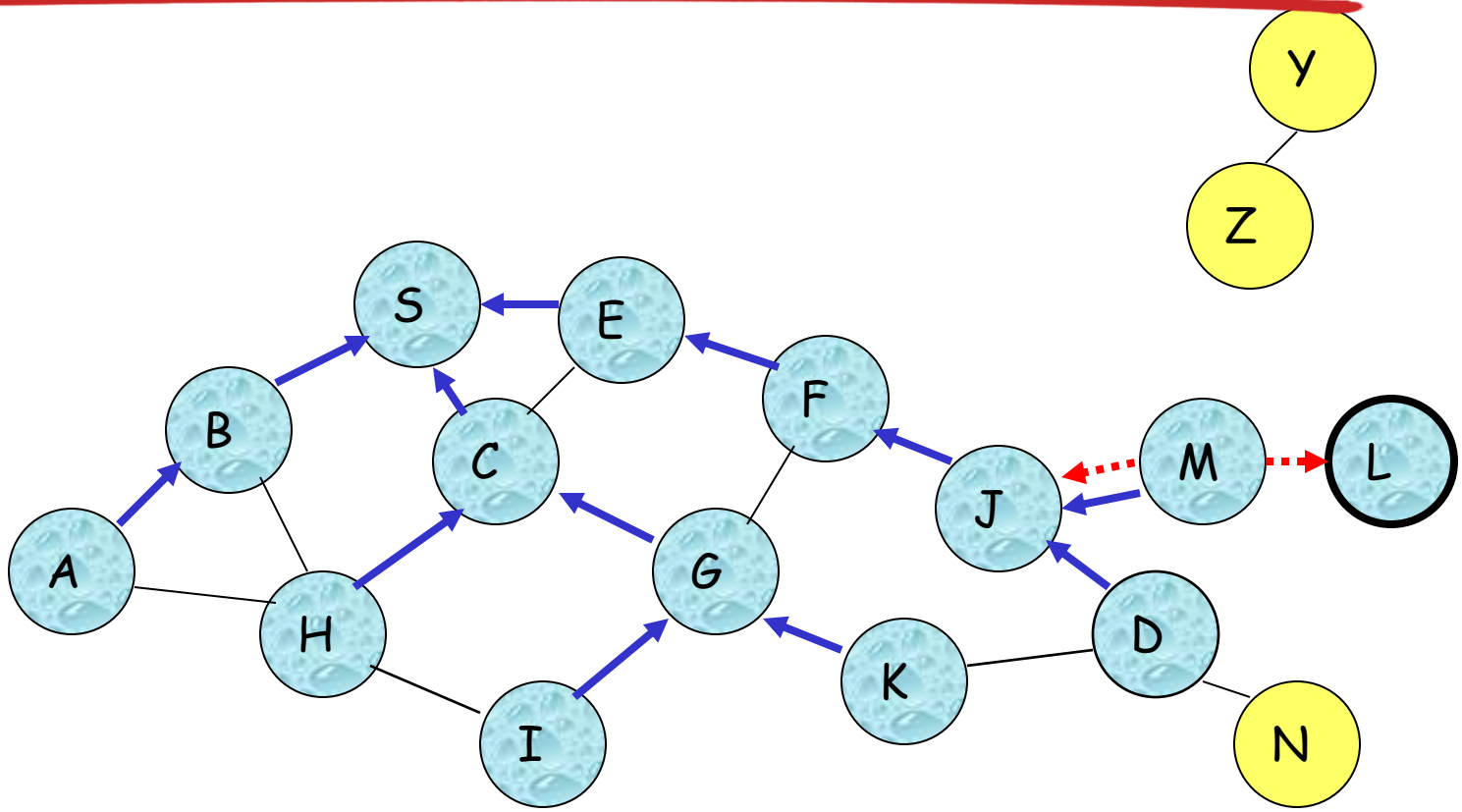


- Node C receives RREQ from G and H, but does not forward it again, because node C has already forwarded RREQ once

Reverse Path Setup in AODV

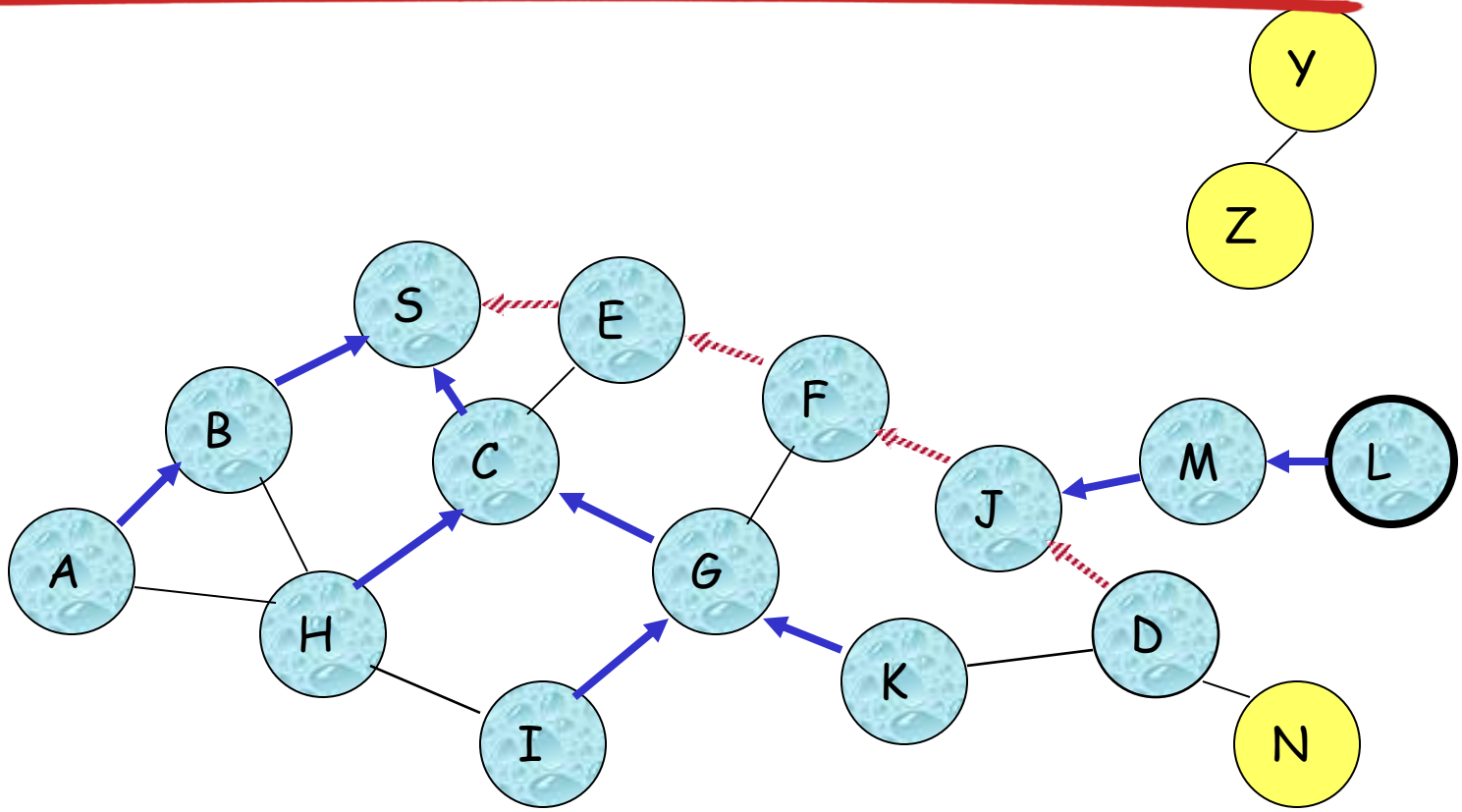


Reverse Path Setup in AODV



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

Route Reply in AODV

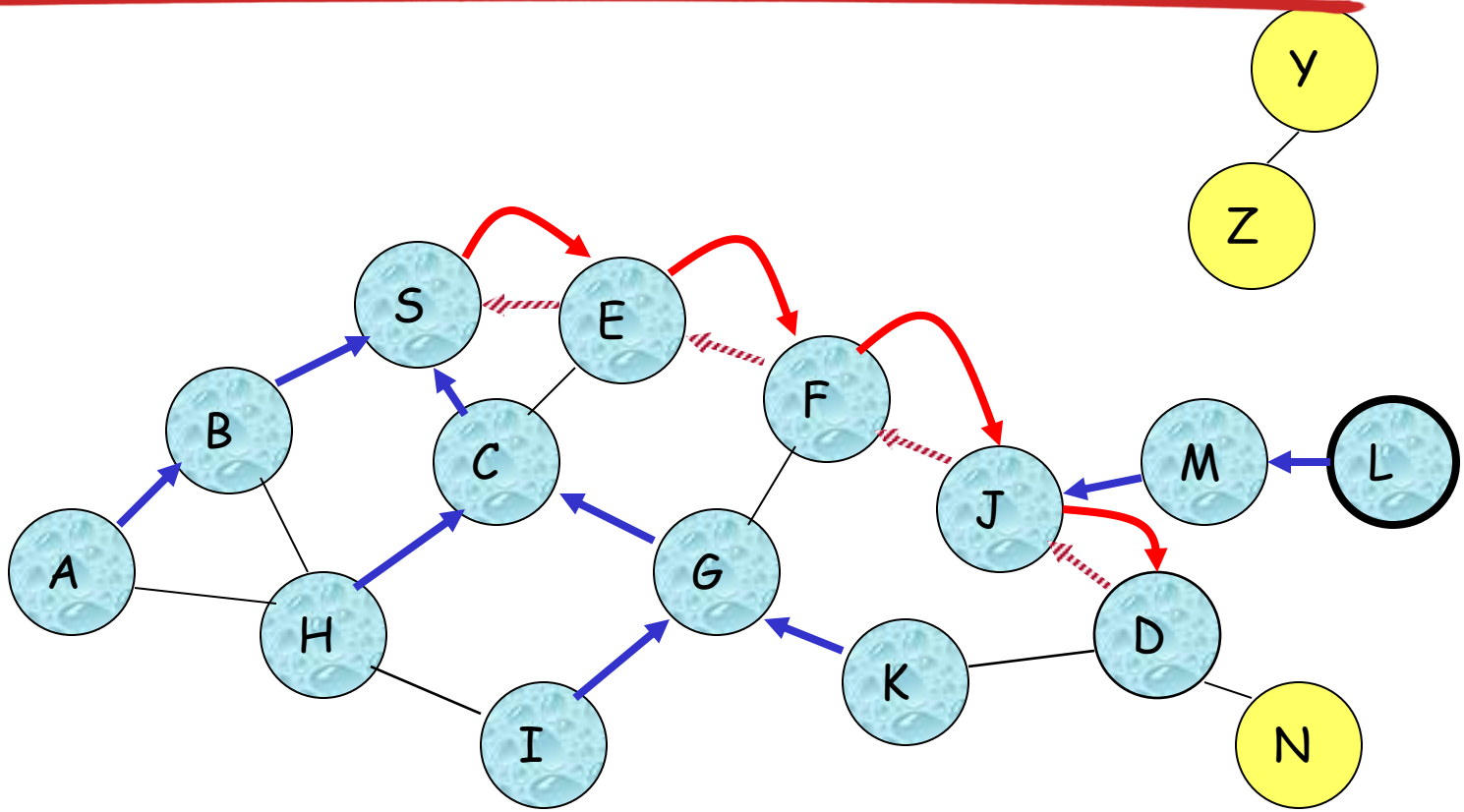


Represents links on path taken by RREP

Route Reply in AODV

- An intermediate node (not the destination) may also send a Route Reply (RREP) provided that it knows a more recent path than the one previously known to sender S
- To determine whether the path known to an intermediate node is more recent, *destination sequence numbers* are used
- The likelihood that an intermediate node will send a Route Reply when using AODV not as high as DSR
  - A new Route Request by node S for a destination is assigned a higher destination sequence number. An intermediate node which knows a route, but with a smaller sequence number, cannot send Route Reply

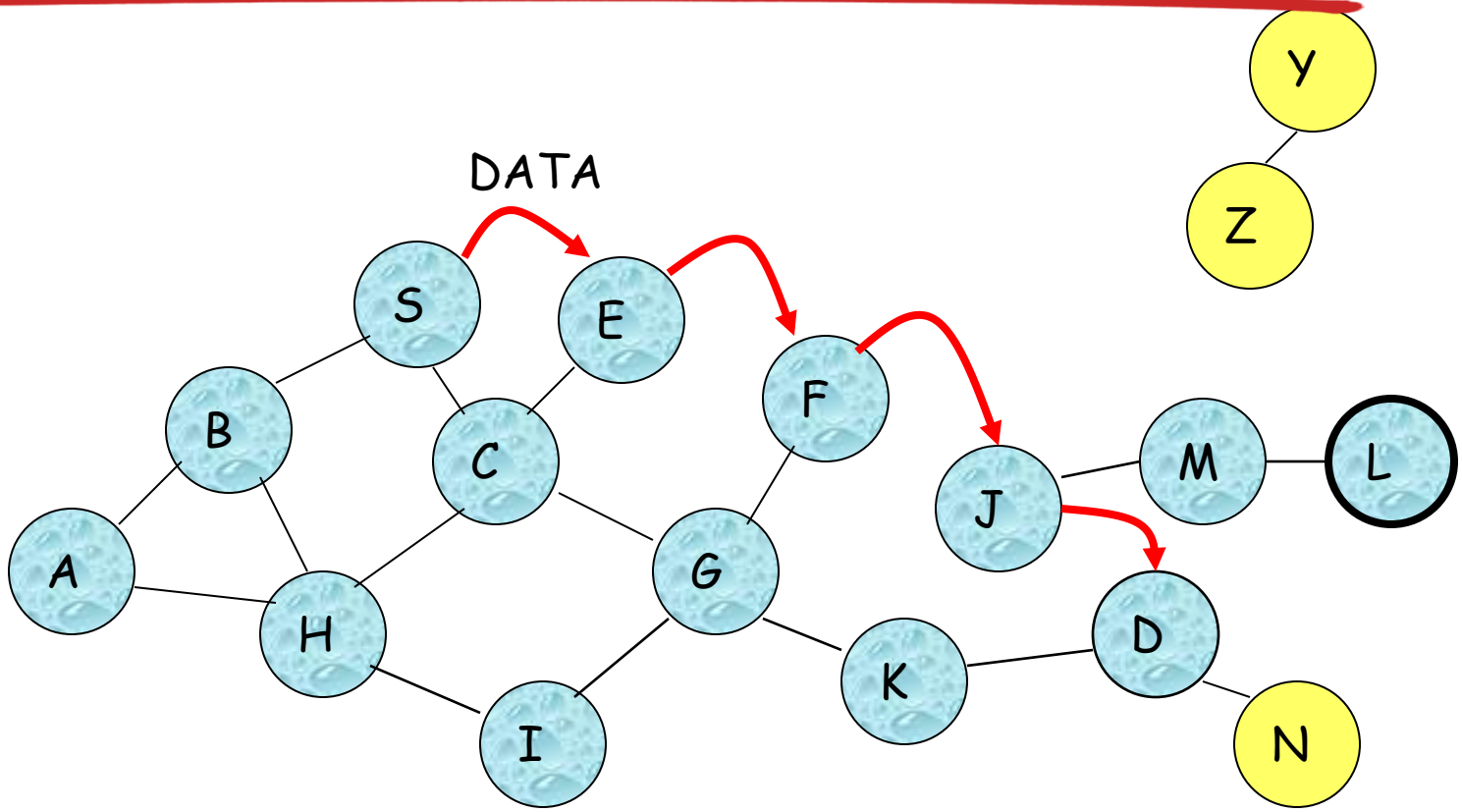
Forward Path Setup in AODV



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 an *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)

Link Failure Reporting

- A neighbor of node X is considered active for a routing table entry if the neighbor sent a packet within *active_route_timeout* interval which was forwarded using that entry
- When the next hop link in a routing table entry breaks, all active neighbors are informed
- Link failures are propagated by means of Route Error messages, which also update destination sequence numbers

Route Error

- When node X is unable to forward packet P (from node S to node D) on link (X,Y), it generates a RERR message
- Node X increments the destination sequence number for D cached at node X
- The incremented sequence number *N* is included in the RERR
- When node S receives the RERR, it initiates a new route discovery for D using destination sequence number at least as large as *N*

Destination Sequence Number

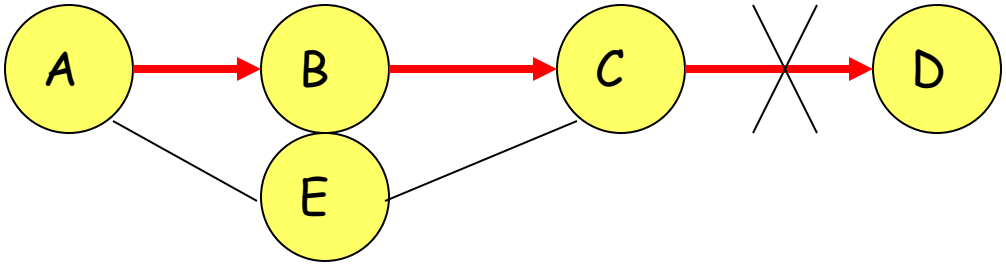
- Continuing from the previous slide …
- When node D receives the route request with destination sequence number N, node D will set its sequence number to N, unless it is already larger than N

Link Failure Detection

- *Hello* messages: Neighboring nodes periodically exchange hello message
- Absence of hello message is used as an indication of link failure
- Alternatively, failure to receive several MAC-level acknowledgement may be used as an indication of link failure

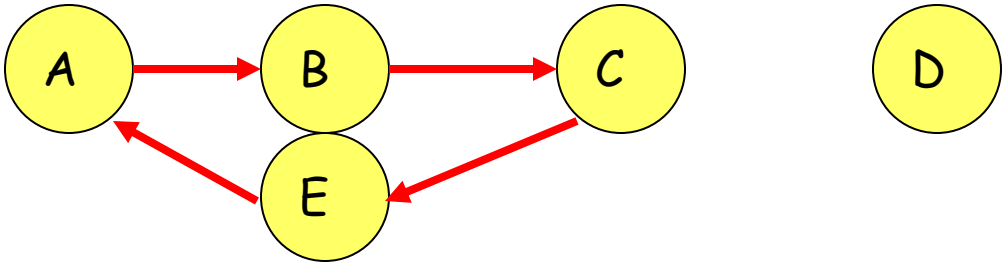
Why Sequence Numbers in AODV

- To avoid using old/broken routes
  - To determine which route is newer
- To prevent formation of loops



  - Assume that A does not know about failure of link C-D because RERR sent by C is lost
  - Now C performs a route discovery for D. Node A receives the RREQ (say, via path C-E-A)
  - Node A will reply since A knows a route to D via node B
  - Results in a loop (for instance, C-E-A-B-C)

Why Sequence Numbers in AODV



- Loop C-E-A-B-C

Optimization: Expanding Ring Search

- Route Requests are initially sent with small Time-to-Live (TTL) field, to limit their propagation
  - DSR also includes a similar optimization
- If no Route Reply is received, then larger TTL tried

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
- Unused routes expire even if topology does not change

WIRELESS ROUTING PROTOCOLS (2):

PROACTIVE PROTOCOLS

Proactive Protocols

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

Link State Routing [Huitema95]

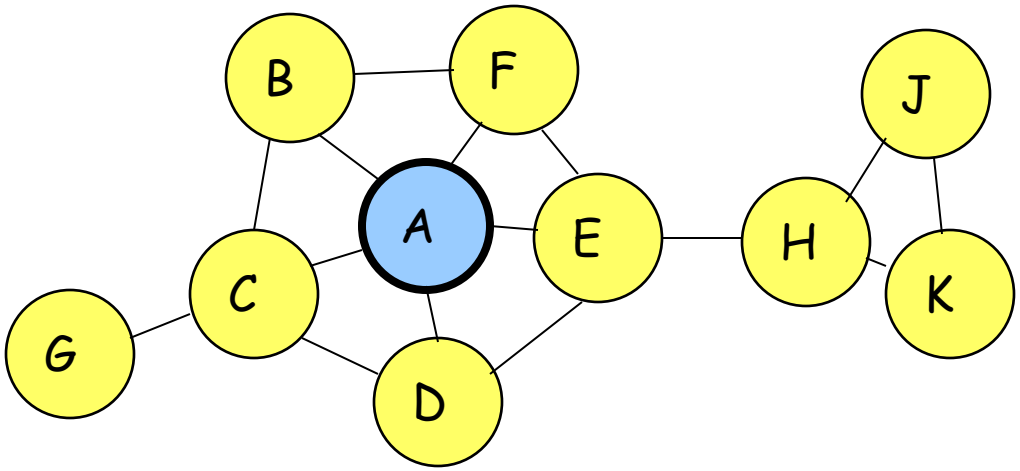
- Each node periodically floods status of its links
- Each node re-broadcasts link state information received from its neighbor
- Each node keeps track of link state information received from other nodes
- Each node uses above information to determine next hop to each destination

Optimized Link State Routing (OLSR) [Jacquet00ietf, Jacquet99Inria]

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

Optimized Link State Routing (OLSR)

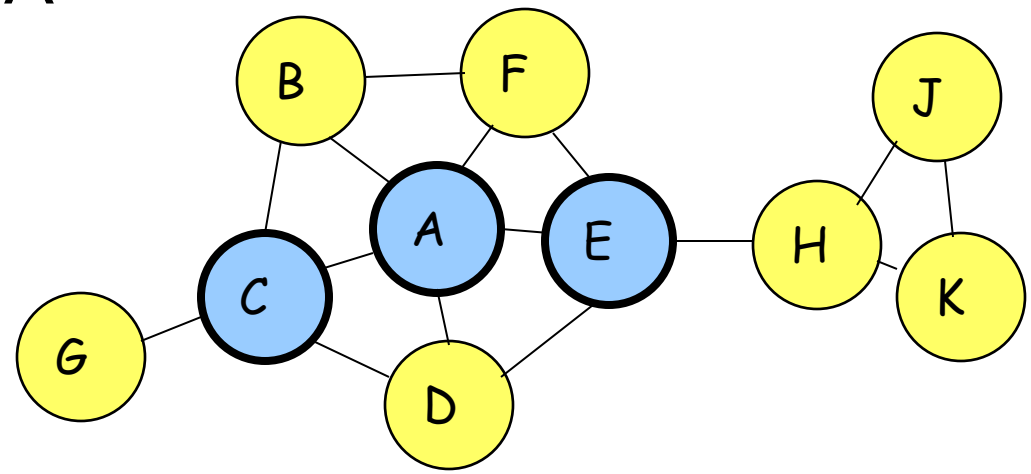
- Nodes C and E are multipoint relays of node A



Node that has broadcast state information from A

Optimized Link State Routing (OLSR)

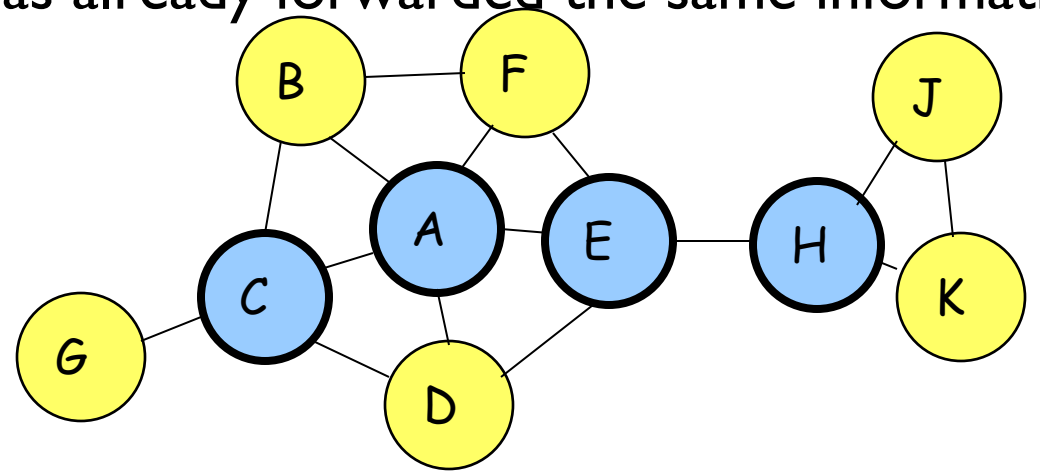
- Nodes C and E forward information received from A



Node that has broadcast state information from A

Optimized Link State Routing (OLSR)

- Nodes E and K are multipoint relays for node H
- Node K forwards information received from H
  - E has already forwarded the same information once



Node that has broadcast state information from A

OLSR

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

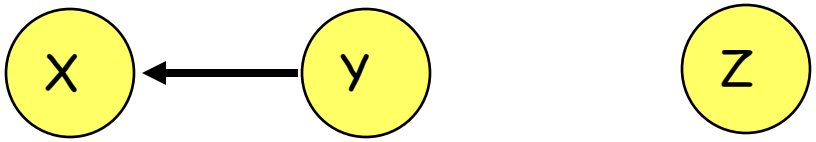
Destination-Sequenced Distance-Vector (DSDV) [Perkins94Sigcomm]

- 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

- 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)

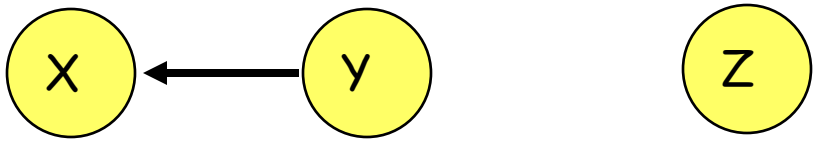
- Assume that node X receives routing information from Y about a route to node Z



- 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

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)

WIRELESS ROUTING PROTOCOLS (1):
HYBRID PROTOCOLS

Zone Routing Protocol (ZRP) [Haas98]

Zone routing protocol combines

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

ZRP

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

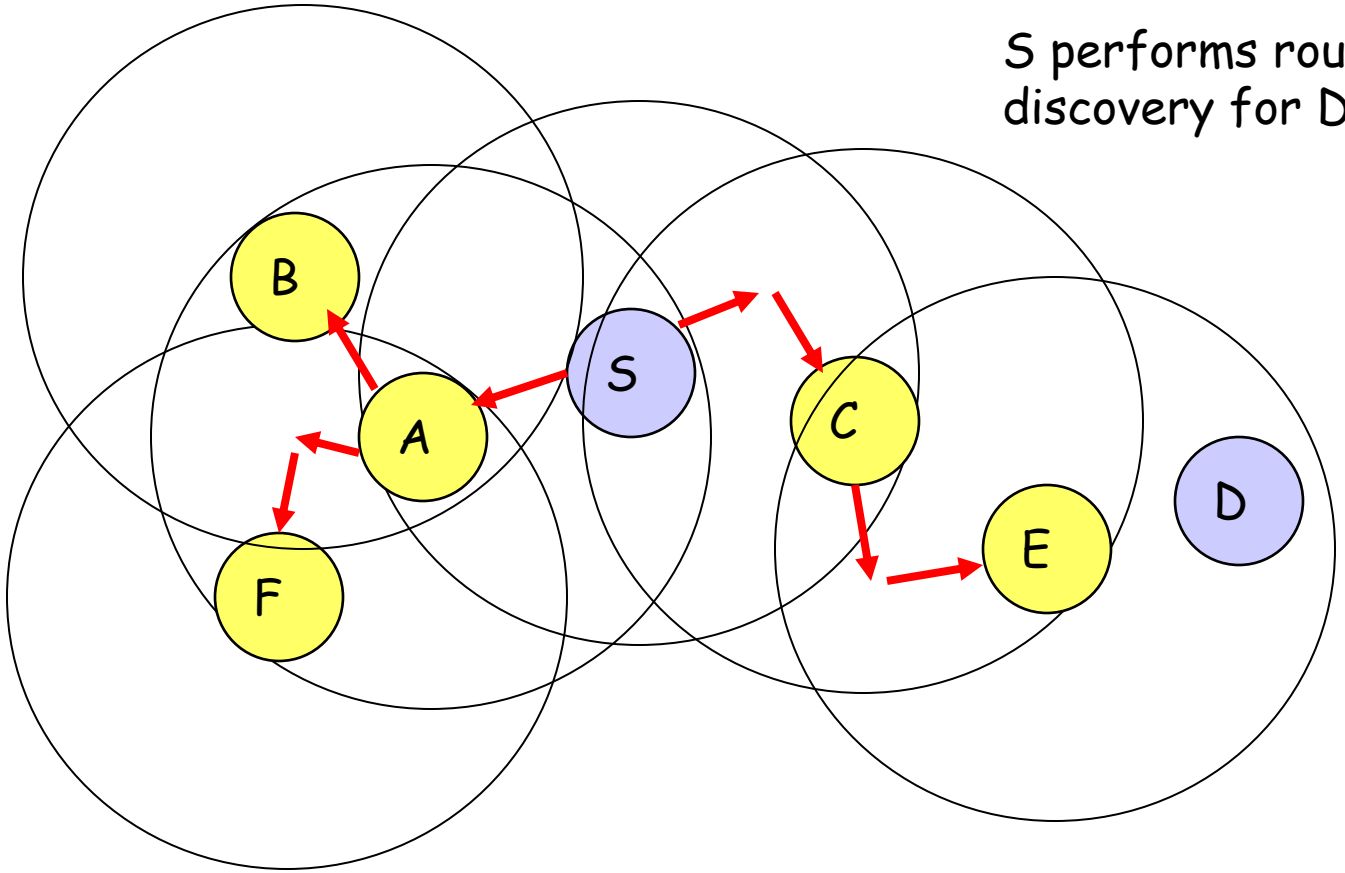
- All nodes at hop distance exactly *d* are said to be peripheral nodes of node X's routing zone

ZRP

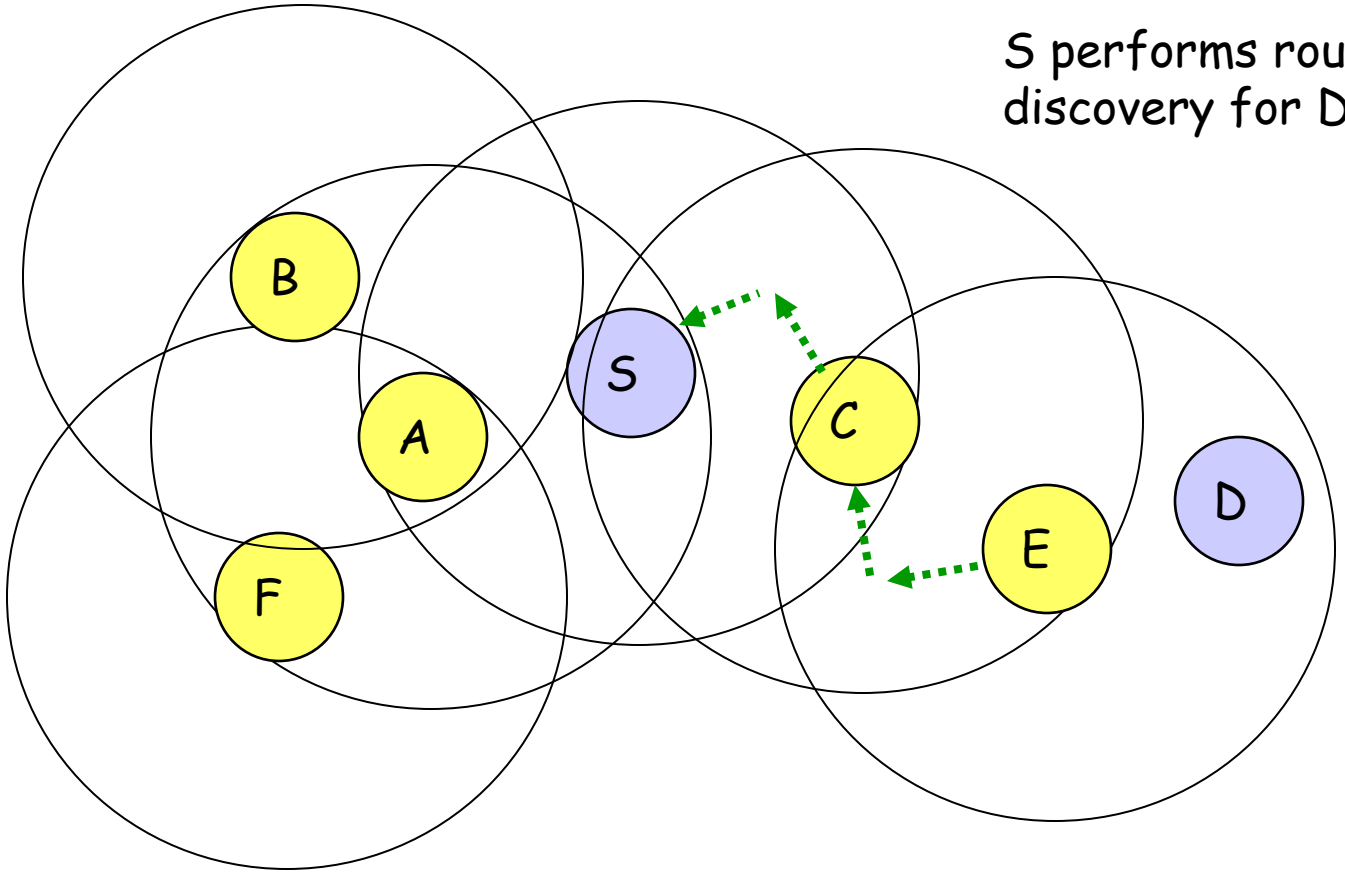
- Intra-zone routing: Pro-actively maintain state information for links within a short distance from any given node
  - Routes to nodes within short distance are thus maintained proactively (using, say, link state or distance vector protocol)

- Inter-zone routing: Use a route discovery protocol for determining routes to far away nodes. Route discovery is similar to DSR with the exception that route requests are propagated via peripheral nodes.

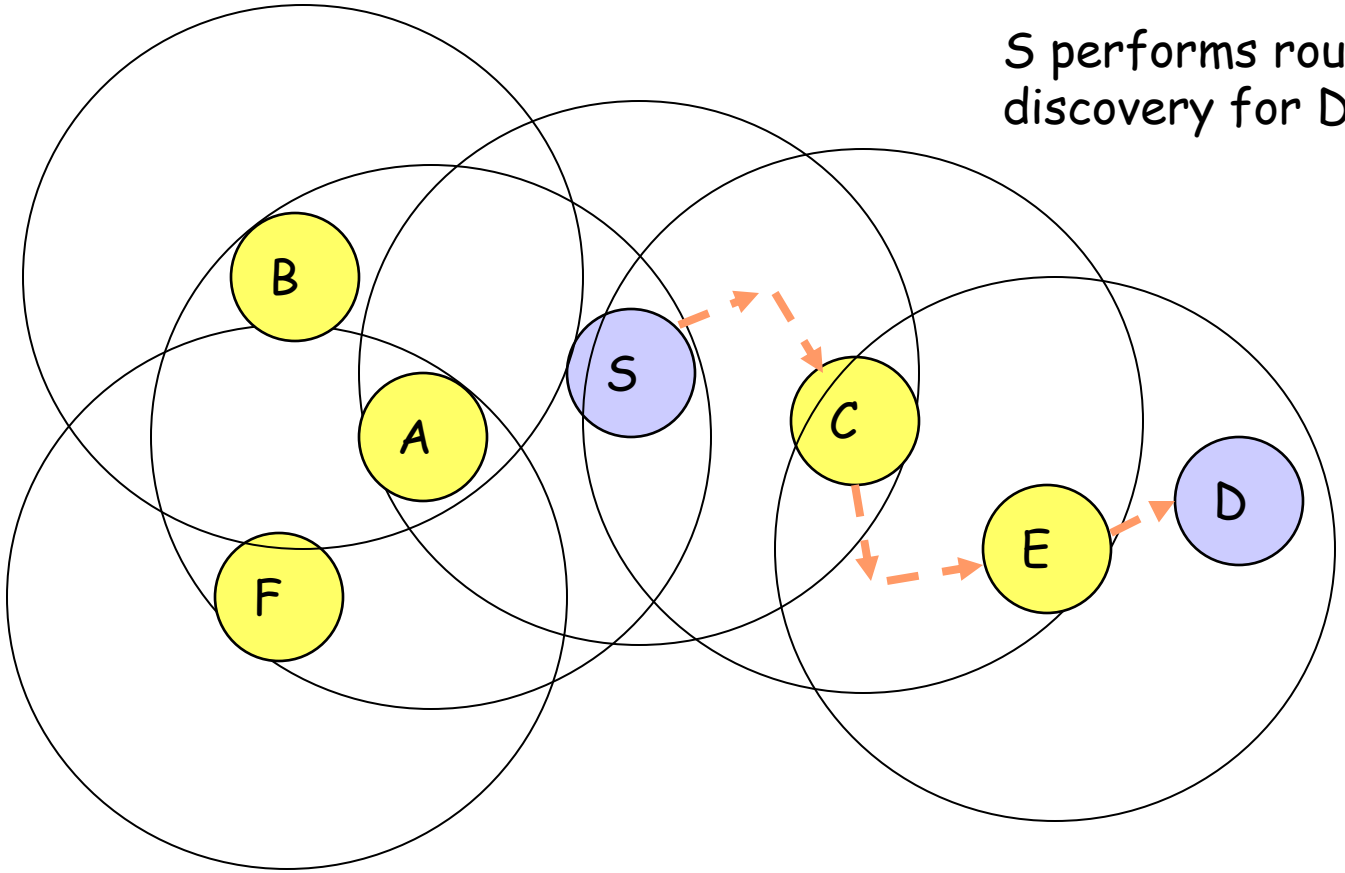
ZRP: Example with Zone Radius = *d* = 2



ZRP: Example with $d = 2$



ZRP: Example with $d = 2$



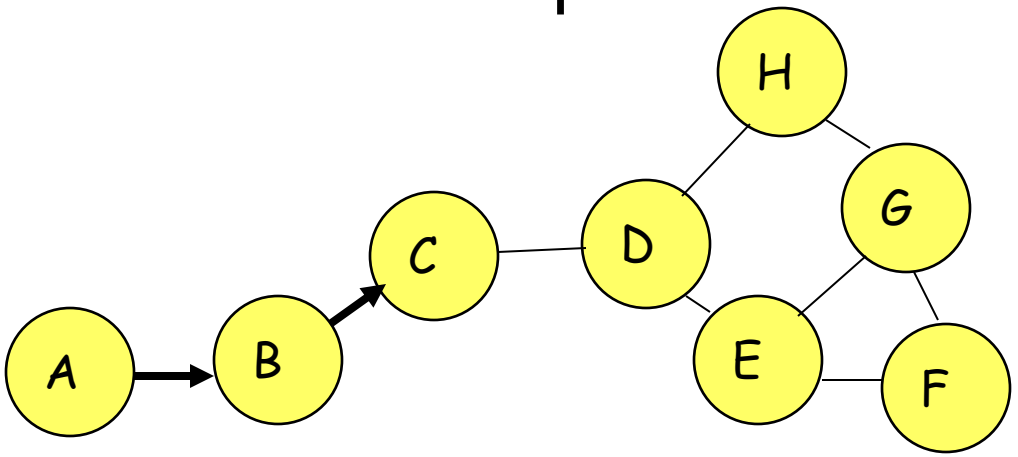
Denotes route taken by Data

Landmark Routing (LANMAR) for MANET with Group Mobility [Pei00Mobihoc]

- A *landmark* node is elected for a group of nodes that are likely to move together
- A *scope* is defined such that each node would typically be within the scope of its landmark node
- Each node propagates *link state* information corresponding only to nodes within it *scope* and *distance-vector* information for all *landmark* nodes
  - Combination of link-state and distance-vector
  - Distance-vector used for landmark nodes outside the scope
  - No state information for non-landmark nodes outside scope maintained

LANMAR Routing to Nodes Within Scope

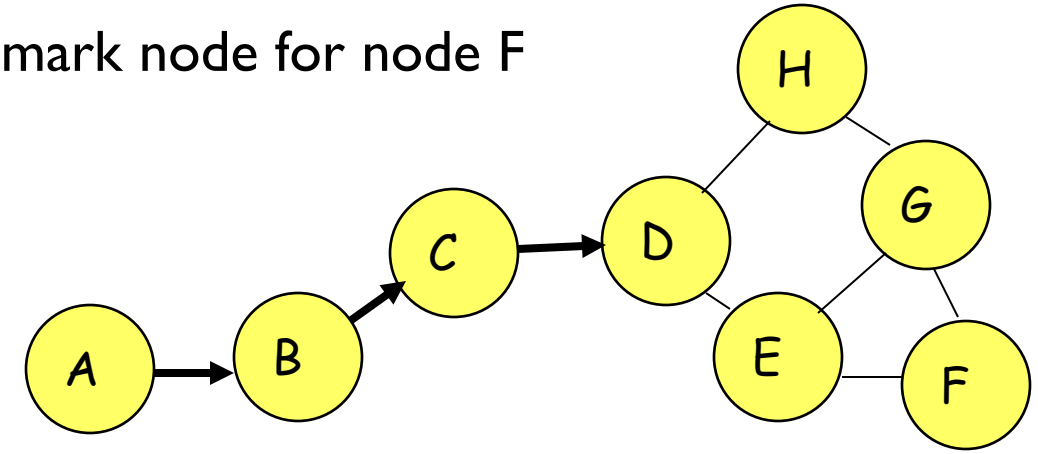
- Assume that node C is within scope of node A



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

LANMAR Routing to Nodes Outside Scope

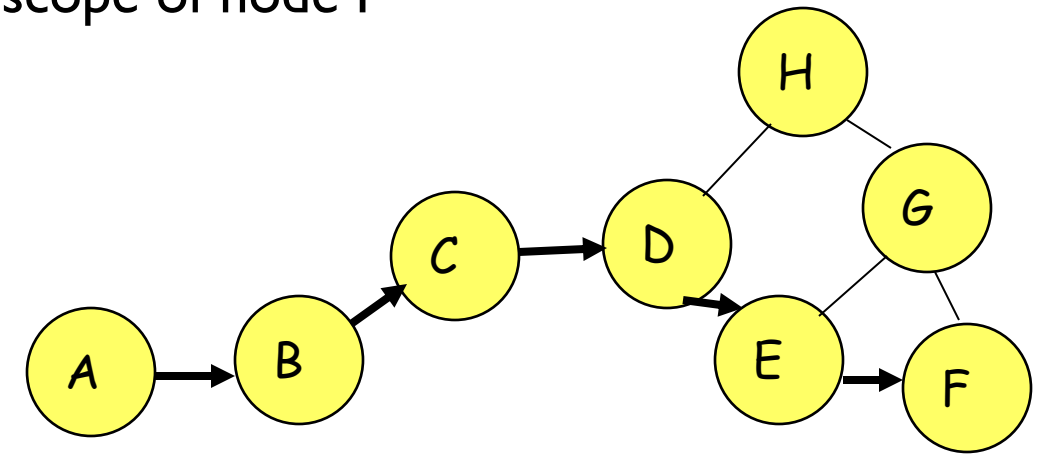
- Routing from node A to F which is outside A's scope
- Let H be the landmark node for node F



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

LANMAR Routing to Nodes Outside Scope

- Node D is within scope of node F



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

Outline

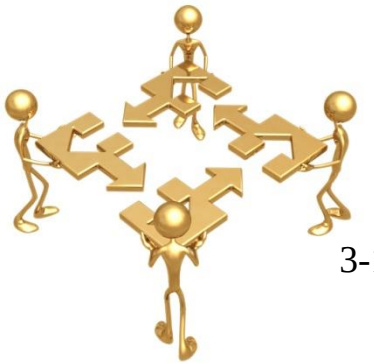
- Overview
- MAC
- Routing
- **Wireless in real world**
- Leverage broadcasting nature
- Explore the characteristic of wireless signal

Wireless in the Real World

- Real world deployment patterns
- Mesh networks and deployments

Wireless Challenges

- Force us to rethink many assumptions
- Need to share airwaves rather than wire
  - Don't know what hosts are involved
  - Host may not be using same link technology
- Mobility
- Other characteristics of wireless
  - Noisy → lots of losses
  - Slow
  - Interaction of multiple transmitters at receiver
    - Collisions, capture, interference
  - Multipath interference



Overview

- IEEE 802.11
  - Deployment patterns
  - Reaction to interference
  - Interference mitigation
- Mesh networks
  - Architecture
  - Measurements

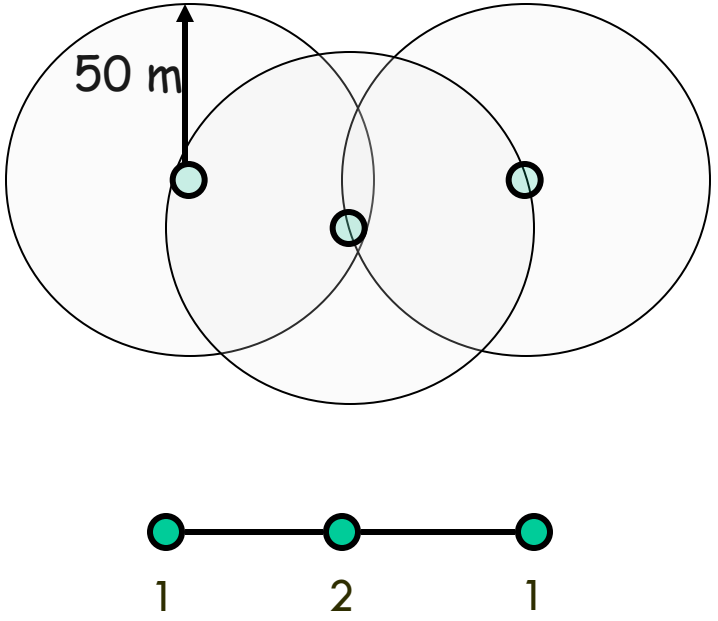
Characterizing Current Deployments

- Datasets
- Place Lab: 28,000 APs
  - MAC, ESSID, GPS
  - Selected US cities
  - www.placelab.org
- Wifimaps: 300,000 APs
  - MAC, ESSID, Channel, GPS (derived)
  - wifimaps.com
- Pittsburgh Wardrive: 667 APs
  - MAC, ESSID, Channel, Supported Rates, GPS

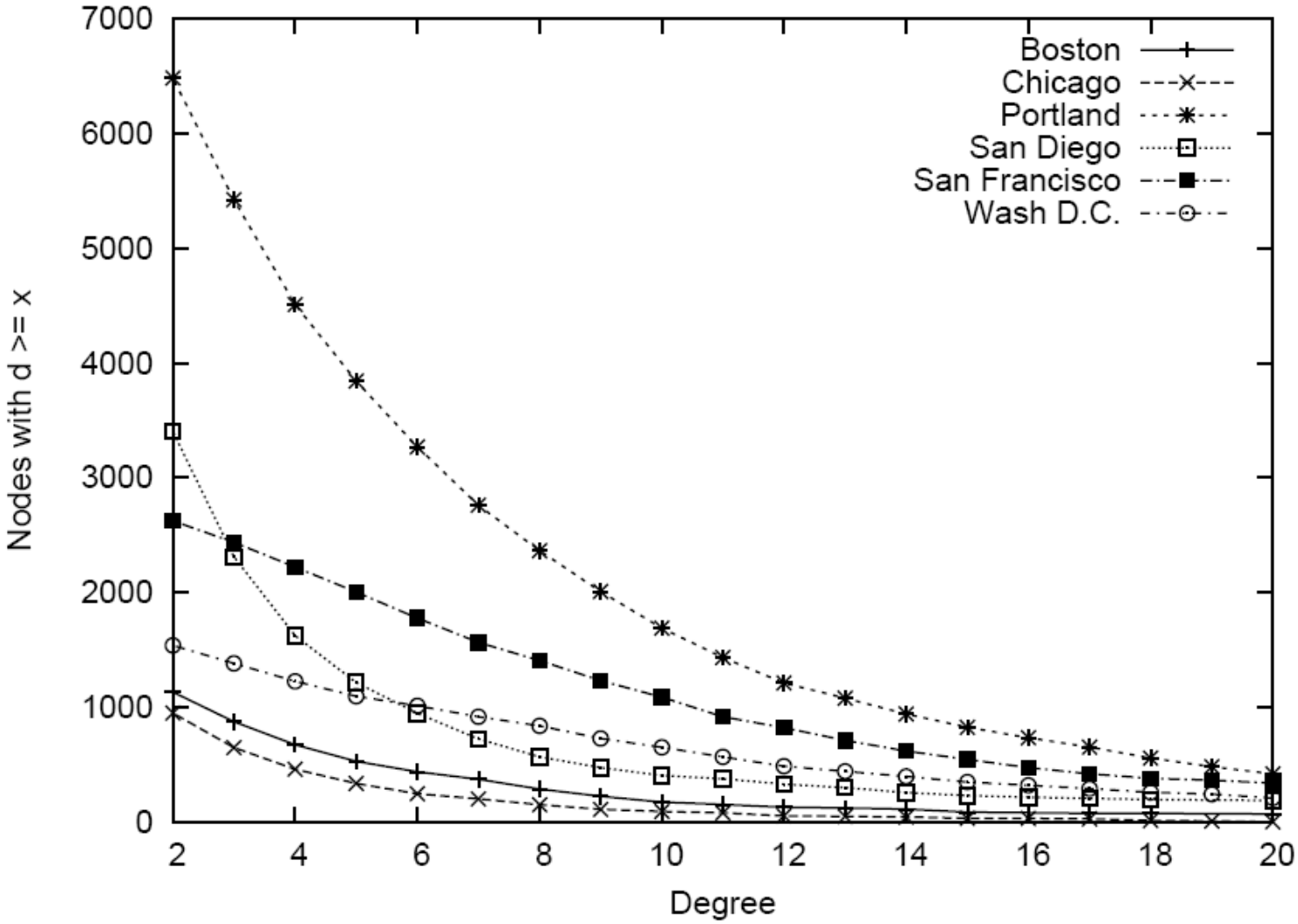
AP Stats, Degrees: Placelab

(Placelab: 28000 APs, MAC, ESSID, GPS)

	#APs	Max. degree (i.e., # neighbors)
Portland	8683	54
San Diego	7934	76
San Francisco	3037	85
Boston	2551	39



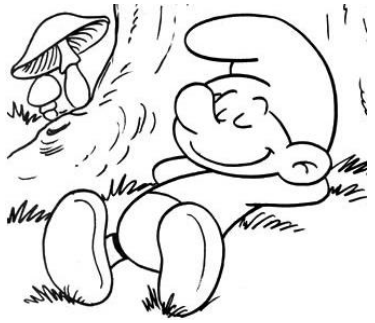
Degree Distribution: Place Lab



Unmanaged Devices

WifiMaps.com
(300,000 APs, MAC, ESSID, Channel)

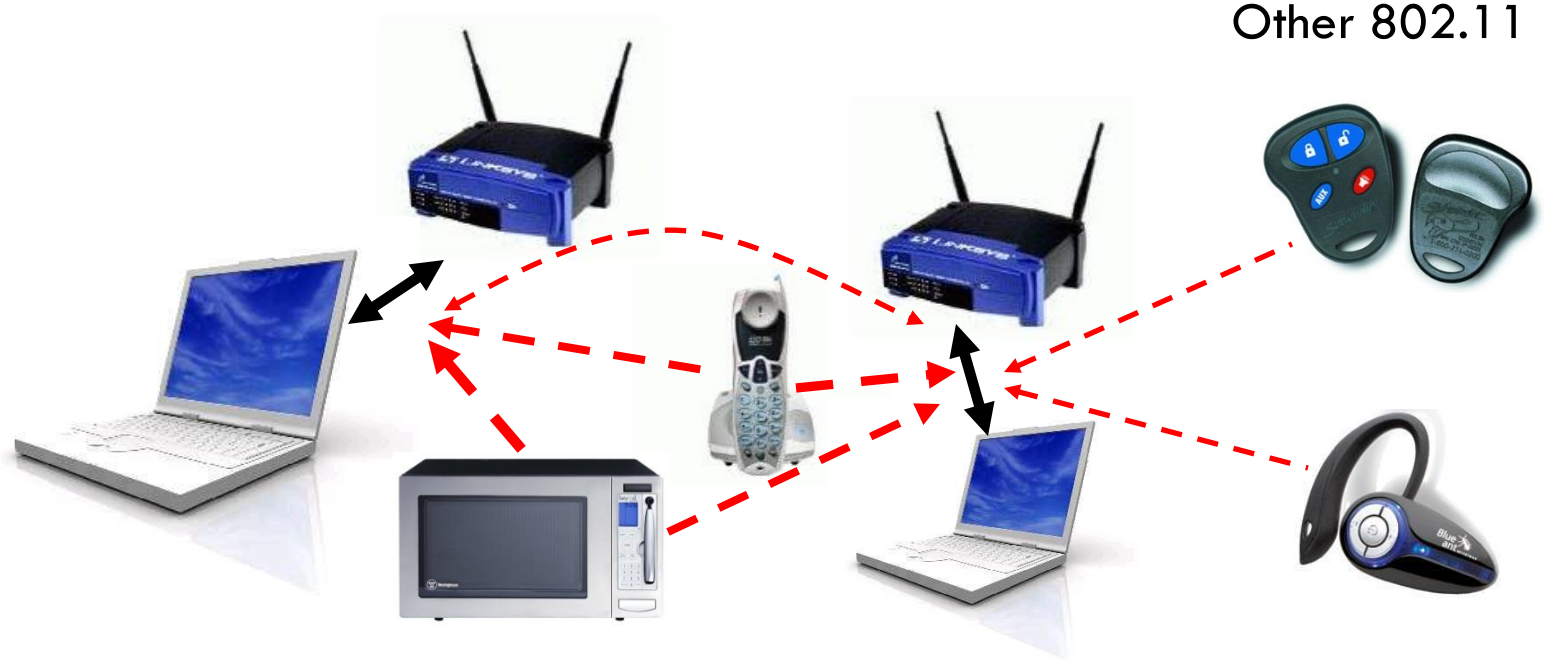
Channel	%age
6	51
11	21
1	14
10	4



- Most users don't change default channel
- Channel selection must be automated

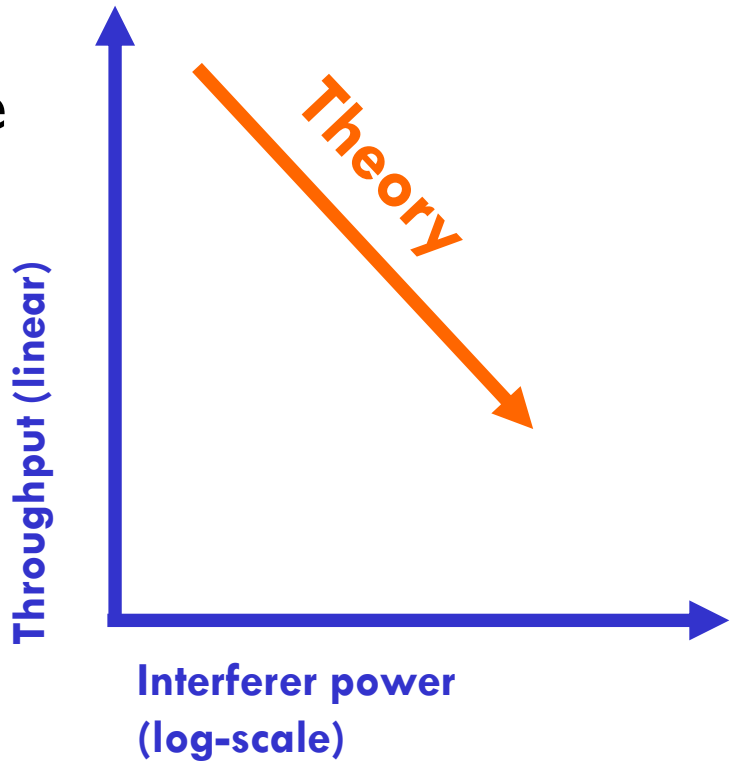
Growing Interference in Unlicensed Bands

- Anecdotal evidence of problems, but how severe?
- Characterize how IEEE 802.11 operates under interference in practice



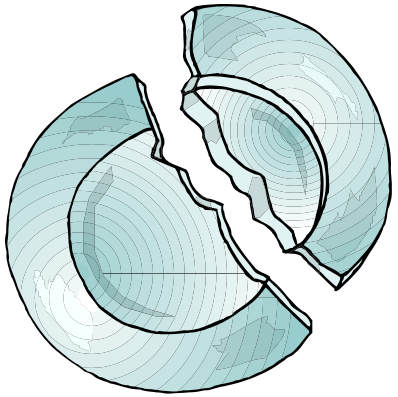
What do We Expect?

- Throughput to decrease linearly with interference
- There to be lots of options for 802.11 devices to tolerate interference
  - Bit-rate adaptation
  - Power control
  - FEC
  - Packet size variation
  - Spread-spectrum processing
  - Transmission and reception diversity



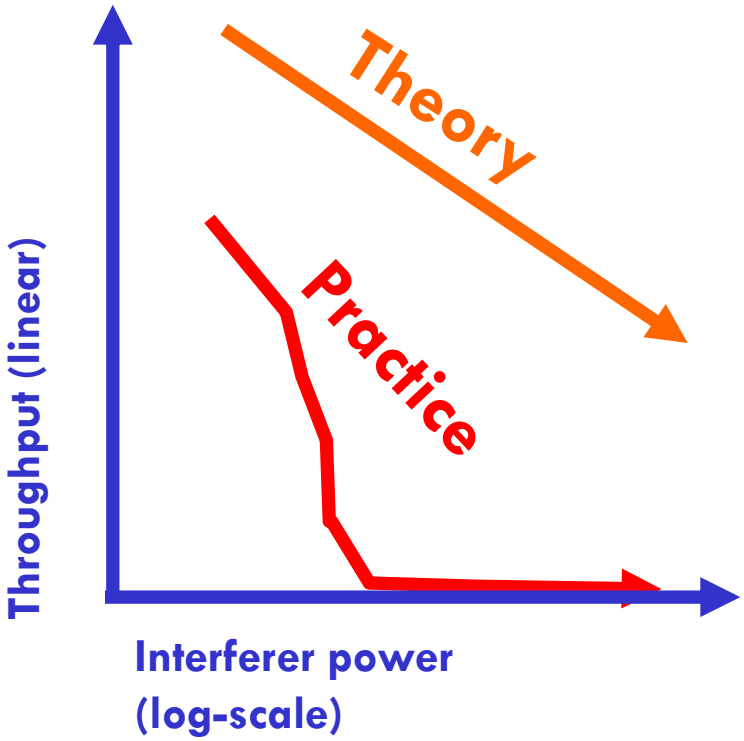
Key Questions

- How damaging can a low-power and/or narrow-band interferer be?
- How can today's hardware tolerate interference well?
  - What 802.11 options work well, and why?



What We See

- Effects of interference more severe in practice
- Caused by hardware limitations of commodity cards, which theory doesn't model



Experimental Setup

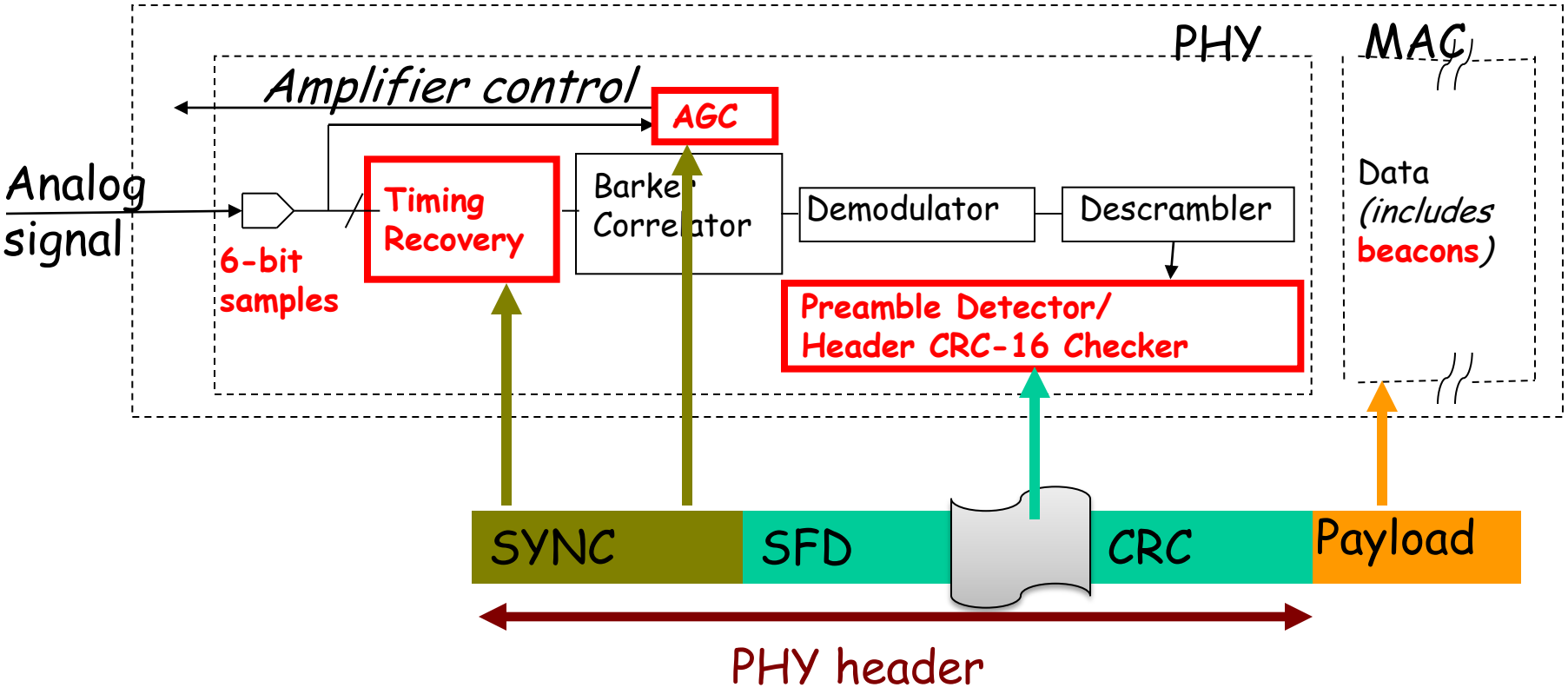
Access Point

UDP flow

802.11 Interferer

802.11 Client

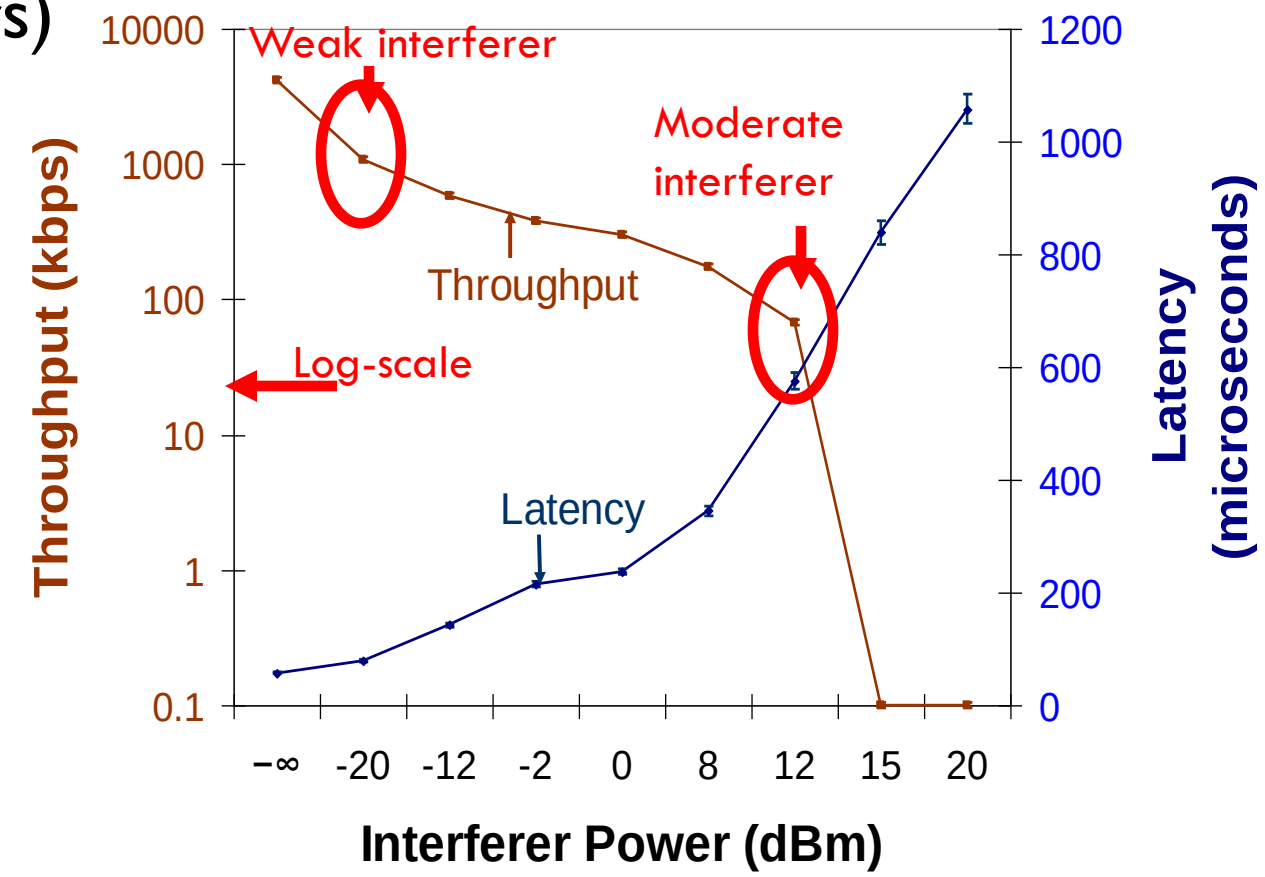
802.11 Receiver Path



- Extend SINR model to capture these vulnerabilities
- Interested in worst-case natural or adversarial interference
  - Have developed range of "attacks" that trigger these vulnerabilities

Timing Recovery Interference

- Interferer sends continuous SYNC pattern
- Interferes with packet acquisition (PHY reception errors)

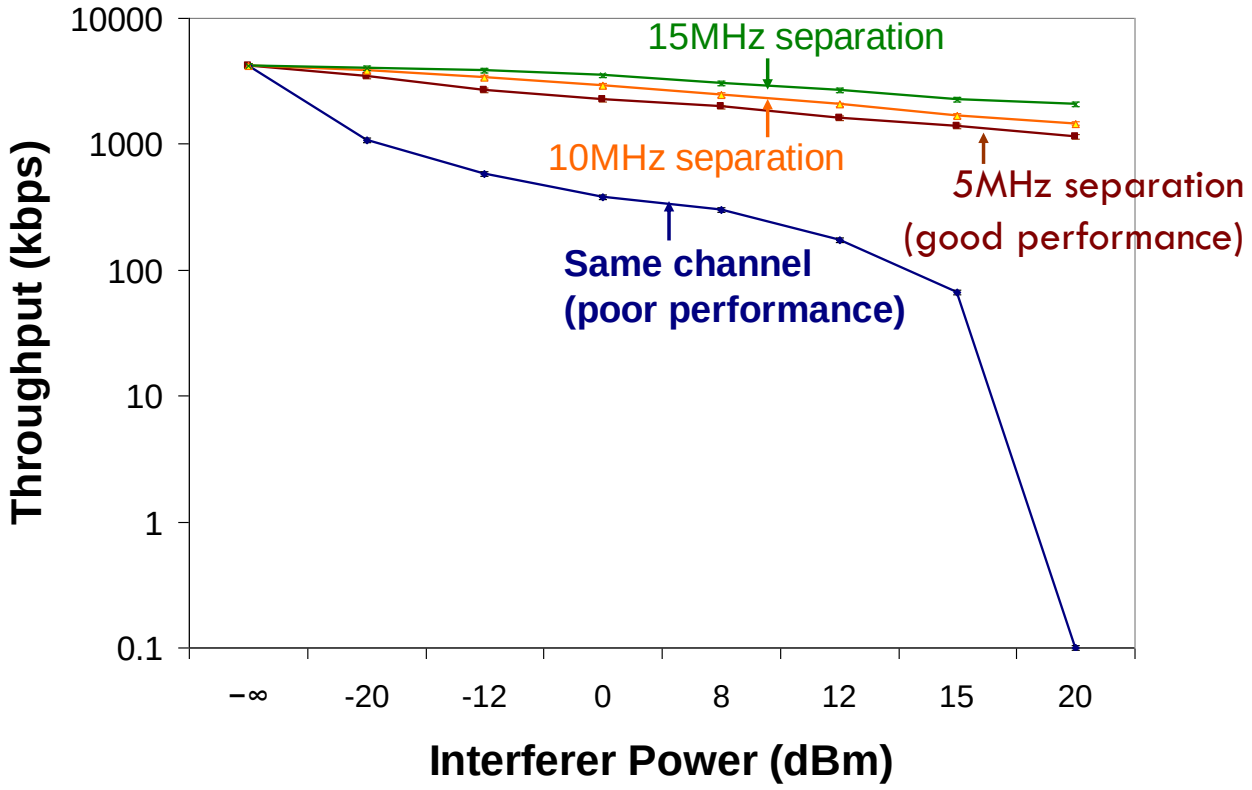


Interference Management

- Interference will get worse
  - Density/device diversity is increasing
  - Unlicensed spectrum is not keeping up
- Spectrum management
  - "Channel hopping" 802.11 effective at mitigating some performance problems [Sigcomm07]
  - Coordinated spectrum use – based on RF sensor network
- Transmission power control
  - Enable spatial reuse of spectrum by controlling transmit power
  - Must also adapt carrier sense behavior to take advantage

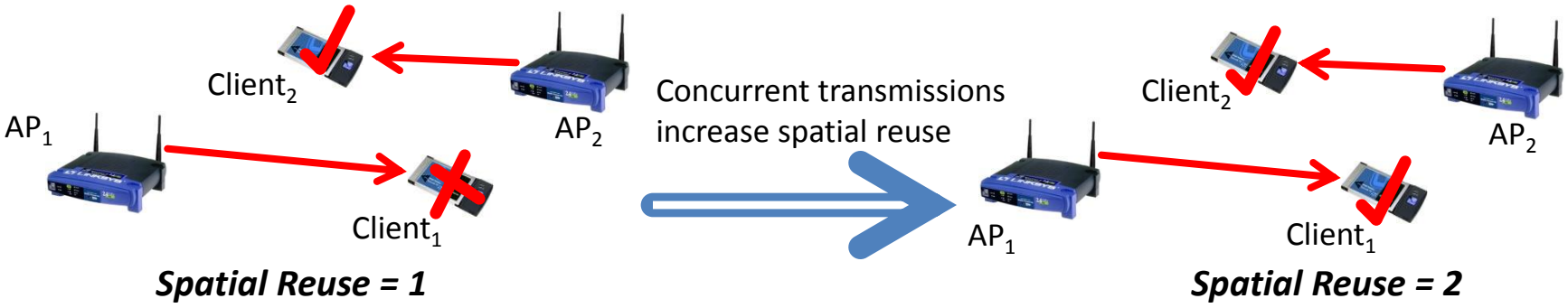
Impact of frequency separation

- Even small frequency separation (i.e., adjacent 802.11 channel) helps



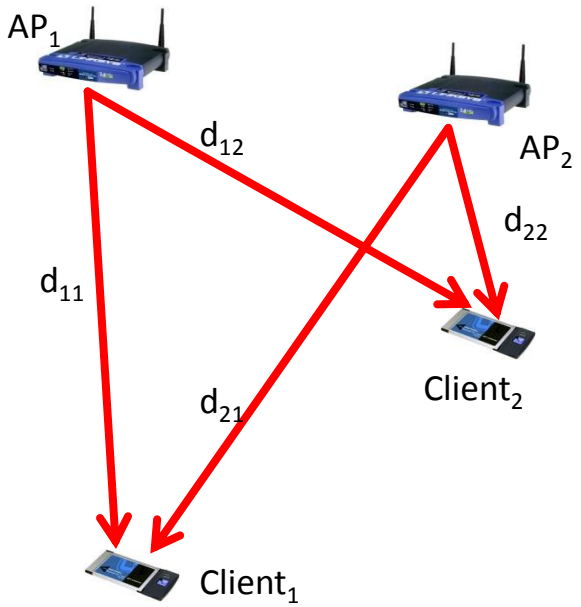
Transmission Power Control

- Choose transmit power levels to maximize *physical* spatial reuse
- Tune MAC to ensure nodes transmit simultaneously when possible
- Spatial reuse = network capacity / link capacity



Transmission Power Control in Practice

- For simple scenario → easy to compute optimal transmit power
  - May or may not enable simultaneous transmit
  - Protocol builds on iterative pair-wise optimization
- Adjusting transmit power → requires adjusting carrier sense thresholds
  - Echos, Alpha or eliminate carrier sense
  - Altrusitic Echos – eliminates starvation in Echos



Details of Power Control

- Hard to do per-packet with many NICs
  - Some even might have to re-init (many ms)
- May have to balance power with rate
  - Reasonable goal: lowest power for max rate
  - But finding ths empirically is hard! Many {power, rate} combinations, and not always easy to predict how each will perform
  - Alternate goal: lowest power for max *needed* rate
    - But this interacts with other people because you use more channel time to send the same data. Uh-oh.
    - Nice example of the difficulty of local vs. global optimization

Rate Adaptation

- General idea:
  - Observe channel conditions like SNR (signal-to-noise ratio), bit errors, packet errors
  - Pick a transmission rate that will get best goodput
    - There are channel conditions when reducing the bitrate can greatly increase throughput – e.g., if a $\frac{1}{2}$ decrease in bitrate gets you from 90% loss to 10% loss.

Simple Rate Adaptation Scheme

- Watch packet error rate over window (K packets or T seconds)
- If loss rate > $thresh_{high}$ (or SNR <, etc)
  - Reduce Tx rate
- If loss rate < $thresh_{low}$
  - Increase Tx rate
- Most devices support a discrete set of rates
  - 802.11 – 1, 2, 5.5, 11Mbps, etc.

Challenges in Rate Adaptation

- Channel conditions change over time
  - Loss rates must be measured over a window
- SNR estimates from the hardware are coarse, and don't always predict loss rate
- May be some overhead (time, transient interruptions, etc.) to changing rates

Power and Rate Selection Algorithms

- Rate Selection
  - Auto Rate Fallback: ARF
  - Estimated Rate Fallback: ERF

- Goal: Transmit at minimum necessary power to reach receiver
  - Minimizes interference with other nodes
  - Paper: Can double or more capacity, *if done right*.

- Joint Power and Rate Selection
  - Power Auto Rate Fallback: PARF
  - Power Estimated Rate Fallback: PERF
  - Conservative Algorithms
    - Always attempt to achieve highest possible modulation rate

Power Control/Rate Control Summary

- Complex interactions….
  - More power:
    - Higher received signal strength
    - May enable faster rate (more S in S/N)
      - May mean you occupy media for less time
    - Interferes with more people
  - Less power
    - Interfere with fewer people
  - Less power + less rate
    - Fewer people but for a longer time

- Gets even harder once you consider
  - Carrier sense
  - Calibration and measurement error
  - Mobility

Overview

- 802.11
  - Deployment patterns
  - Reaction to interference
  - Interference mitigation
- Mesh networks
  - Architecture
  - Measurements

Community Wireless Network

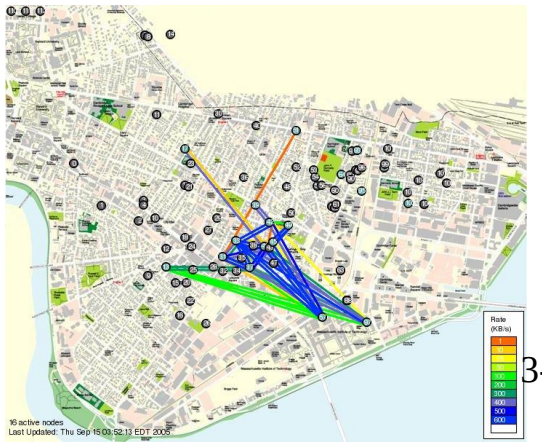
- Share a few wired Internet connections
- Construction of community networks
  - Multi-hop network
    - Nodes in chosen locations
    - Directional antennas
    - Require well-coordination
  - Access point
    - Clients directly connect
    - Access points operates independe
    - Do not require much coordinatio

Roofnet

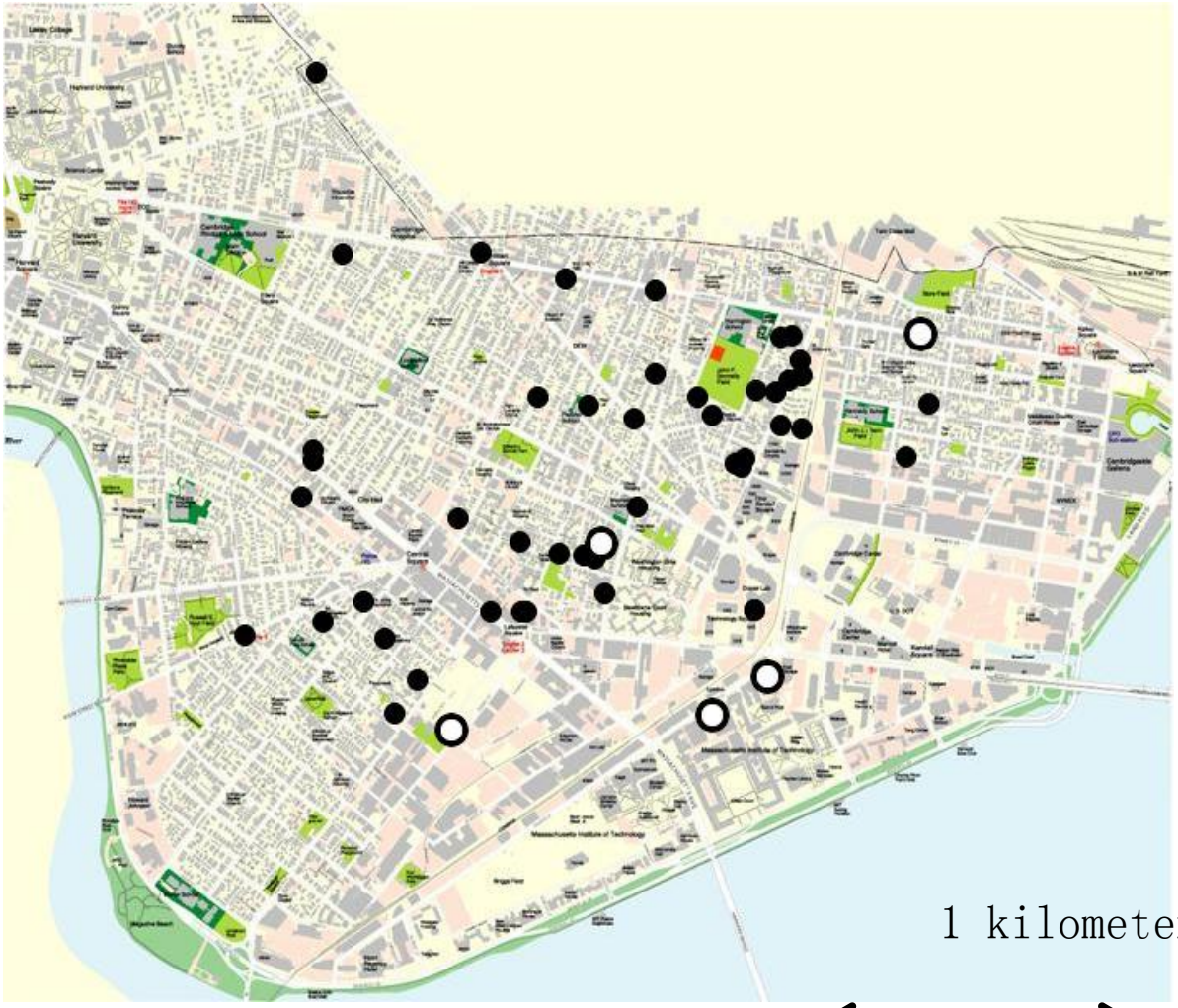
- Goals
  - Operate without extensive planning or central management
  - Provide wide coverage and acceptable performance
- Design decisions
  - Unconstrained node placement
  - Omni-directional antennas
  - Multi-hop routing
  - Optimization of routing for throughput in a slowly changing network

Roofnet Design

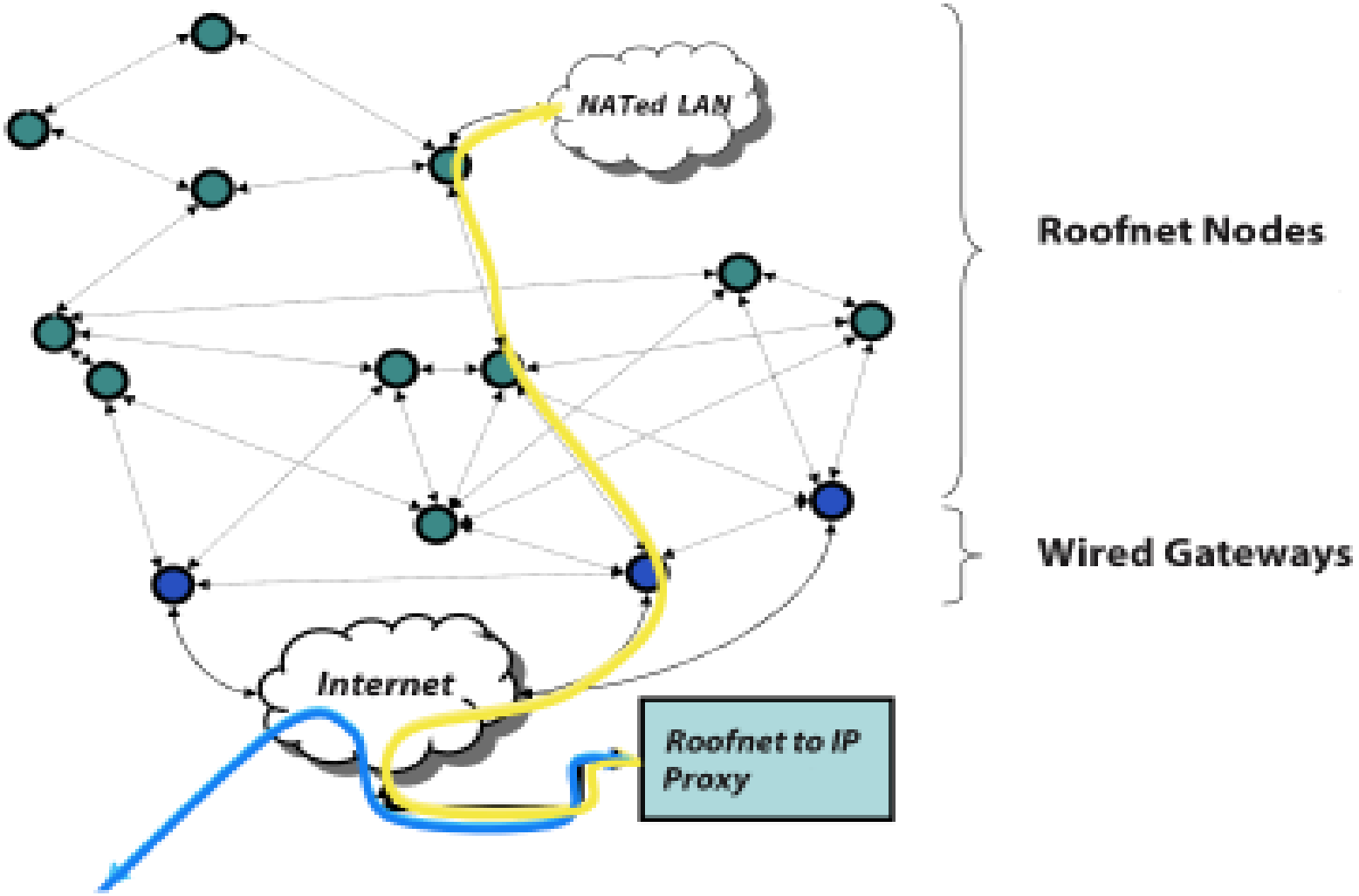
- Deployment
  - Over an area of about four square kilometers in Cambridge, Messachusetts
  - Most nodes are located in buildings
    - 3~4 story apartment buildings
    - 8 nodes are in taller buildings
  - Each Rooftnet node is hosted by a volunteer user
- Hardware
  - PC, omni-directional antenna, hard drive …
  - 802.11b card
    - RTS/CTS disabled
    - Share the same 802.11b channel
    - Non-standard "pseudo-IBSS" mode
      Similar to standard 802.11b IBSS (ad hoc)
      Omit beacon and BSSID (network ID)



Roofnet Node Map



Roofnet


NATed LAN
Roofnet Nodes
Wired Gateways
Internet
Roofnet to IP Proxy

Typical Rooftop View

A Roofnet Self-Installation Kit

Antenna ($65)
8dBi, 20 degree vertical

Computer ($340)
533 MHz PC, hard disk, CDROM

802.11b card ($155)
Engenius Prism 2.5, 200mW

50 ft. Cable ($40)
Low loss (3dB/100ft)

Miscellaneous ($75)
Chimney Mount, Lightning Arrestor, etc.

Software ("free")
Our networking software based on Click

Total: $685

Takes a user about 45 minutes to install on a flat roof

Software and Auto-Configuration

- Linux, routing software, DHCP server, web server …
- Automatically solve a number of problems
  - Allocating addresses
  - Finding a gateway between Roofnet and the Internet
  - Choosing a good multi-hop route to that gateway
- Addressing
  - Roofnet carries IP packets inside its own header format and routing protocol
  - Assign addresses automatically
  - Only meaningful inside Roofnet, not globally routable
  - The address of Roofnet nodes
    - Low 24 bits are the low 24 bits of the node's Ethernet address
    - High 8 bits are an unused class-A IP address block
  - The address of hosts
    - Allocate 192.168.1.x via DHCP and use NAT between the Ethernet and Roofnet

Software and Auto-Configuration

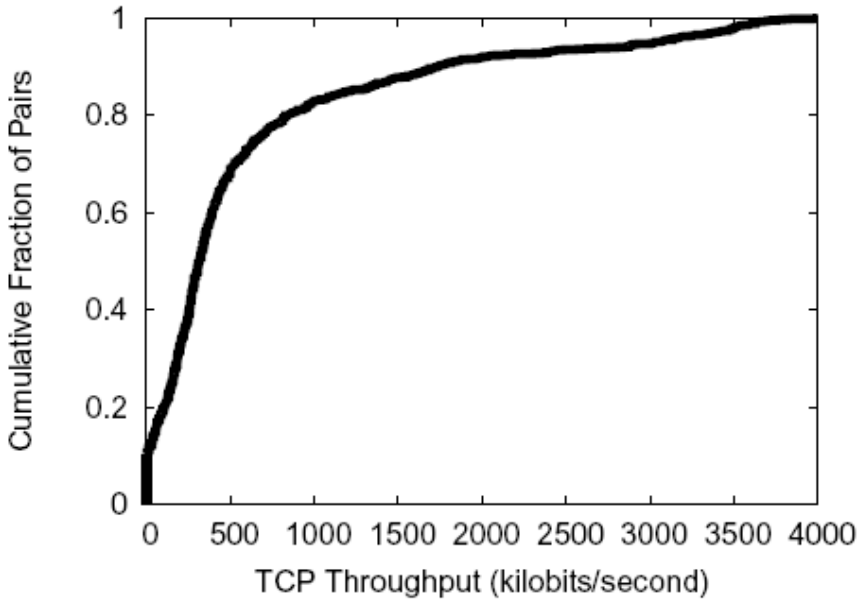
- Gateway and Internet Access
  - A small fraction of Roofnet users will share their wired Internet access links
  - Nodes which can reach the Internet
    - Advertise itself to Roofnet as an Internet gateway
    - Acts as a NAT for connection from Roofnet to the Internet
  - Other nodes
    - Select the gateway which has the best route metric
  - Roofnet currently has four Internet gateways

Evaluation

- Method
  - Multi-hop TCP
    - 15 second one-way bulk TCP transfer between each pair of Roofnet nodes
  - Single-hop TCP
    - The direct radio link between each pair of routes
  - Loss matrix
    - The loss rate between each pair of nodes using 1500-byte broadcasts
  - Multi-hop density
    - TCP throughput between a fixed set of four nodes
    - Varying the number of Roofnet nodes that are participating in routing

Evaluation

- Basic Performance (Multi-hop TCP)
  - The routes with low hop-count have much higher throughput
  - Multi-hop routes suffer from inter-hop collisions



Hops	Number of Pairs	Throughput (kbits/sec)	Latency (ms)
1	158	2451	4
2	303	771	26
3	301	362	45
4	223	266	50
5	120	210	60
6	43	272	100
7	33	181	83
8	14	159	119
9	4	175	182
10	1	182	218
no route	132	0	–
Avg: 2.9	Total: 1332	Avg: 627	Avg: 39

Evaluation

- Basic Performance (Multi-hop TCP)
  - TCP throughput to each node from its chosen gateway
  - Round-trip latencies for 84-byte ping packets to estimate interactive delay

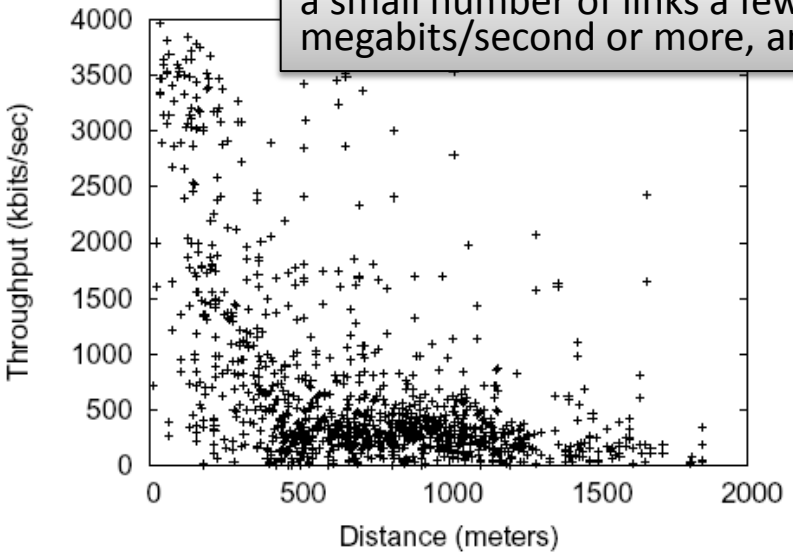
Hops	Number of nodes	Throughput (kbits/sec)	Latency (ms)
1	12	2752	9
2	8	940	19
3	5	552	27
4	7	379	43
5	1	89	37
Avg: 2.3	Total: 33	Avg: 1395	Avg: 22

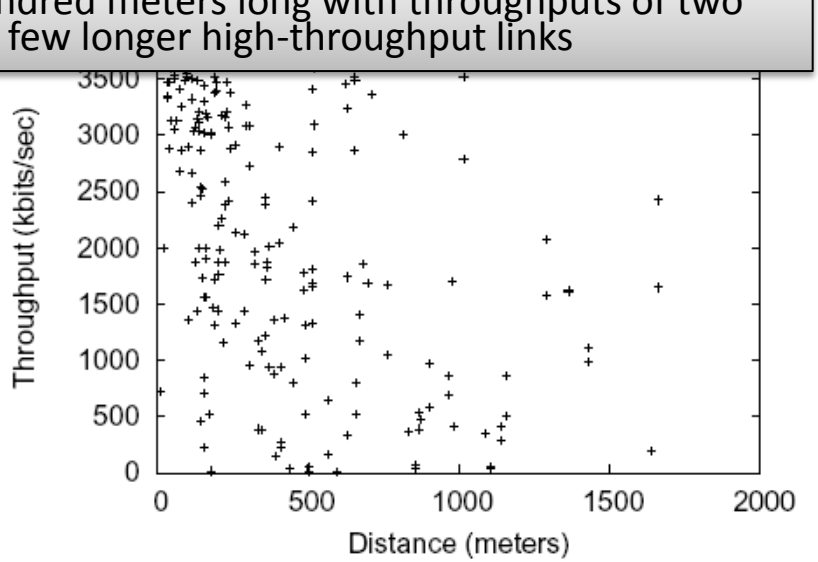
No problem in interactive sessions

Evaluation

- Link Quality and Distance (Single-hop TCP, Multi-hop TCP)
  - Most available links are between 500m and 1300m and 500 kbits/s (most cases)
  - Srcr
    - Use almost all of the links faster than 2 Mbits/s and ignore majority of the links which are slower than that
    - Fast short hops are the best policy

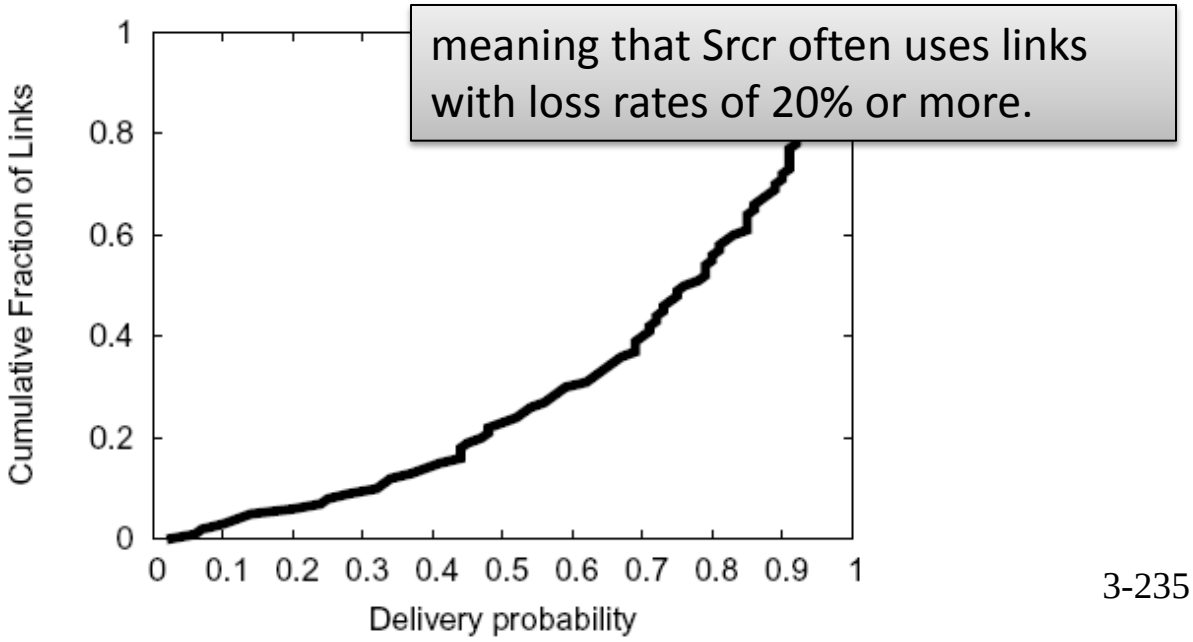
a small number of links a few hundred meters long with throughputs of two megabits/second or more, and a few longer high-throughput links





Evaluation

- Link Quality and Distance (Multi-hop TCP, Loss matrix)
  - Median delivery probability is 0.8
  - 1/4 links have loss rates of 50% or more
  - 802.11 detects the losses with its ACK mechanism and resends the packets



Evaluation

Comparison against communication over a direct radio link to a gateway (Access-point Network)

- Architectural Alternatives
  - Maximize the number of additional nodes with non-zero throughput to some gateway
  - Ties are broken by average throughput

For small numbers of gateways, multi-hop routing improves both connectivity and throughput.

3	37	1871	34	1102
4	37	2131	36	1140
5	37	2355	37	1364
6	37	2450	37	2123
7	37	2529	37	2312
8	37	2614	37	2475
9	37	2702	37	2564
10	37	2795	37	2659
⋮	⋮	⋮	⋮	⋮
15	37	3197	37	3180
20	37	3508	37	3476
25	37	3721	37	3658

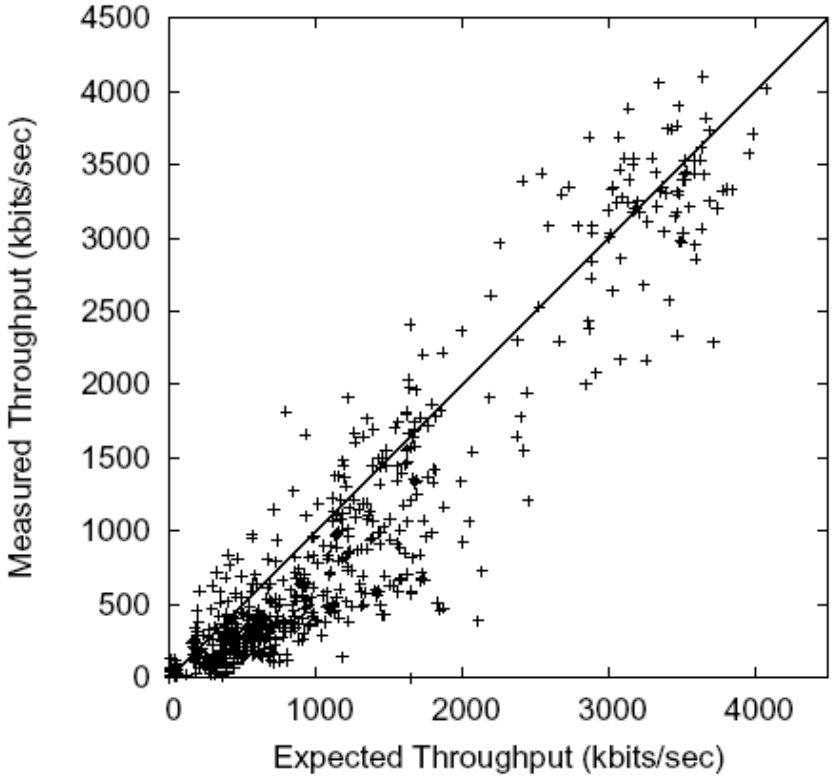
Comparison of multi-hop and single-hop architectures, with "optimal" choice of gateways.

	Multi-Hop		Single-Hop	
GWs	Conn	Throughput (kbits/sec)	Conn	Throughput (kbits/sec)
1	34	760	10	535
2	35	1051	17	585
3	35	1485	22	900
4	35	2021	25	1260
5	36	1565	28	1221
6	36	1954	30	1192
7	36	1931	31	1662
8	37	1447	32	1579
9	37	1700	33	1627
10	37	1945	34	1689
⋮	⋮	⋮	⋮	⋮
15	37	2305	36	1714
20	37	2509	36	2695
25	37	2703	37	2317

Comparison of multi-hop and single-hop architectures with random gateway choice.

Evaluation

- Inter-hop Interference (Multi-hop TCP, Single-hop TCP)
  - Concurrent transmissions on different hops of a route collide and cause packet loss



The expected multi-hop throughputs are mostly higher than the measured throughputs.

Roofnet Summary

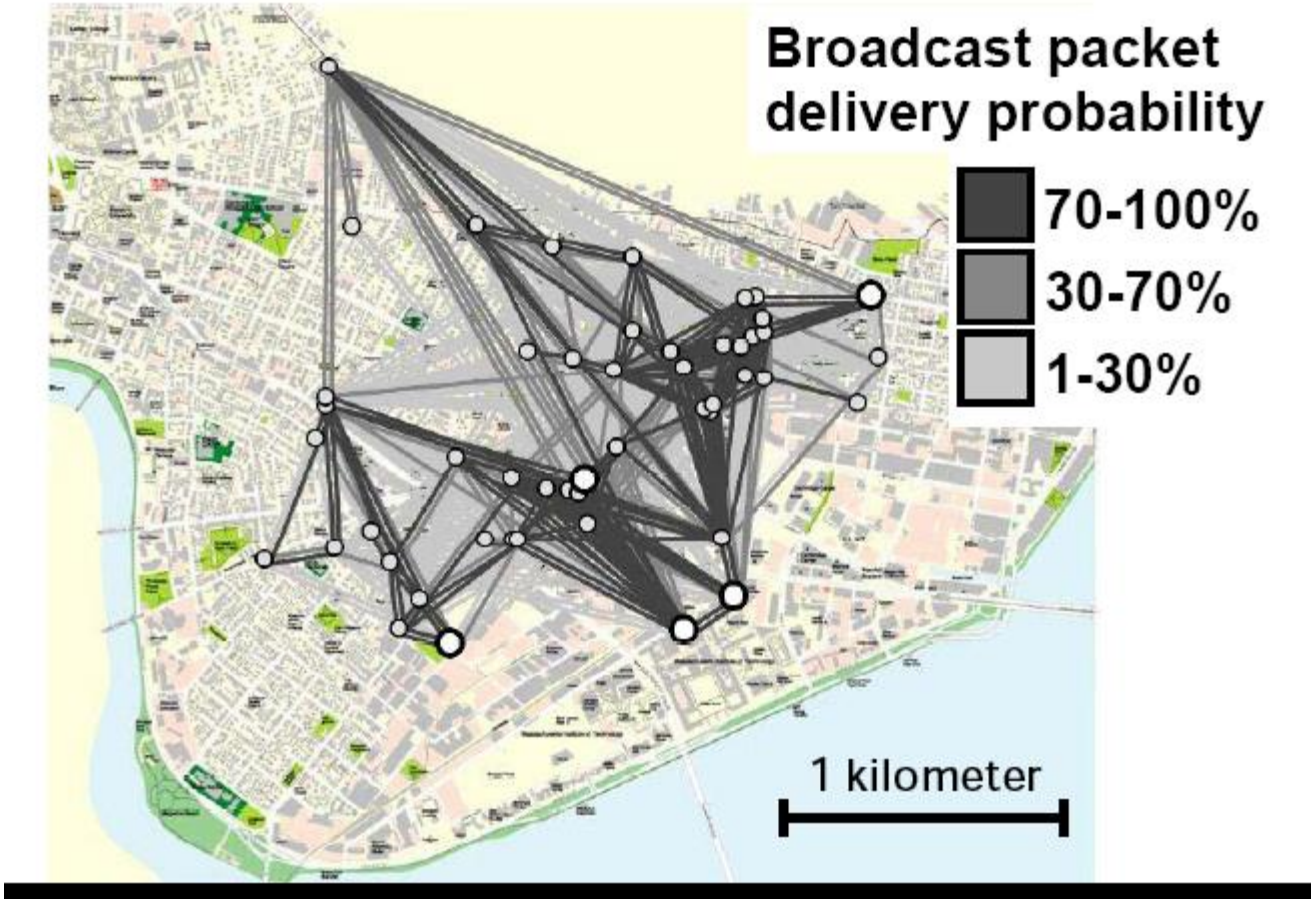
- The network's architectures favors
  - Ease of deployment
  - Omni-directional antennas
  - Self-configuring software
  - Link-quality-aware multi-hop routing
- Evaluation of network performance
  - Average throughput between nodes is 627kbits/s
  - Well served by just a few gateways whose position is determined by convenience
  - Multi-hop mesh increases both connectivity and throughput

Roofnet Link Level Measurements

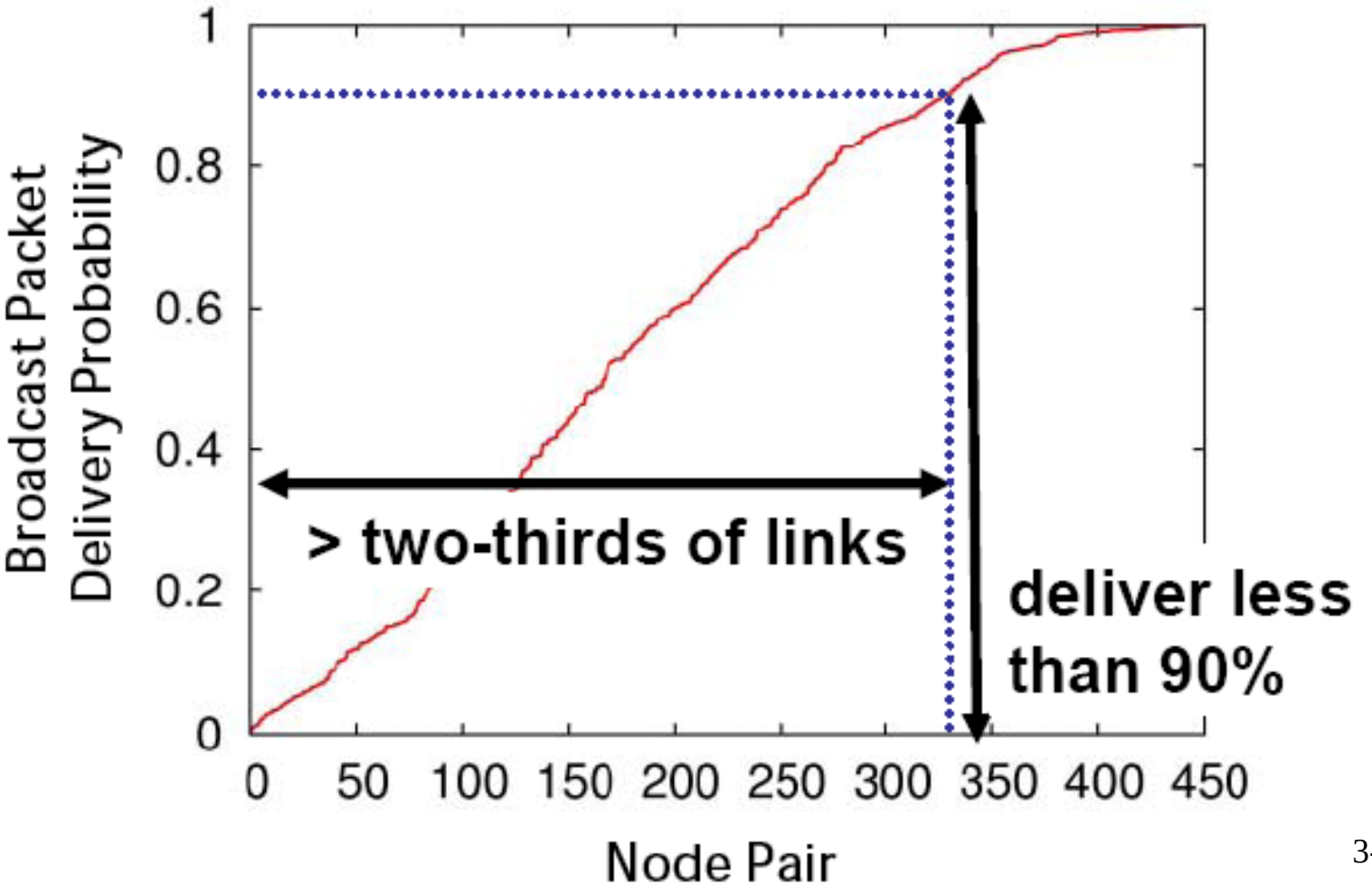
- Analyze cause of packet loss
- Neighbor Abstraction
  - Ability to hear control packets or No Interference
  - Strong correlation between BER and S/N
- RoofNet pairs communicate
  - At intermediate loss rates
  - Temporal Variation
  - Spatial Variation

neighbor abstraction is a poor approximation of reality

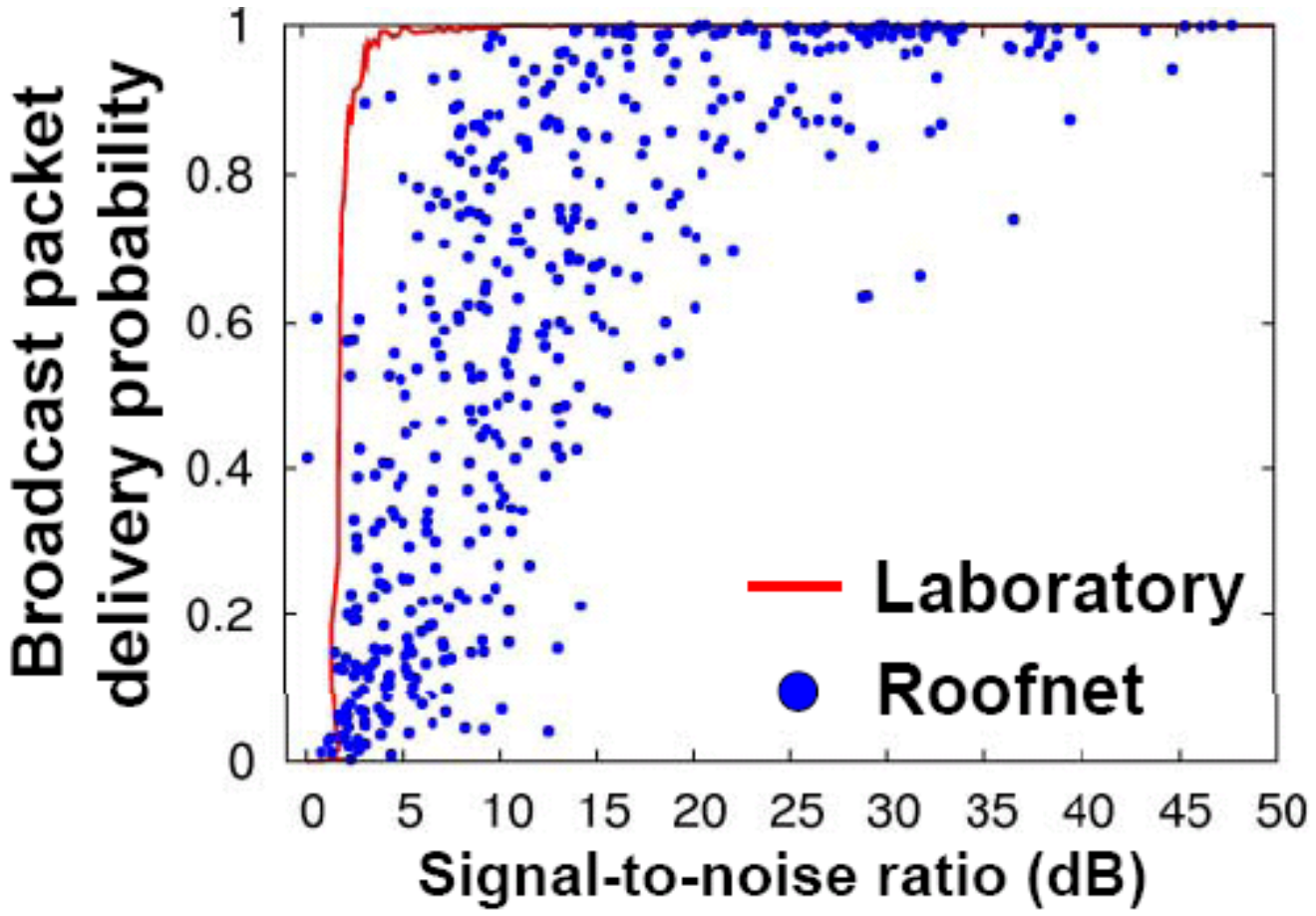
Lossy Links are Common



Delivery Probabilities are Uniformly Distributed



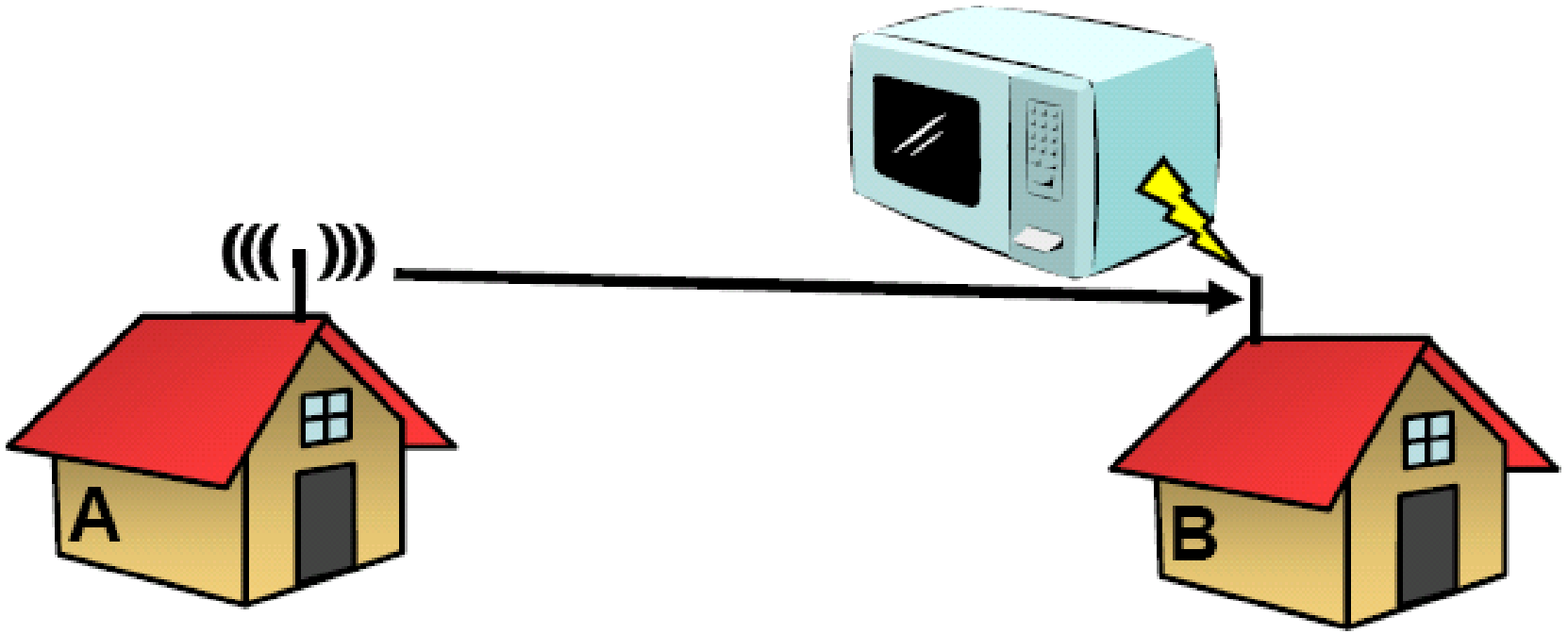
Delivery vs. SNR



- SNR not a good predictor

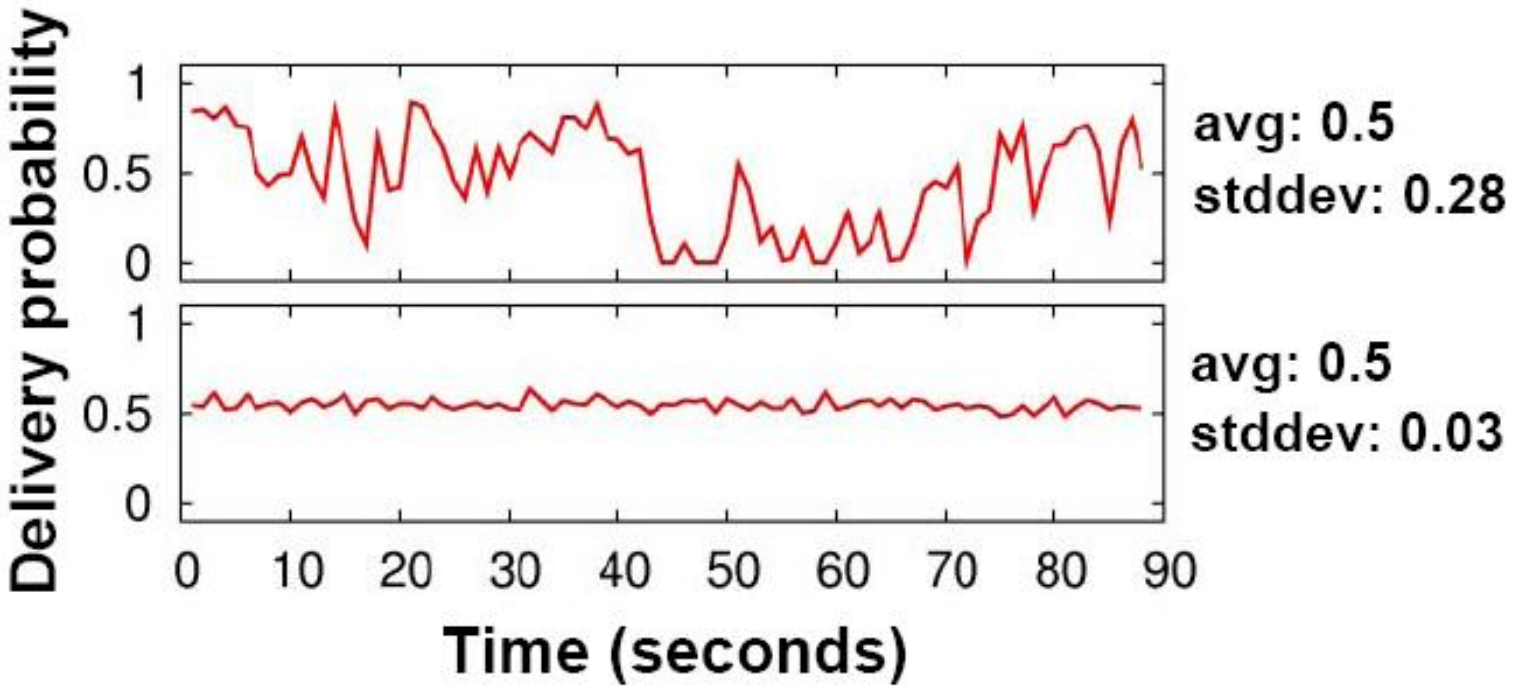
Is it Bursty Interference?

- May interfere but not impact SNR measurement

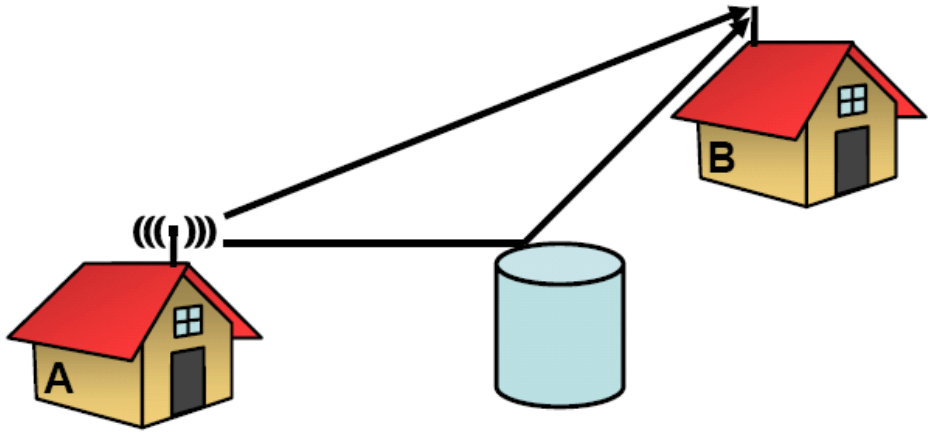


Two Different Roofnet Links

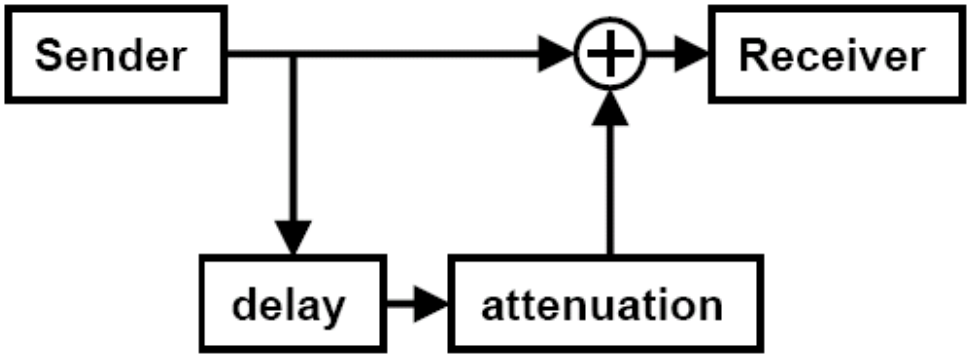
- Top is typical of bursty interference, bottom is not
- Most links are like the bottom



Is it Multipath Interference?

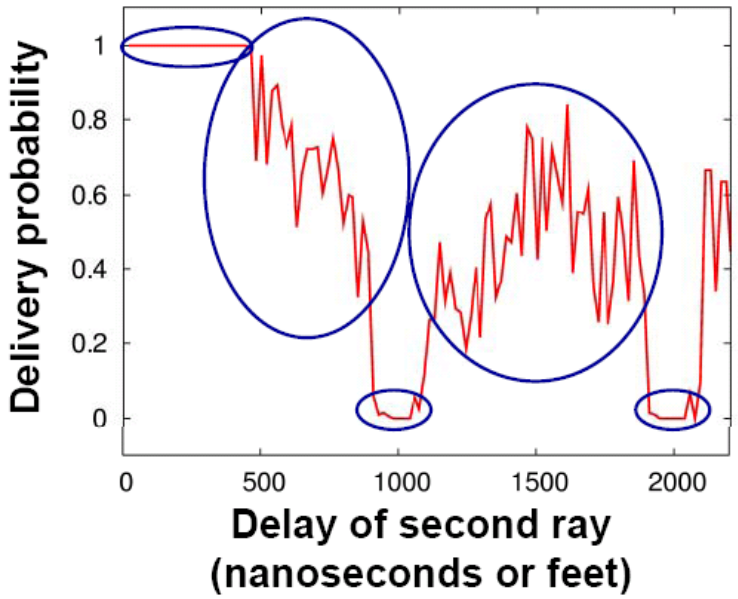


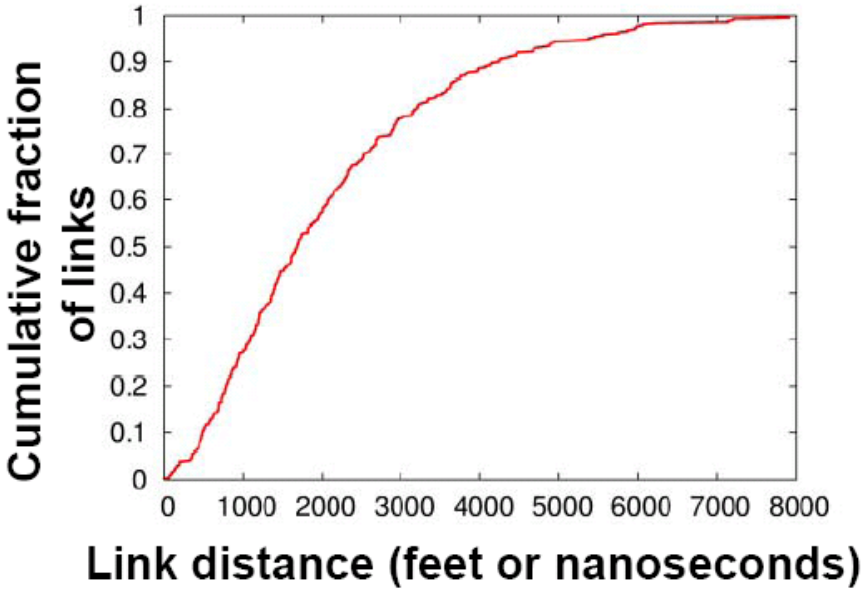
- Simulate with channel emulator



A Plausible Explanation

- Multi-path can produce intermediate loss rates
- Appropriate multi-path delay is possible due to long-links





Key Implications

- Lack of a link abstraction!
  - Links aren't on or off… sometimes in-between
- Protocols must take advantage of these intermediate quality links to perform well
- How unique is this to Roofnet?
  - Cards designed for indoor environments used outdoors

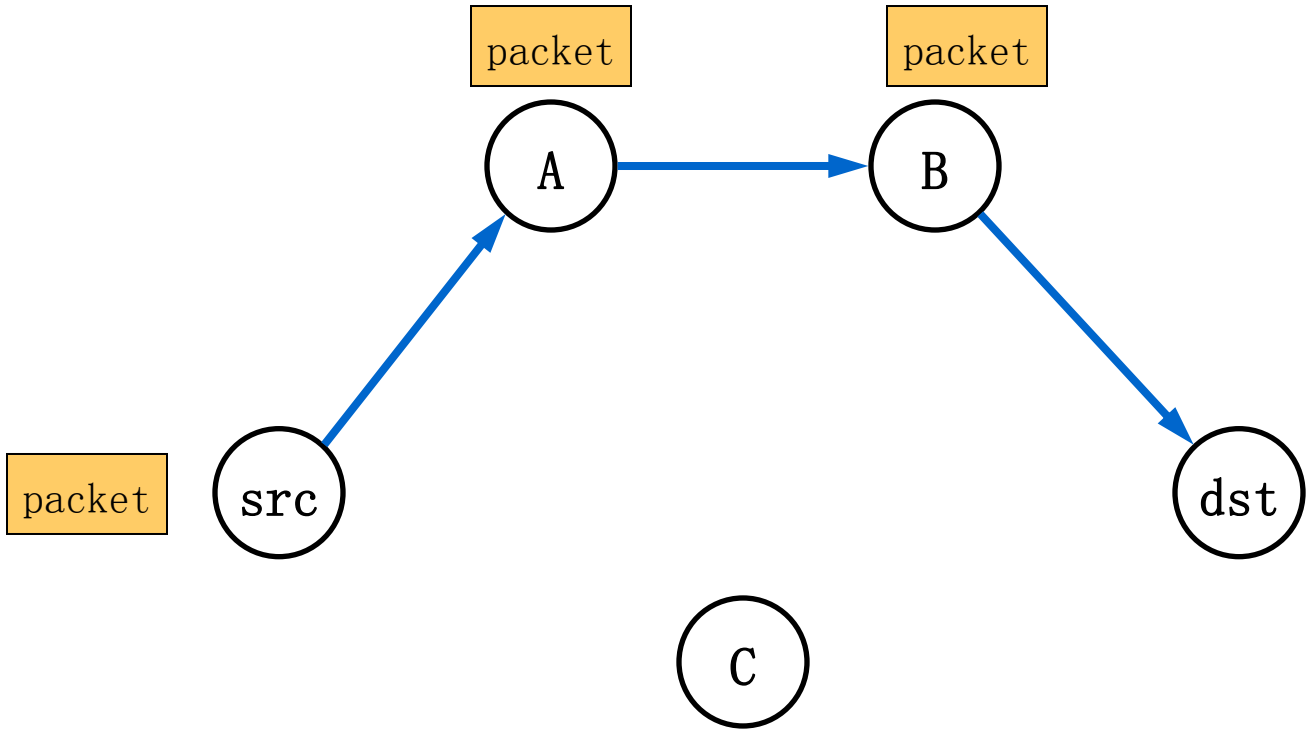
Outline

- Overview
- MAC
- Routing
- Wireless in real world
- **Leverage broadcasting nature**
- Explore the characteristic of wireless signal

Taking Advantage of Broadcast

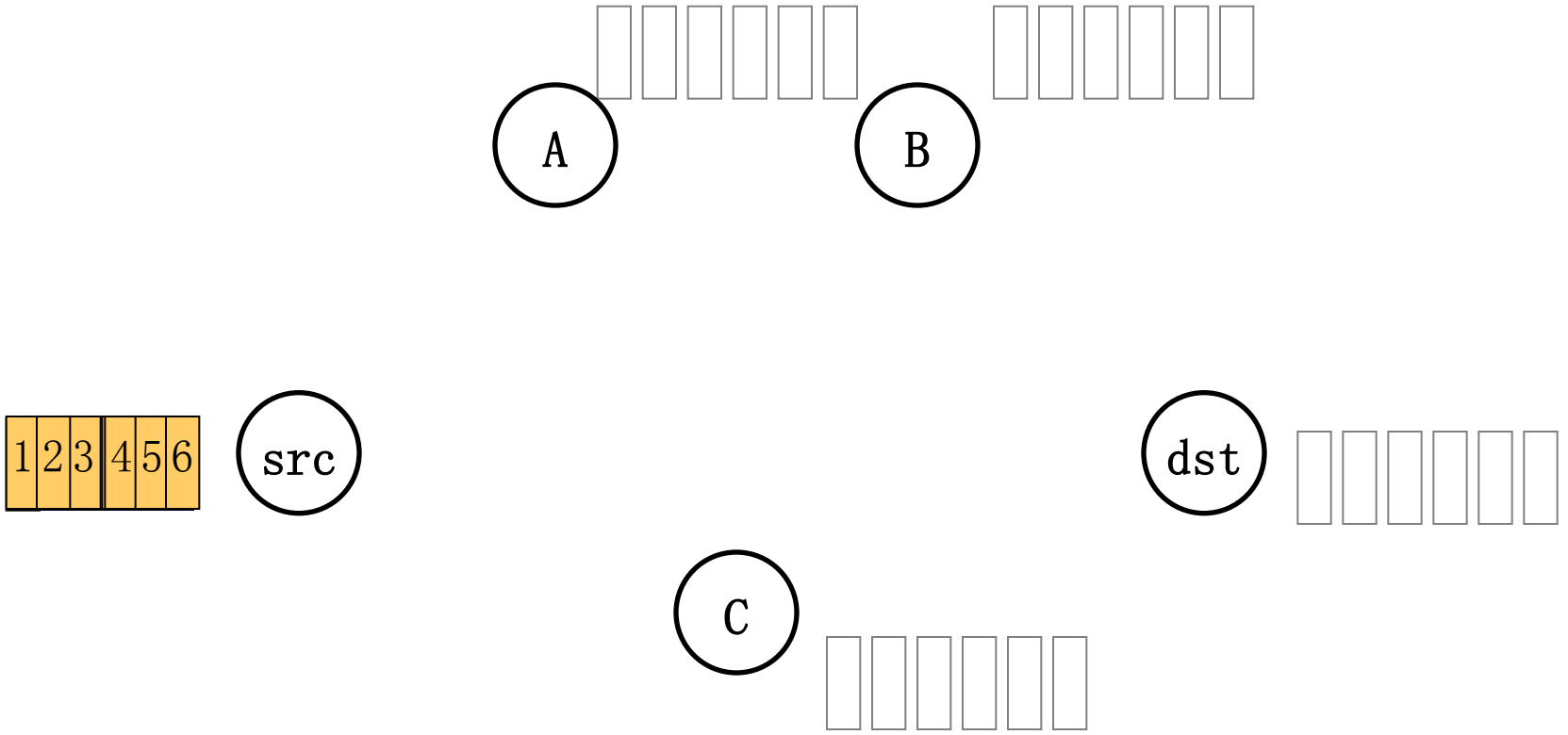
- Opportunistic forwarding (ExOR)
- Network coding (COPE)

Initial Approach: Traditional Routing



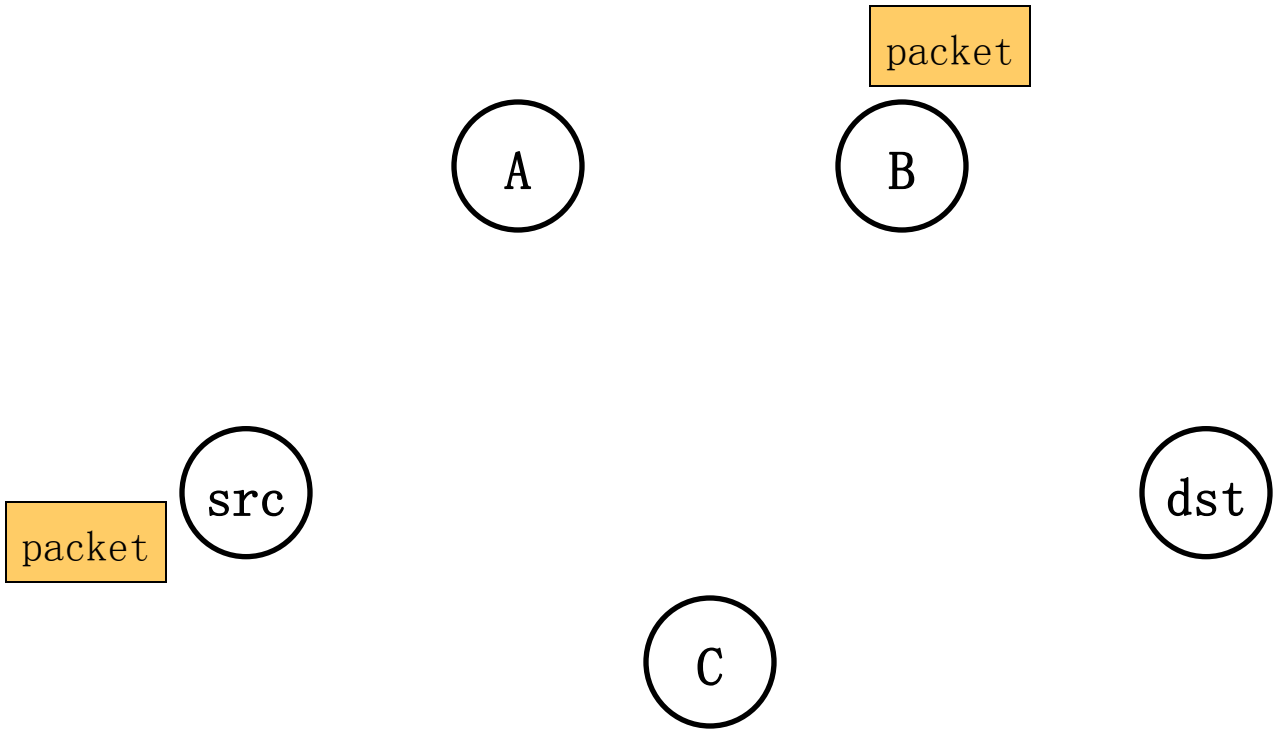
- Identify a route, forward over links
- Abstract radio to look like a wired link

Radios Aren't Wires



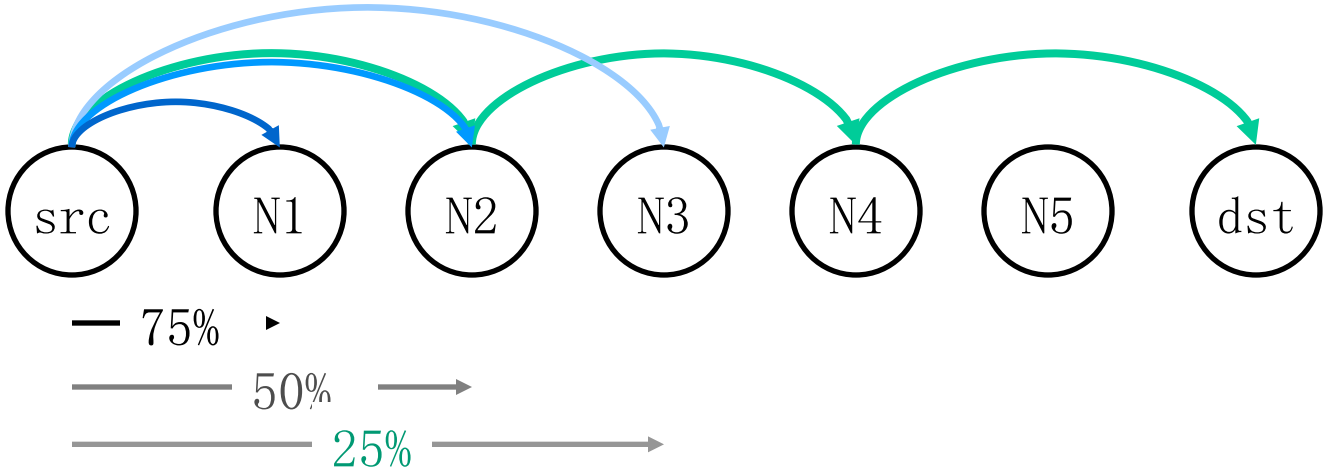
- Every packet is broadcast
- Reception is probabilistic

Exploiting Probabilistic Broadcast



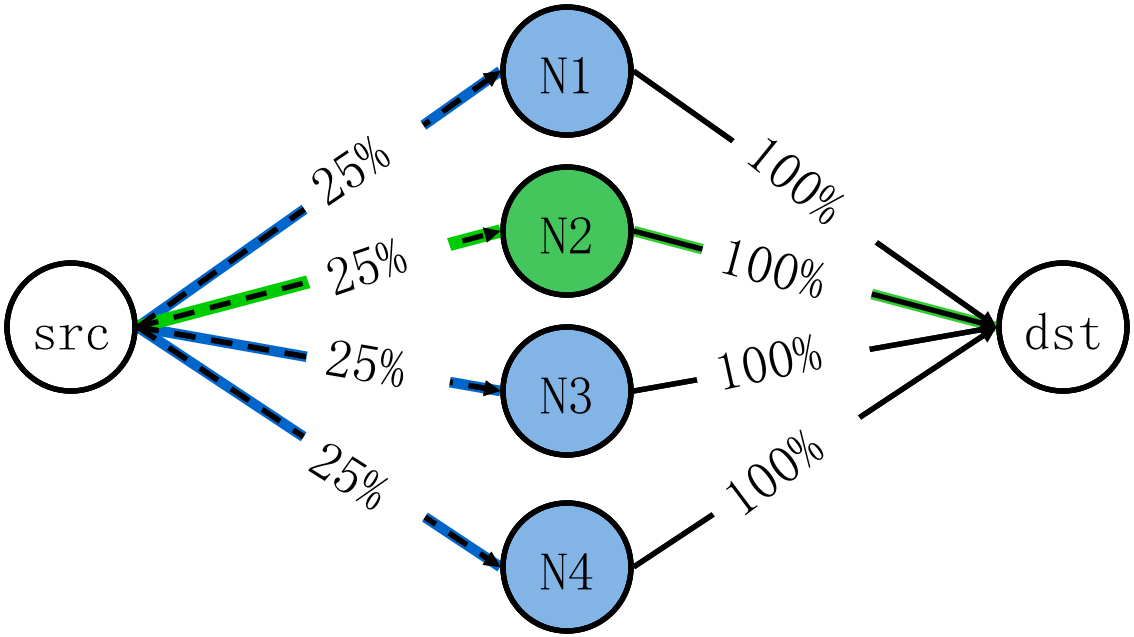
- Decide who forwards after reception
- Goal: only closest receiver should forward
- Challenge: agree efficiently and avoid duplicate transmissions

Why ExOR Might Increase Throughput



- Best traditional route over 50% hops: $3(1/0.5) = 6$ tx
- Throughput $\cong 1/\#\text{ transmissions}$
- ExOR exploits lucky long receptions: 4 transmissions
- Assumes probability falls off gradually with distance

Why ExOR Might Increase Throughput

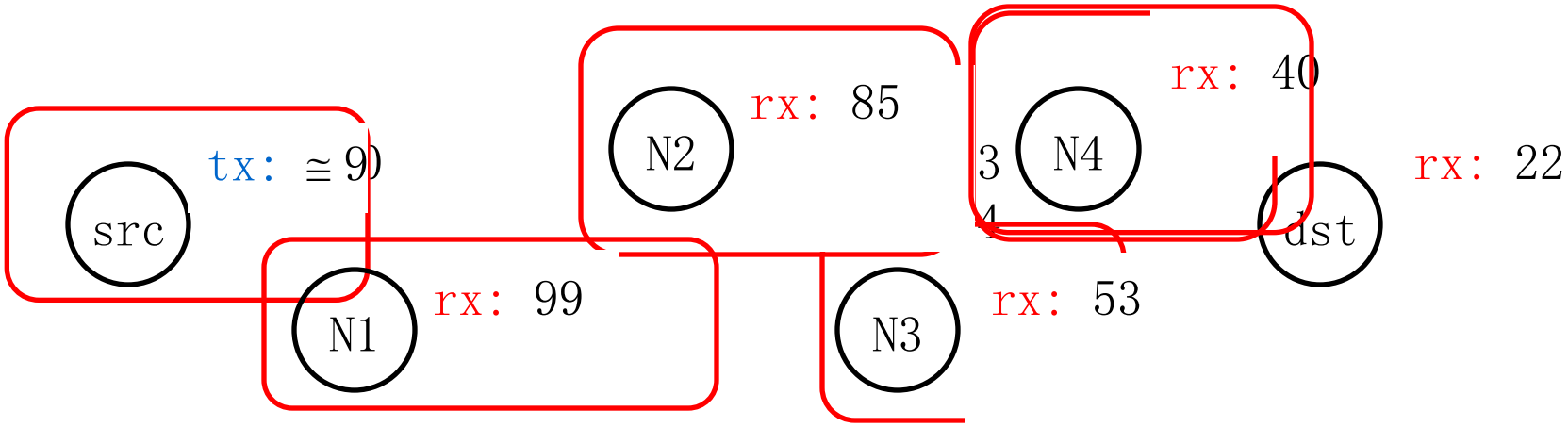


- Traditional routing: $^{1}/_{0.25}$ + 1 = 5 tx
- ExOR: $^{1}/_{(1-(1-0.25)^4)}$ + 1 = 2.5 transmissions
- Assumes independent losses

Comparing ExOR

- Traditional Routing:
  - One path followed from source to destination
  - All packets sent along that path
- Co-operative Diversity:
  - Broadcast of packets ***by all nodes***
  - Destination chooses the best one
- ExOR:
  - Broadcast packets ***to all nodes***
  - Only one node forwards the packet
  - Basic idea is delayed forwarding

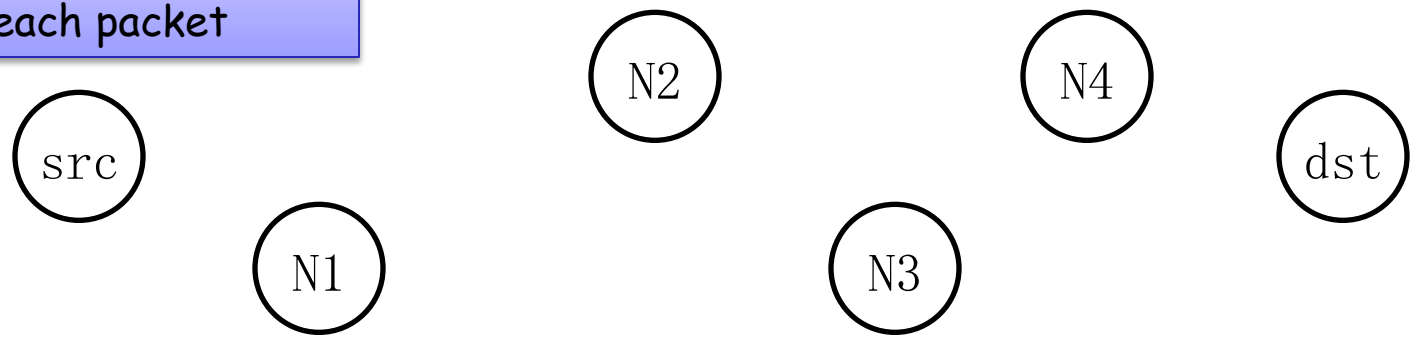
ExOR Batching



- Challenge: finding the closest node to have rx'd
- Send batches of packets for efficiency
- Node closest to the dst sends first
  - Other nodes listen, send remaining packets in turn
- Repeat schedule until dst has whole batch

Reliable Summaries

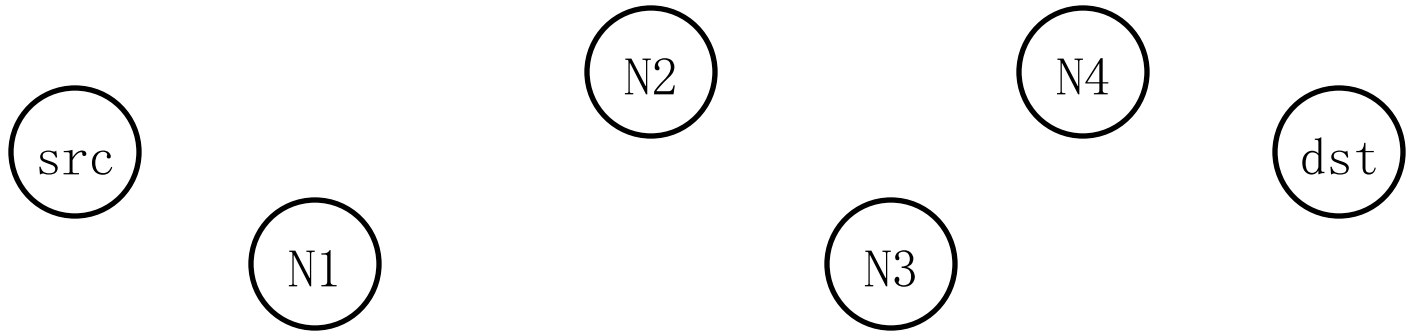
contains the sender's best guess of the highest priority node to have received each packet



The remaining forwarders transmit in order, but only send packets which were not acknowledged in the batch maps of higher priority nodes.

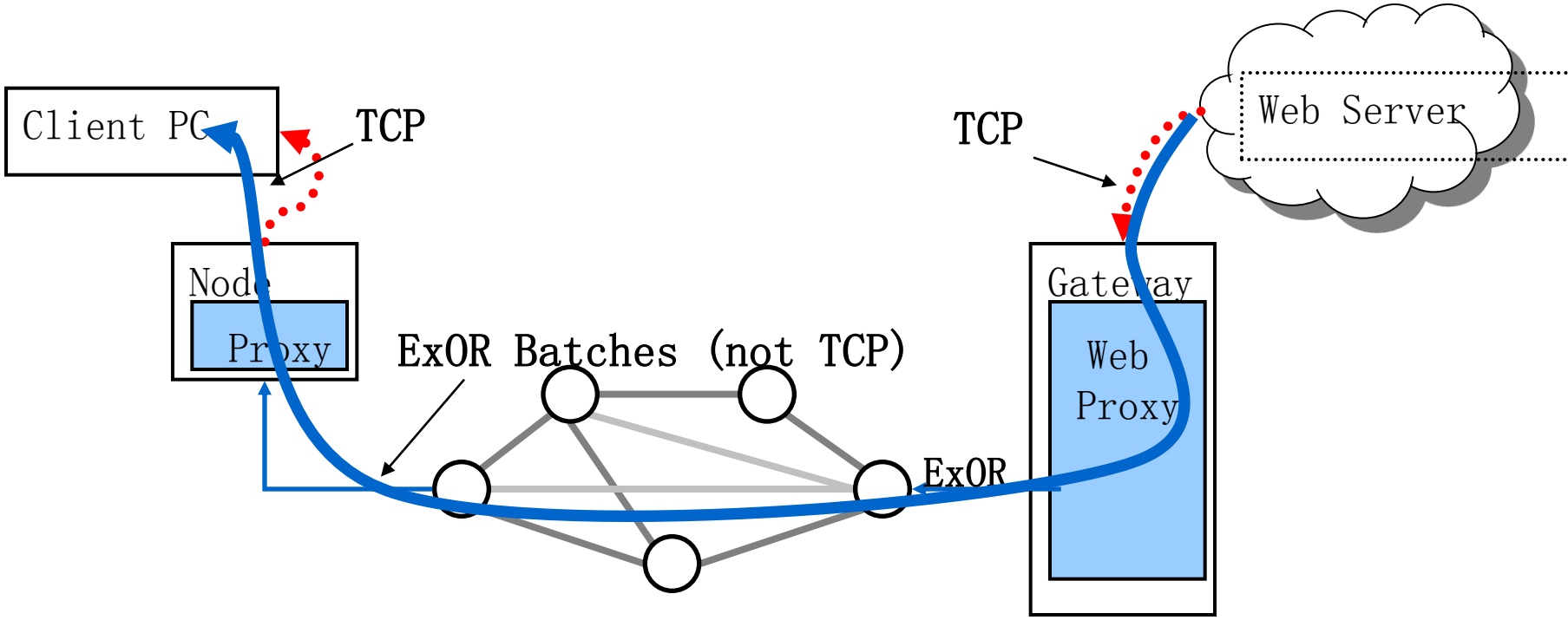
- Repeat summaries in every data packet
- Cumulative: what all previous nodes rx'd
- This is a gossip mechanism for summaries

Priority Ordering



- Goal: nodes "closest" to the destination send first
- Sort by ETX metric to dst
  - Nodes periodically flood ETX "link state" measurements
  - Path ETX is weighted shortest path (Dijkstra's algorithm)
- Source sorts, includes list in ExOR header

Using ExOR with TCP



- Batching requires more packets than typical TCP window

Summary

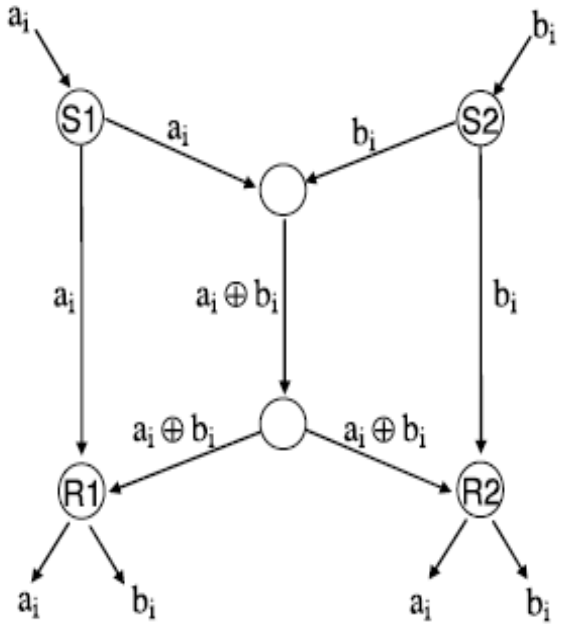
- ExOR achieves 2x throughput improvement
- ExOR implemented on Roofnet
- Exploits radio properties, instead of hiding them

Outline

- Opportunistic forwarding (ExOR)
- Network coding (COPE)

Background

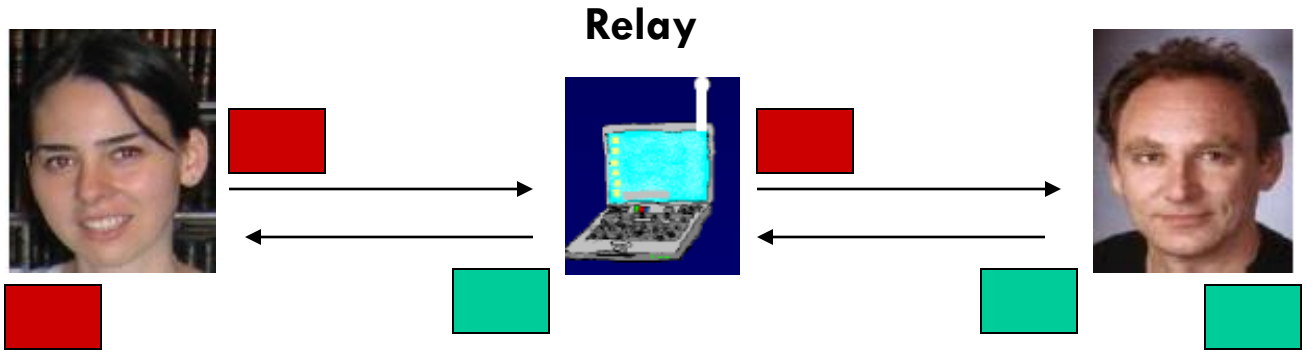
- Famous butterfly example:



- All links can send one message per unit of time
  - Coding increases overall throughput

Background

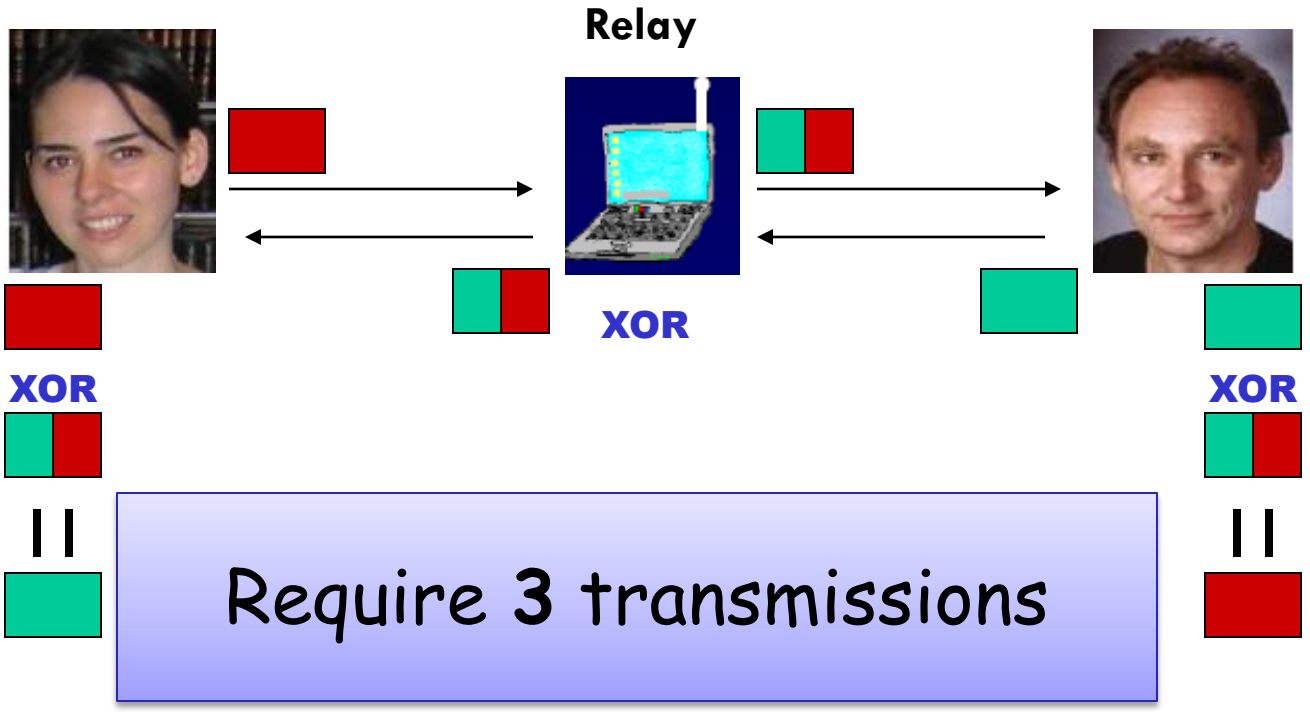
- Bob and Alice



Require 4 transmissions

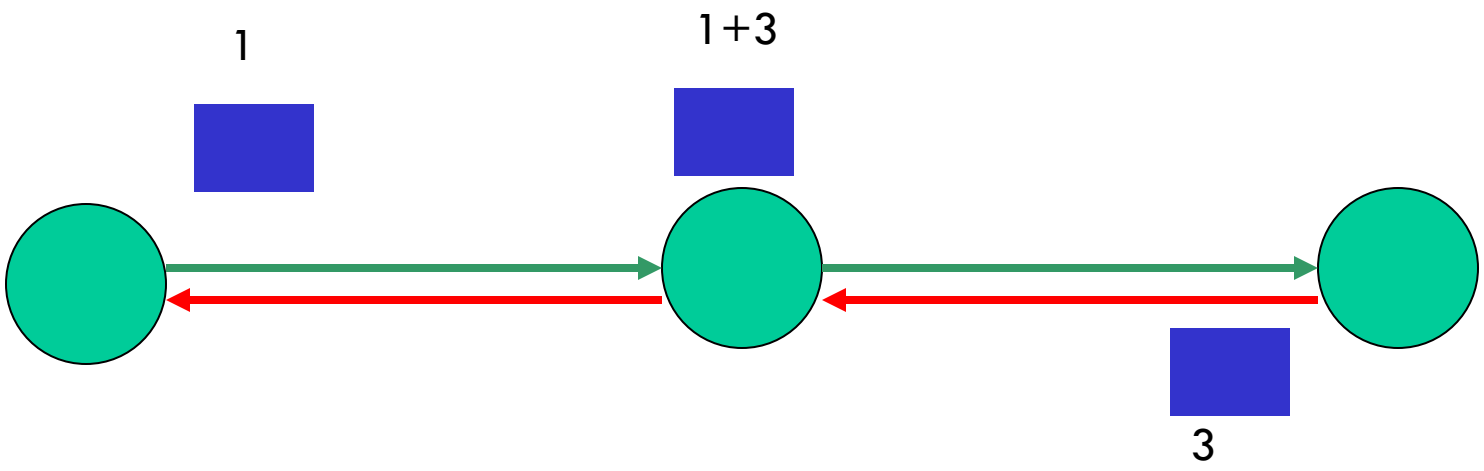
Background

- Bob and Alice



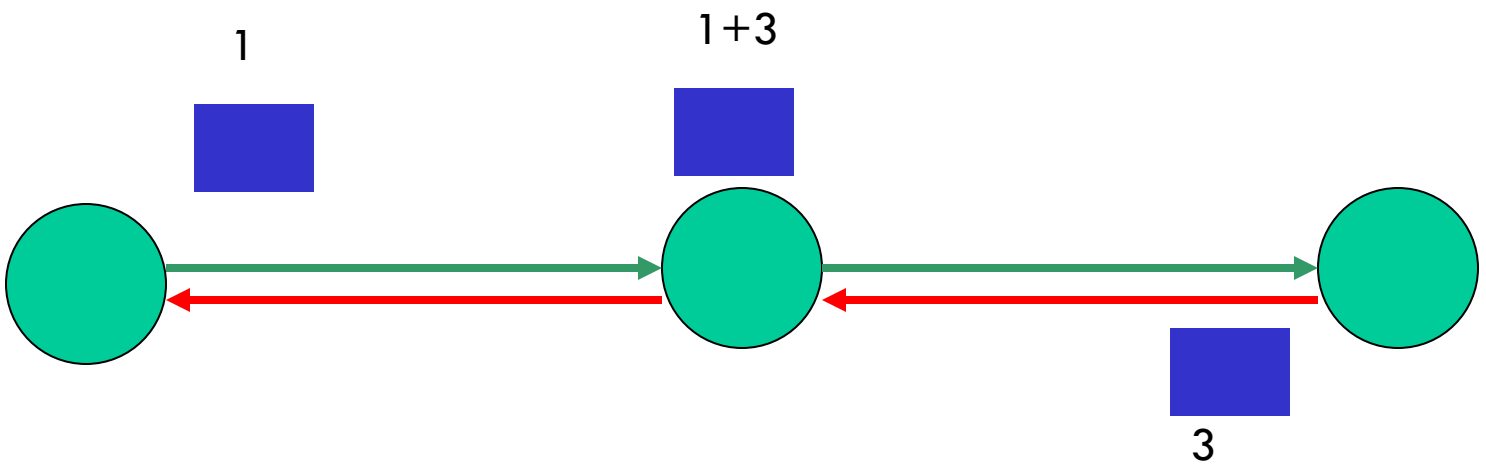
Coding Gain

- Coding gain = 4/3

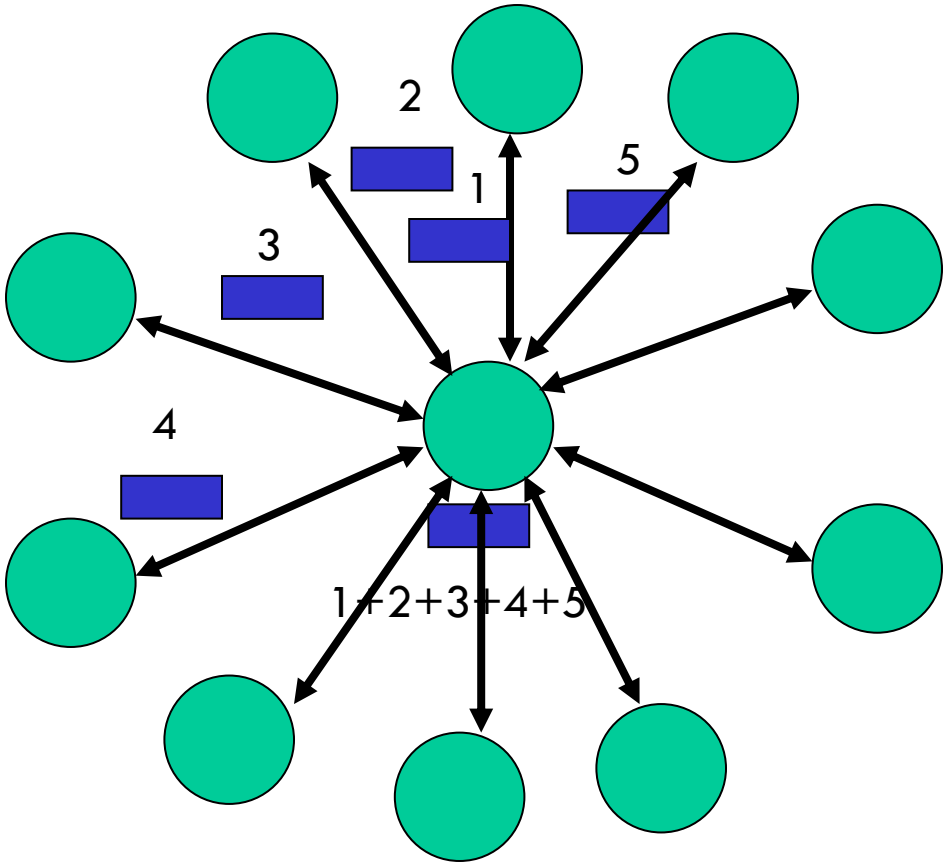


Throughput Improvement

- UDP throughput improvement ~ a factor 2 > 4/3 coding gain



Coding Gain: more examples



- Opportunistic Listening:
  - Every node listens to all packets
  - It stores all heard packets for a limited time

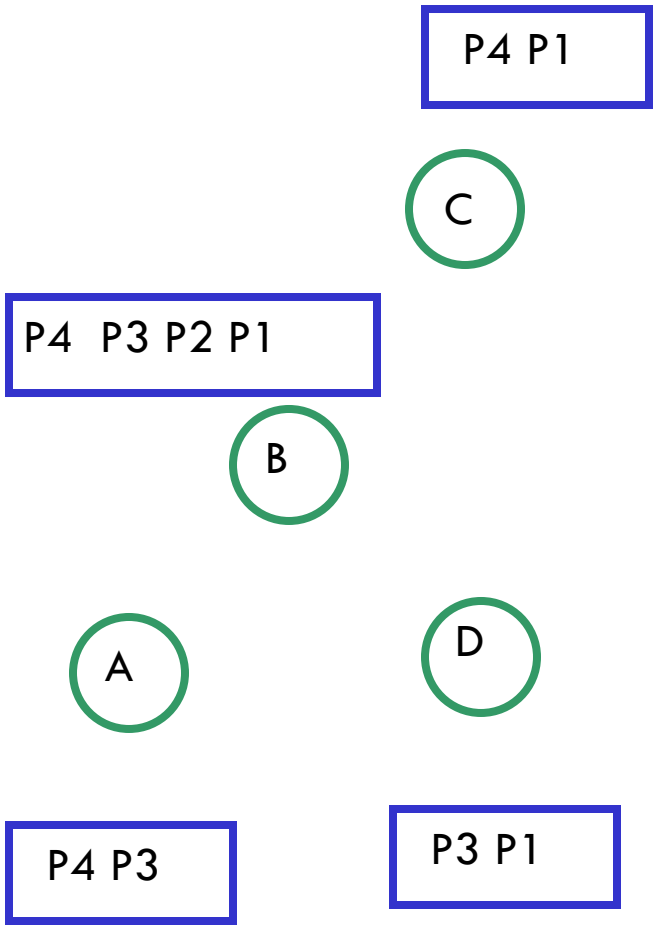
Without opportunistic listening, coding [+MAC] gain=2N/(1+N) → 2.
With opportunistic listening, coding gain + MAC gain → ∞

COPE (Coding Opportunistically)

- Overhear neighbors' transmissions
- Store these packets in a ***Packet Pool*** for a short time
- Report the packet pool info. to neighbors
- Determine what packets to code based on the info.
- Send encoded packets

- To send packet *p* to neighbor *A, XOR p* with packets already known to *A*. Thus, *A* can decode
- But how can multiple neighbors benefit from a single transmission?

Opportunistic Coding



B's queue	Next hop
P1	A
P2	C
P3	C
P4	D

Coding	Is it good?
P1+P2	Bad (only C can decode)
P1+P3	Better coding (Both A and C can decode)
P1+P3+P4	Best coding (A, C, D can decode)

Packet Coding Algorithm

- When to send?
  - Option 1: delay packets till enough packets to code with
  - Option 2: never delaying packets -- when there's a transmission opportunity, send packet right away
- Which packets to use for XOR?
  - Prefer XOR-ing packets of similar lengths
  - Never code together packets headed to the same next hop
  - Limit packet re-ordering
  - XORing a packet as long as all its nexthops can decode it with a high enough probability

Packet Decoding

- Where to decode?
  - Decode at each intermediate hop
- How to decode?
  - Upon receiving a packet encoded with n native packets
    - find n-1 native packets from its queue
    - XOR these n-1 native packets with the received packet to extract the new packet

Prevent Packet Reordering

- Packet reordering due to async acks degrade TCP performance
- Ordering agent
  - Deliver in-sequence packets immediately
  - Order the packets until the gap in seq. no is filled or timer expires

Summary of Results

- Improve UDP throughput by a factor of 3-4
- Improve TCP by
  - wo/ hidden terminal: up to 38% improvement
  - w/ hidden terminal and high loss: little improvement
- Improvement is largest when uplink to downlink has similar traffic
- Interesting follow-on work using analog coding

Reasons for Lower Improvement in TCP

- COPE introduces packet re-ordering
- Router queue is small ➔ smaller coding opportunity
  - TCP congestion window does not sufficiently open up due to wireless losses
- TCP doesn't provide fair allocation across different flows

Outline

- Overview
- MAC
- Routing
- Wireless in real world
- Leverage broadcasting nature
- **Explore the characteristic of wireless signal**

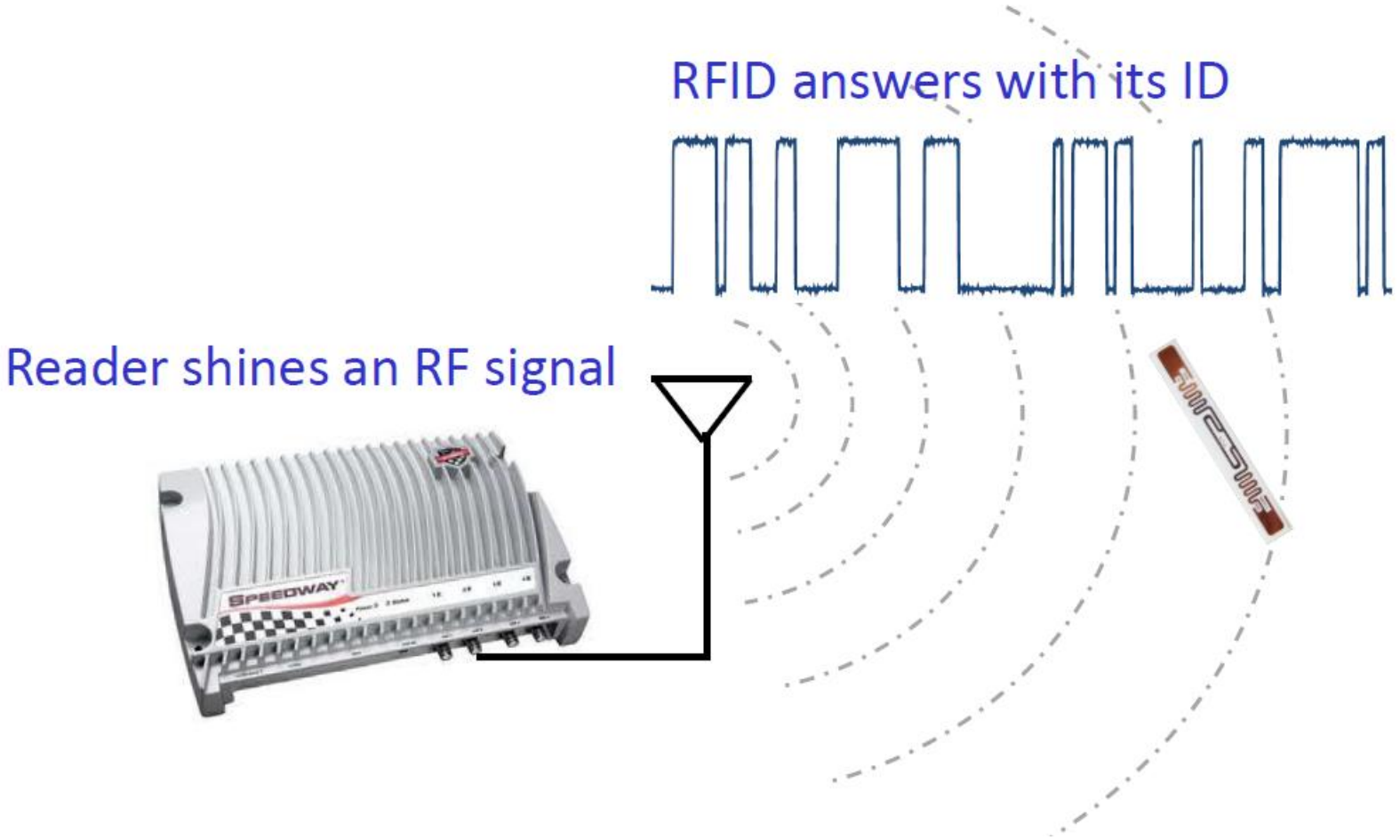
Accurate RFID Positioning in Multipath Environments

Jue Wang & Dina Katabi

ACM Sigcomm 2013

RFIDs

Battery-free RF stickers with unique IDs



RFIDs

5-cent stickers to tag any and every object

Reader's range is ~15m

Imagine you can localize RFIDs to within 10 to 15 cm!

If we can locate RFID to within 10 to 15cm

No more customer checkout lines

If we can locate RFID to within 10 to 15cm

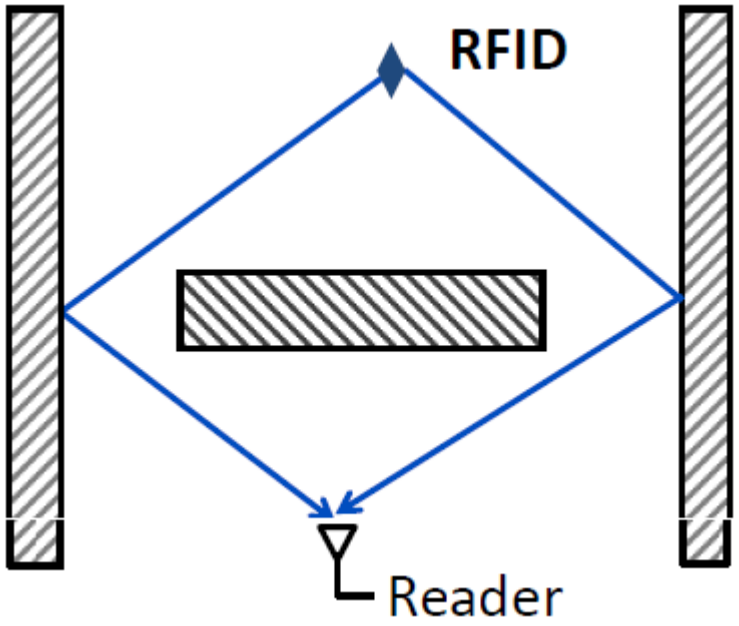
No more customer checkout lines

RFIDs on Basket

The Challenge: Multipath Effect

Localization uses **RSSI or Angle-of-Arrival (AoA)**

But, signal bounces off objects in the environment



Angle of signal is not the direction of the RFID

Multipath propagation limits the Accuracy of RFID localizations

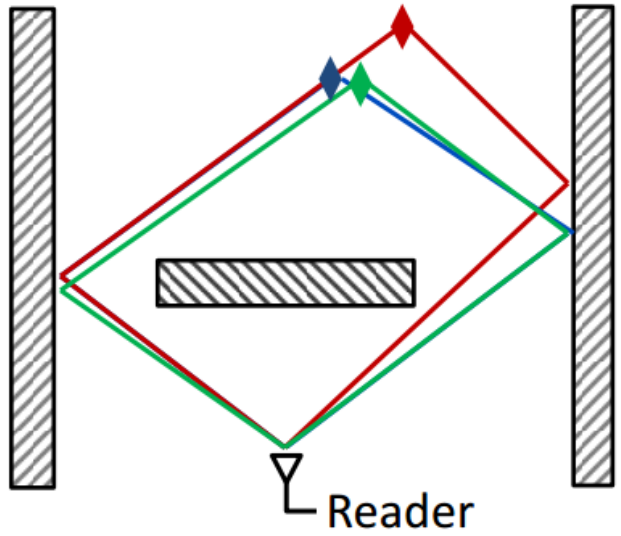
PinIt

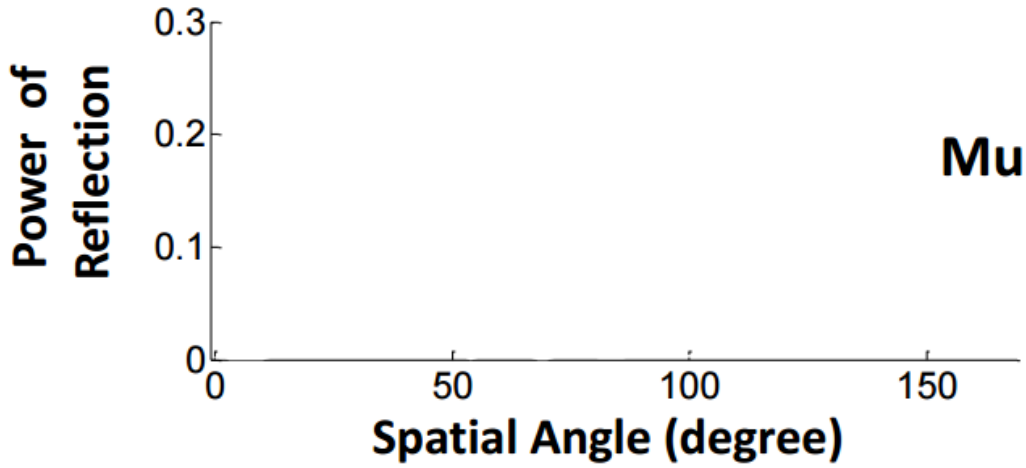
Accurate RFID localization (e.g., 10 to 15cm) even in multipath and non-line-of-sight settings

- Focuses on proximity to reference RFIDS
- Exploits multipath effects to increase accuracy

PinIt Exploits Multipath

Signals from nearby RFIDs propagate along closer paths and experience similar reflections

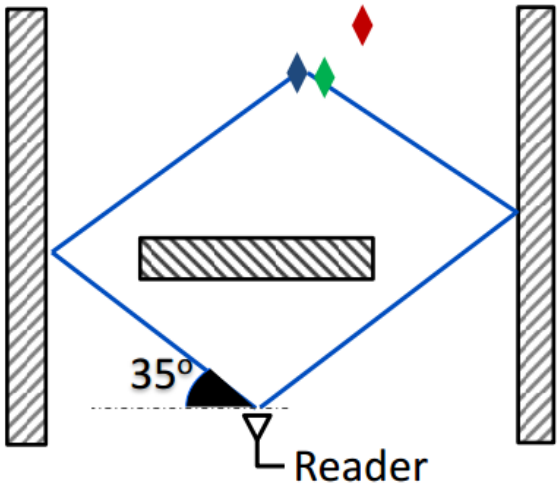


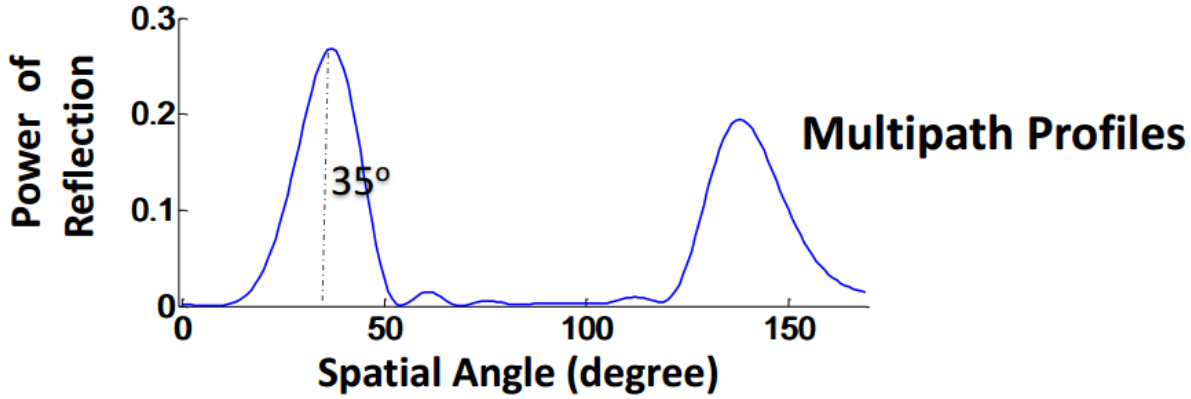


Multipath Profiles

PinIt Exploits Multipath

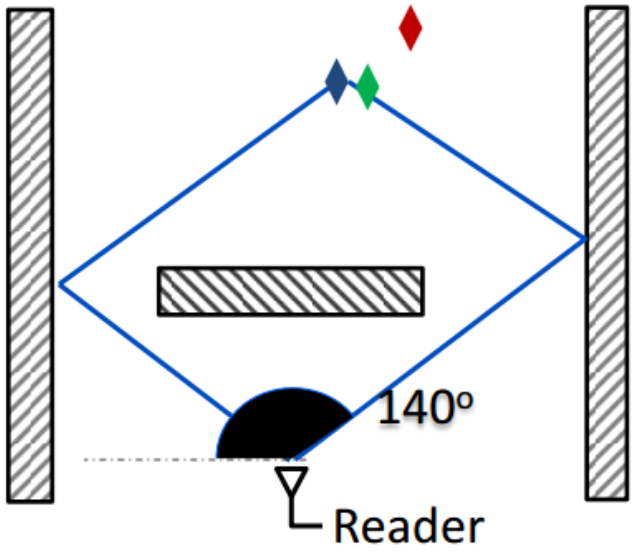
Signals from nearby RFIDs propagate along closer paths and experience similar reflections

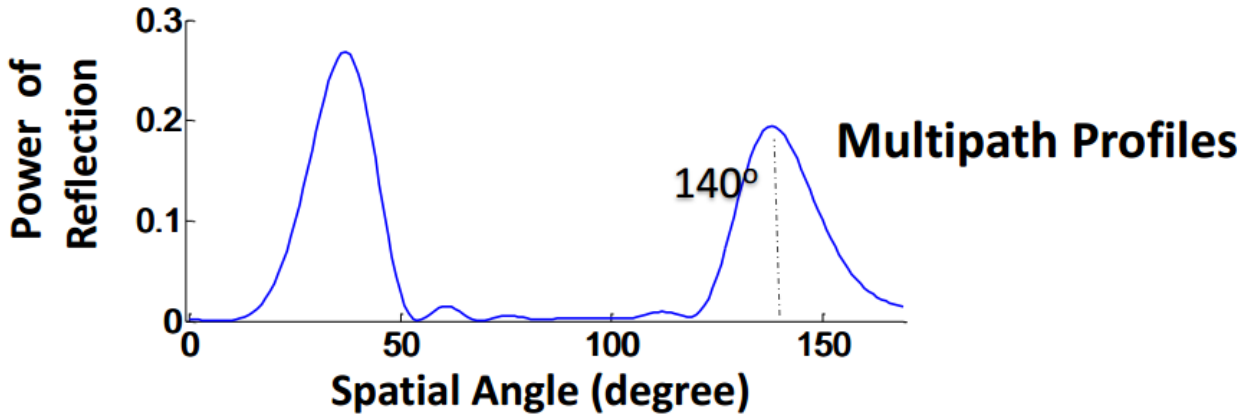




PinIt Exploits Multipath

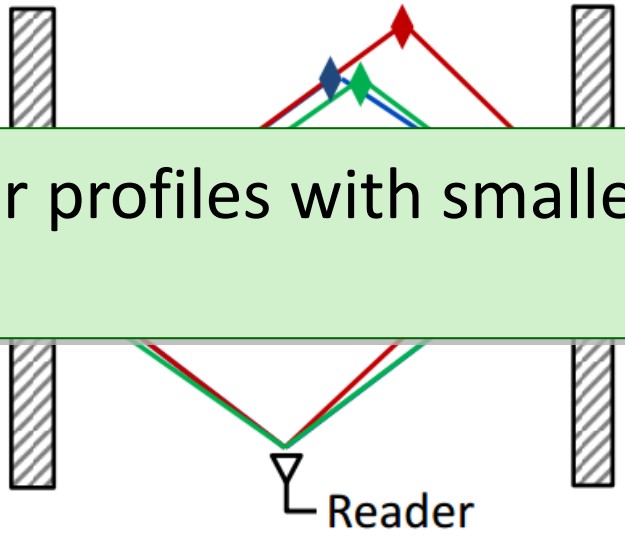
Signals from nearby RFIDs propagate along closer paths and experience similar reflections



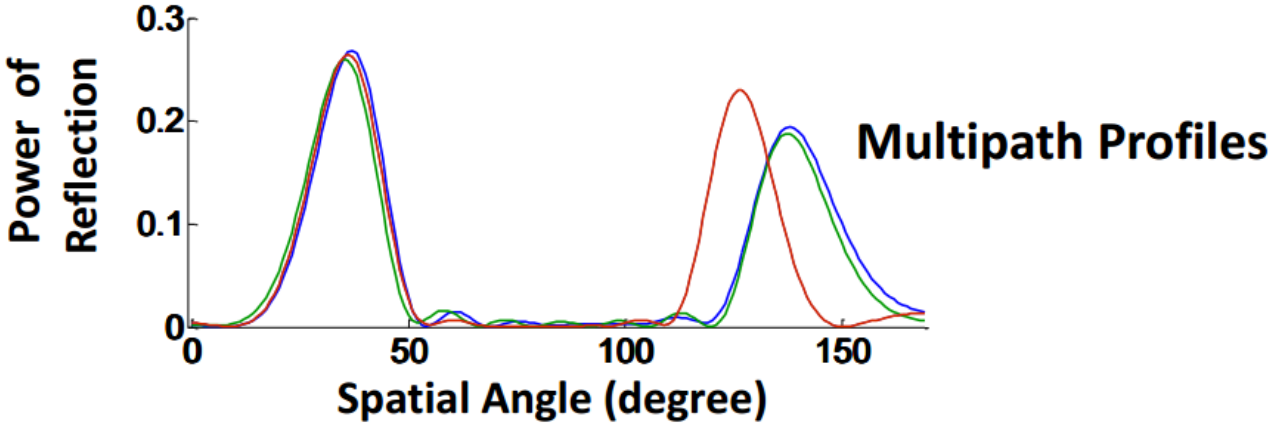


PinIt Exploits Multipath

Signals from nearby RFIDs propagate along closer paths and experience similar reflections



Nearby RFIDs have similar profiles with smaller shifts in the peaks

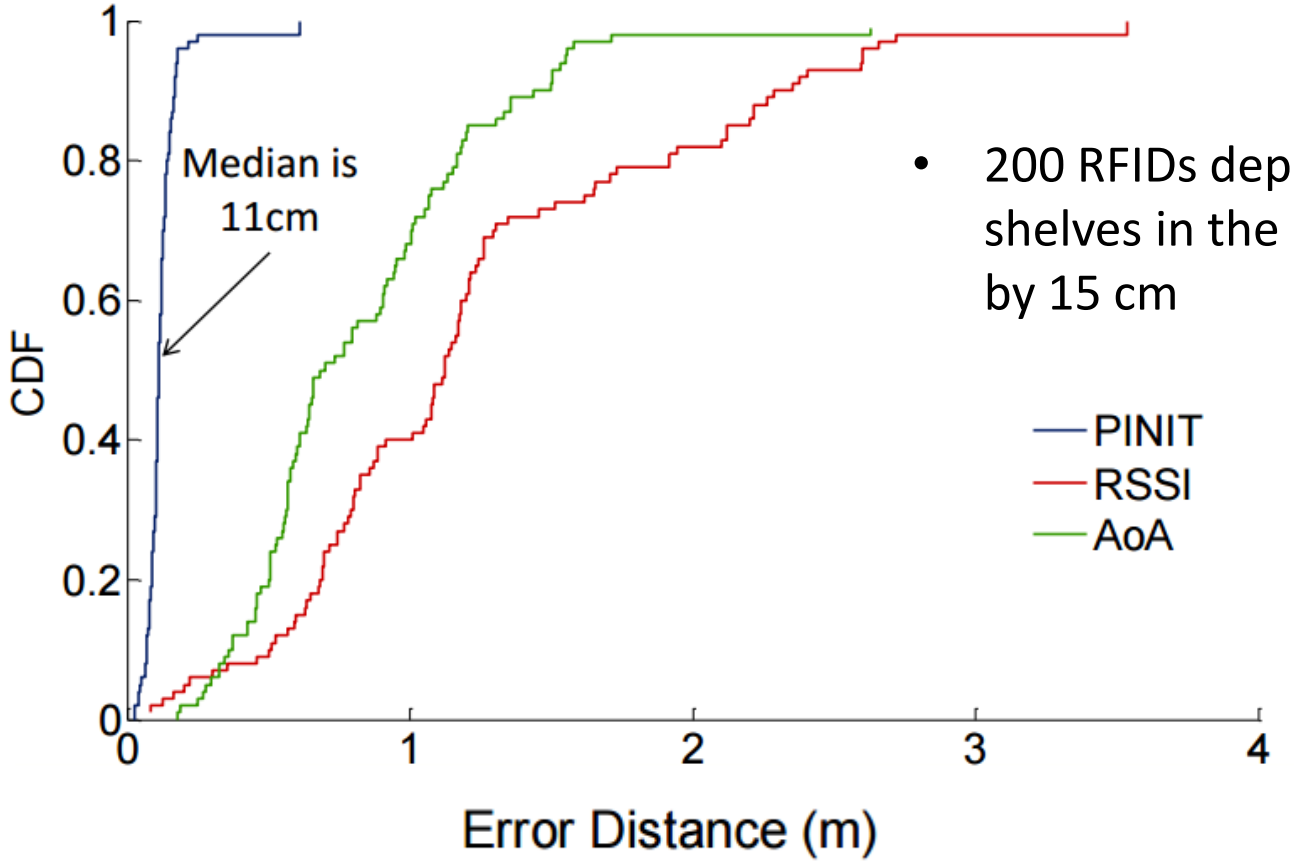


Implementation & Evaluation

- Implemented a PinIt Reader in USRP
- Commercial off-the-shelf RFIDs

- Mounted the antenna on an iRobot that slides back and forth

Positioning Accuracy



- 200 RFIDs deployed on the shelves in the library spaced by 15 cm

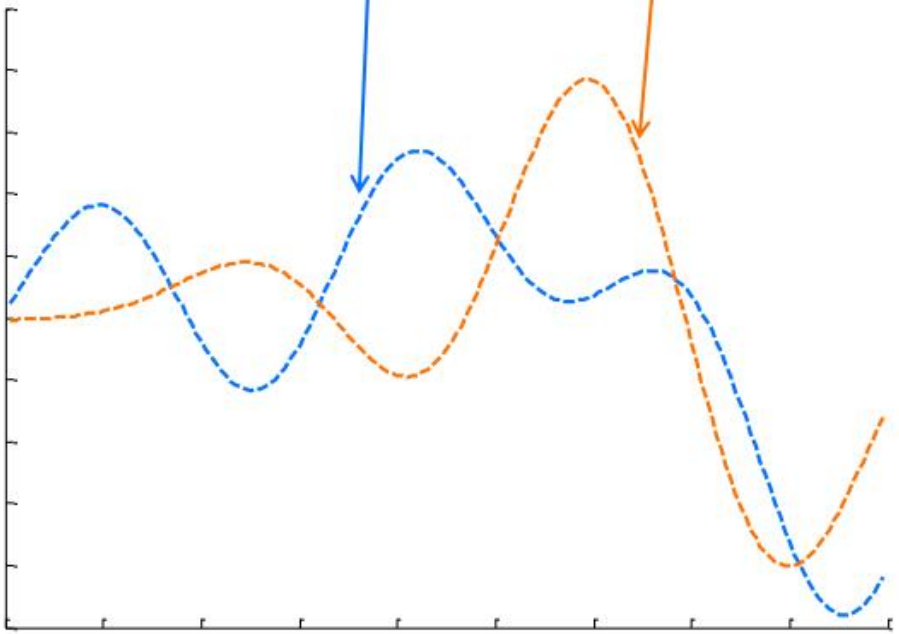
PinIt improve the accuracy by 6x in comparison to AoA and 10x in comparison to RSSI

Automatic Checkout

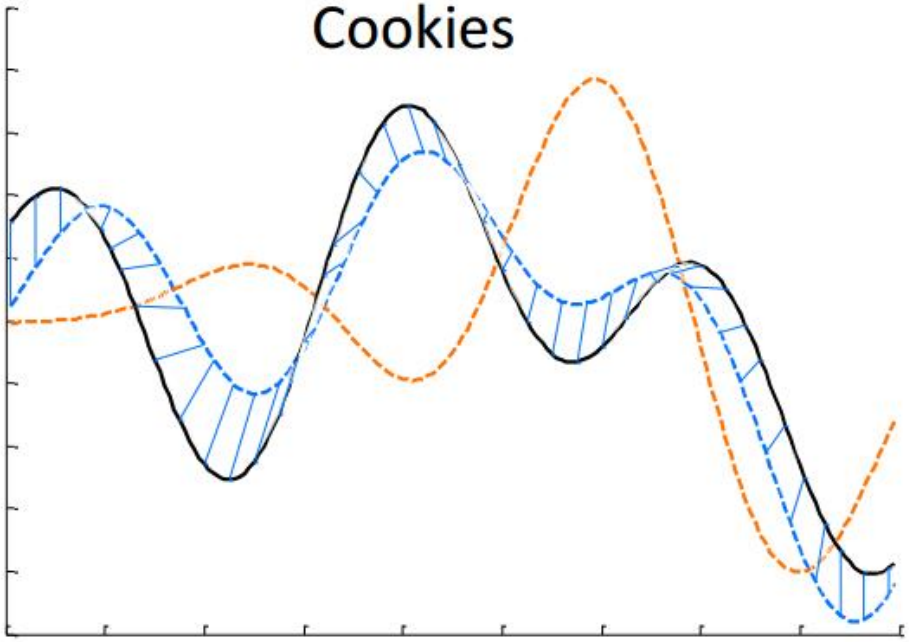
Five items in two adjacent baskets at checkout

Which Items Belong to Which Basket?

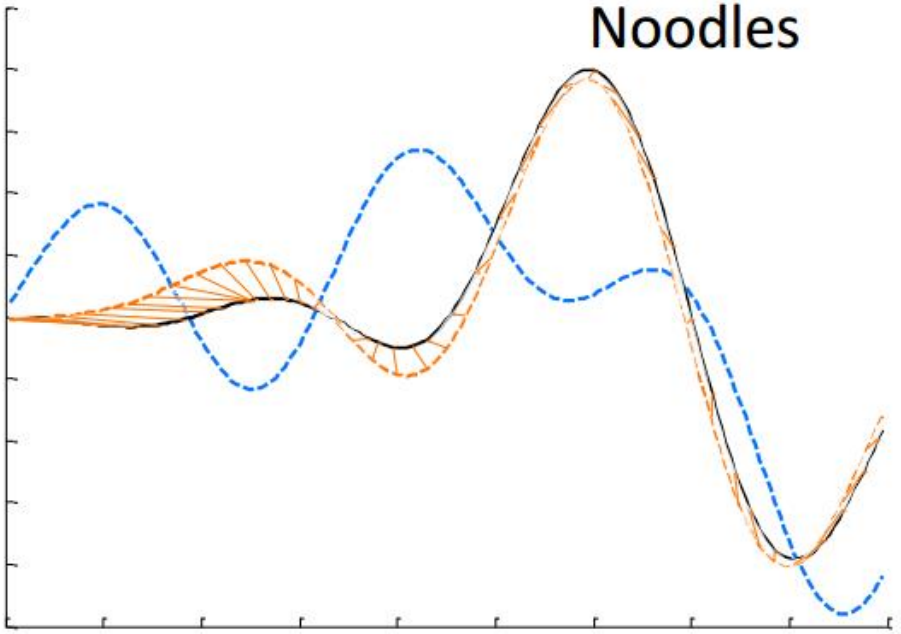
?



Is the Cookie Bag in the Orange or Blue Basket?



Is the Noodle in the Orange or Blue Basket?



Brief Summary

- PinIt provides accurate RFID positioning even in multipath and NLOS settings
- It uses DTW to compare RFID multipath profiles
- It enables new applications including eliminating checkout lines, object tracking in libraries and pharmacies, smart homes, …