Wireless Networking

Dave Eckhardt

15-441, Computer Networks

Carnegie Mellon University

Many slides stolen from Dave Maltz

(some of them stolen from Dave Johnson)

Synchronization

- Homework 3
  - Out today, due next Monday

The Problem

- Not really possible to cover “wireless” in one lecture
  - Includes everything from ELF to X-rays
- Approach
  - Give some sense the field

Outline

- Background
- 802.11
  - Reminder about physical, MAC layer issues
  - Interesting higher-level features
- Something different
  - Cellular, WiMax
  - BlueTooth - “Personal Area Networking”
  - “ZigBee” sensor/control networks

What's Special?

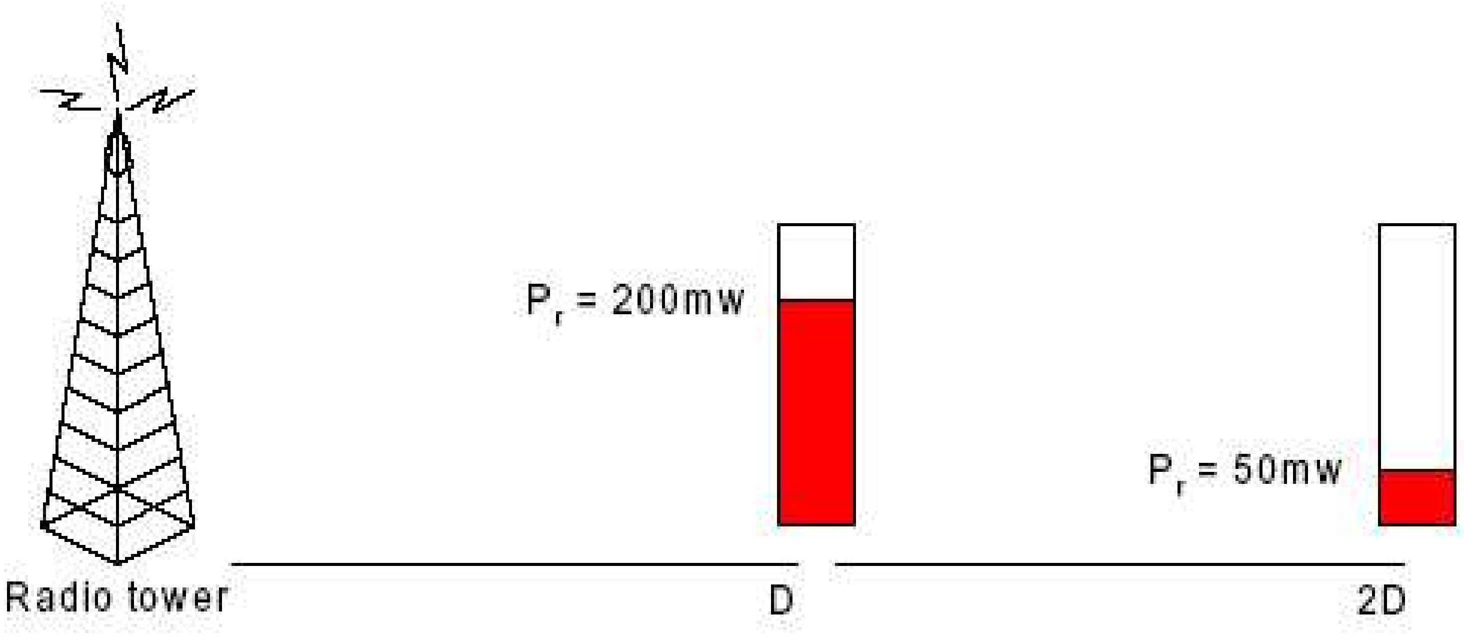
- Medium Access Control
  - Solved for wires, but distributed noisy coordination is hard
- Errors
  - Wired links have BER ~ 10-9
  - Wireless links may have BER 10-4 to 10-7
- Boundaries
  - Machines aren't “sort of” connected to an Ethernet
  - Radio propagation boundaries fuzzy at best

The Physics of Wireless Radio

Free Space Propagation

In a vacuum, signal strength follows ***inverse square law:***

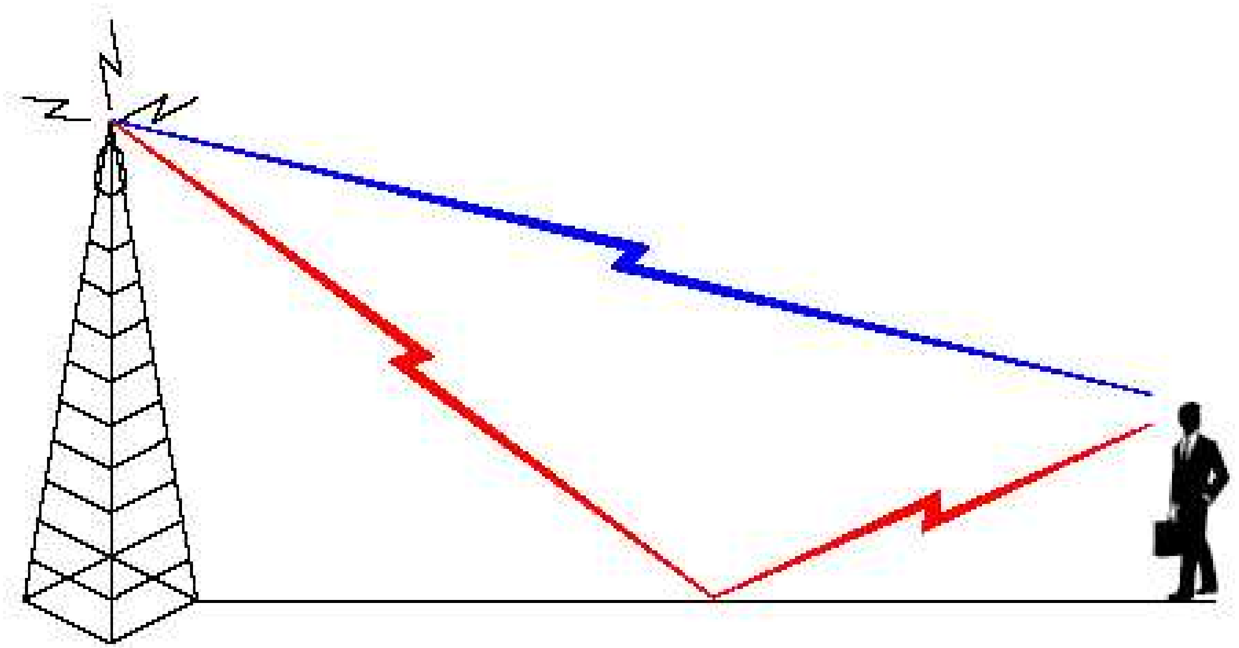
- Strength attenuates inversely with square of distance
- Strength at 2D meters is ¼ strength at D meters
- In an atmosphere, signal strength loss is much worse



Reflection

- Occurs when a radio wave strikes an object with large size compared to the wavelength
- Reflection may occur from buildings, walls, ground

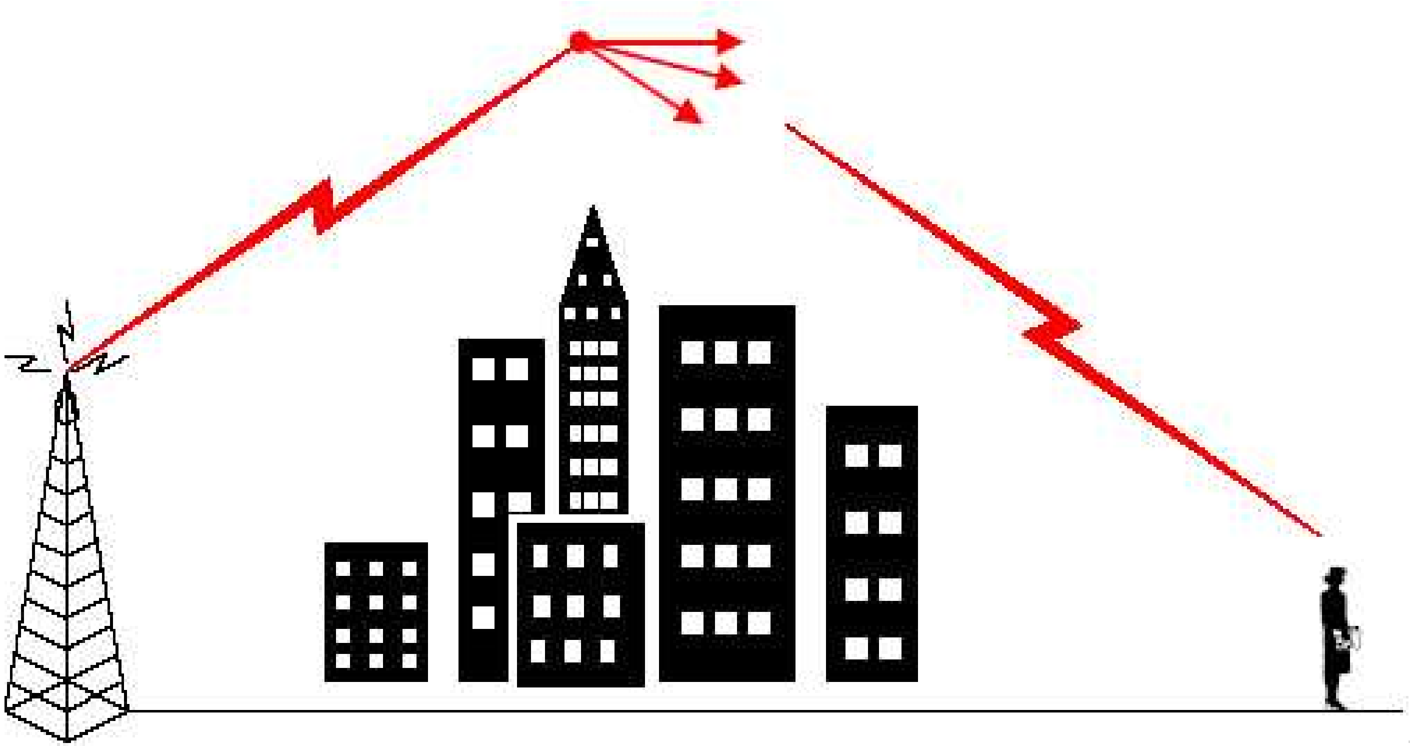
Signal strength attenuation ~ $1/D^4$



Diffraction

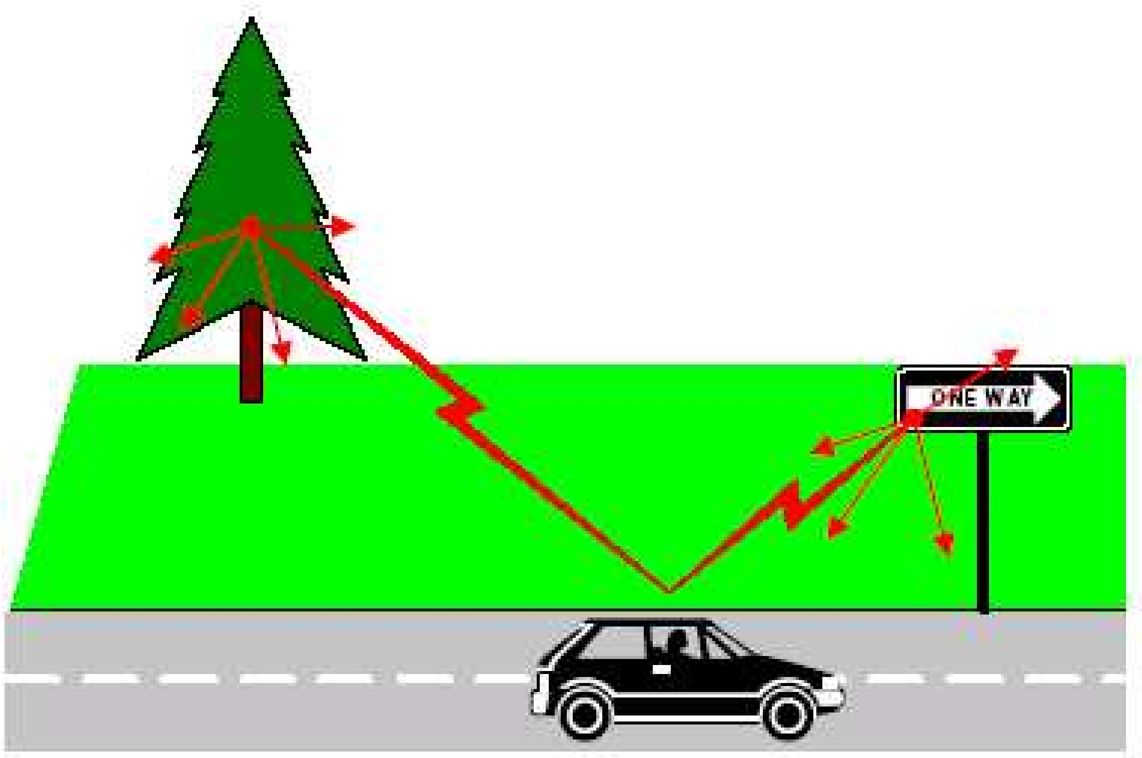
Allows radio signals to propagate

- Around curved surface of the earth
- Behind obstructions



Scattering

- Occurs when a radio wave strikes an object with small dimensions compared to the wavelength
- Scattering may occur from foliage, street signs, lamps, stuff on your desk



Absorption (Blockage)

Radio waves are absorbed (energy dissipated) by objects they go through

- Outdoors: buildings, rain, humidity
- Indoors: walls, desks, glass

Amount of absorption depends on material and frequency. Generally:

- Lower frequencies penetrate objects better
- Higher frequencies have more attenuation

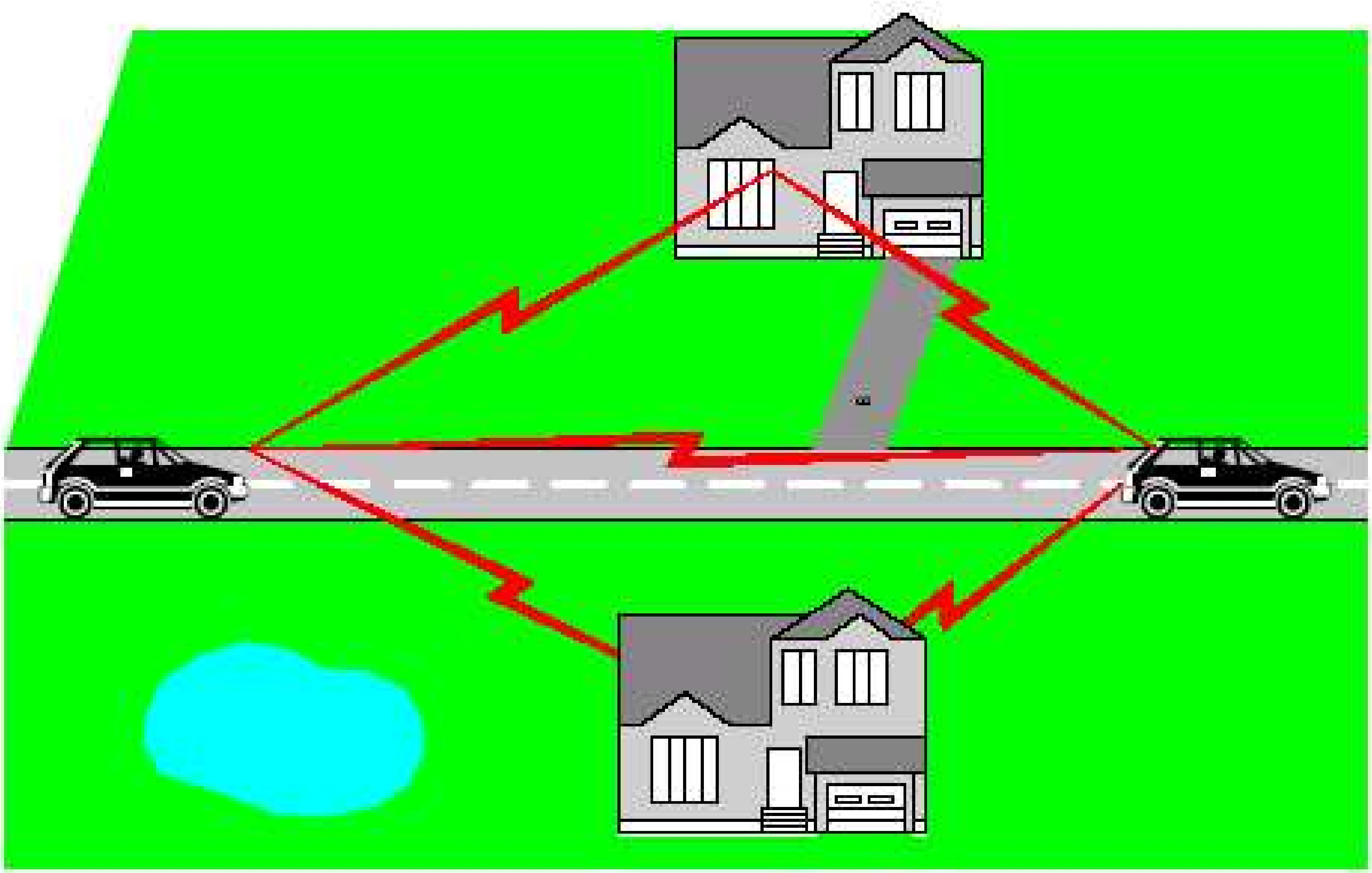
Absorption Values

Material	Loss (dB)	Frequency
Concrete block	13-20	1.3 GHz
Plywood (3/4”)	2	9.6 GHz
Plywood (2 sheets)	4	9.6 GHz
Plywood (2 sheets)	6	28.8 GHz
Aluminum siding	20.4	815 MHz
Sheetrock (3/4”)	2	9.6 GHz
Sheetrock (3/4”)	5	57.6 GHz
Turn corner in corridor	10-15	1.3 GHz

From Girod99

Multipath

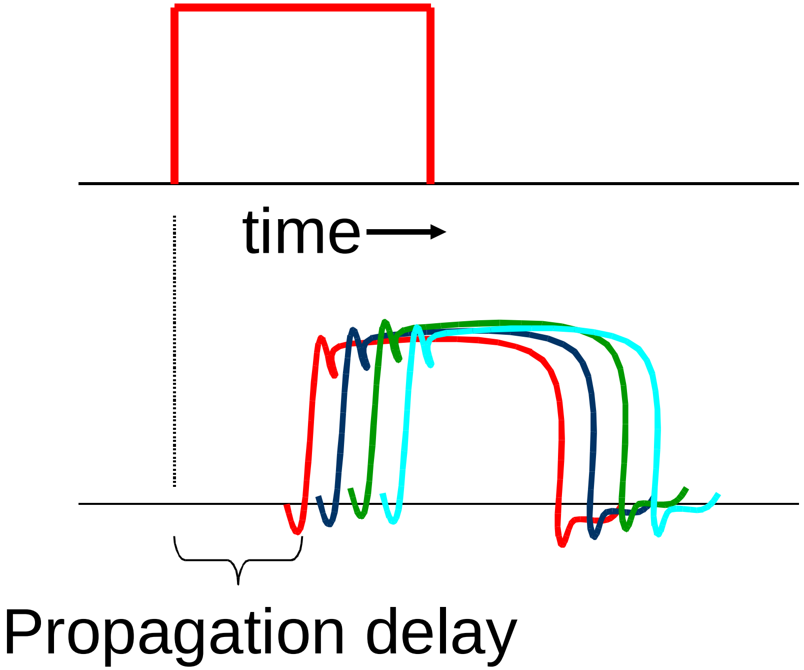
Fundamental problem for wireless networks



Multipath Problems - 1

Intersymbol Interference (Delay spread)

- Signals along different paths arrive at different times
- One symbol may overlap with another
- Worse at higher bit rates



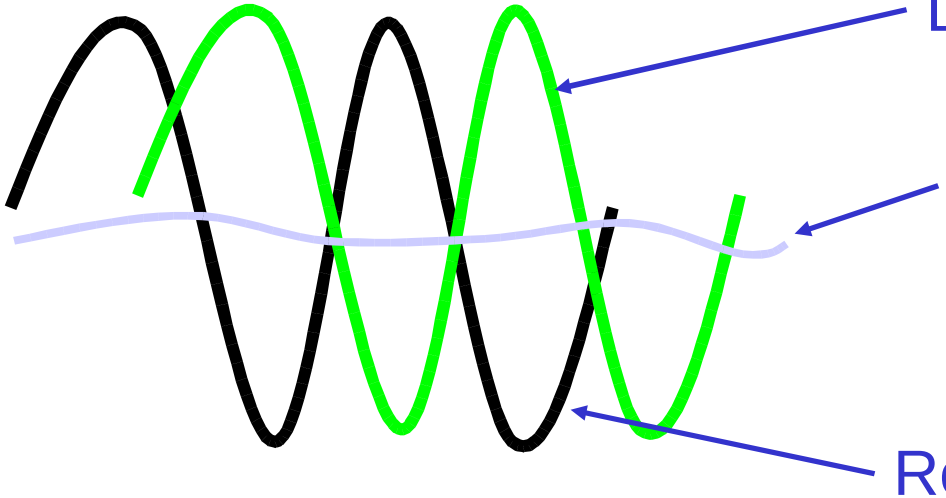
Original transmitted symbol

Sum of original signal plus delayed copies seen at receiver

Multipath Problems - 2

Rayleigh fading

- Each reflected signal may have different phase
- Signal arrivals out of phase cancel each other out
- Movement creates large random changes



Direct LOS signal

Resulting signal

Reflected/delayed signal

From Girod99

What To Do?

Digital Signal Processing

- Use big math and high-speed processors to tease signal out of noise

Antenna Diversity

- Destructive interference is very localized
- If you have two antennas, you have two locations

Phased Arrays, Steerable Antennas

- Combine many antennas electrically into one

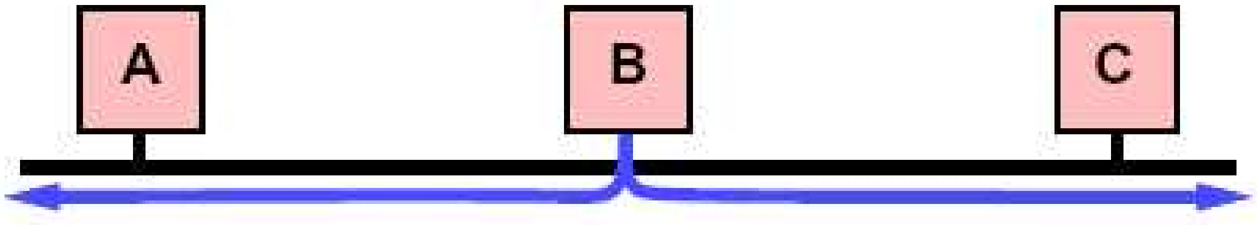
Why is Throughput on a Wireless Link So Low?

Why is sharing so hard?…

Wired Carrier Sense Multiple Access (CSMA)

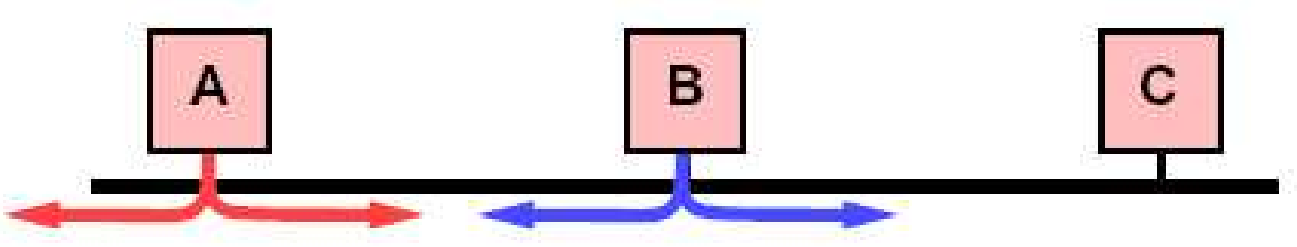
How to share a common channel?

- Listen for ***carrier*** before transmitting
- Carrier is just energy from another transmission
- While you hear carrier, wait before transmitting



Wired Collision Detect (CD)

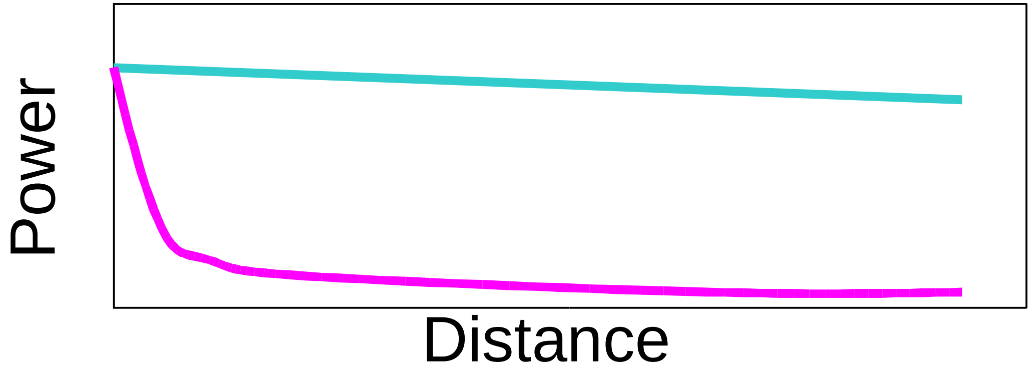
- Listen while transmitting
- If what you hear isn't what you're sending, then ***collision***:
  - Abort transmission of current packet
  - Try again after a random delay
  - Each collision for same packet doubles average delay



Wireless CSMA

CSMA can be used in wireless, but has problems

- ***wired*** network: signal strength at sender and receiver are essentially the same
- ***wireless*** network: ***inverse square law*** (or worse) applies ($P_{recv} = P_{xmit}/D^k$, $k > 2$)



CSMA does not give the right information in wireless:

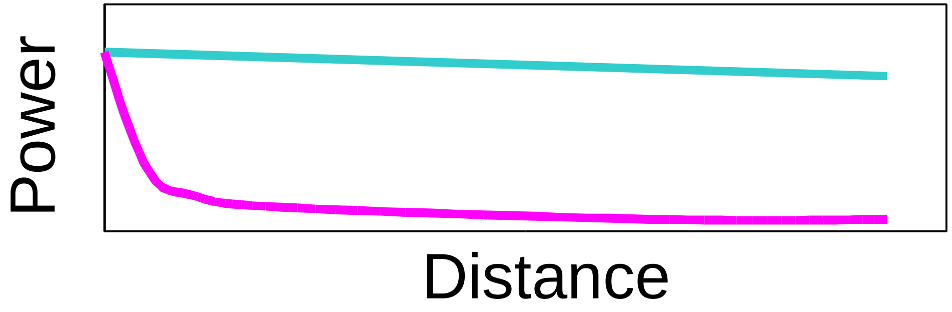
- Carrier sense detects signals at the ***transmitter***
- But collisions occur ***at the receiver***

Issue 1: Wireless Collision Detect

Wireless can’t do collision detect like Ethernet

Can’t effectively listen while you send:

- In some systems, the hardware isn’t flexible enough:
  - Transmit and receive are on different frequencies
  - Transceiver might be half-duplex

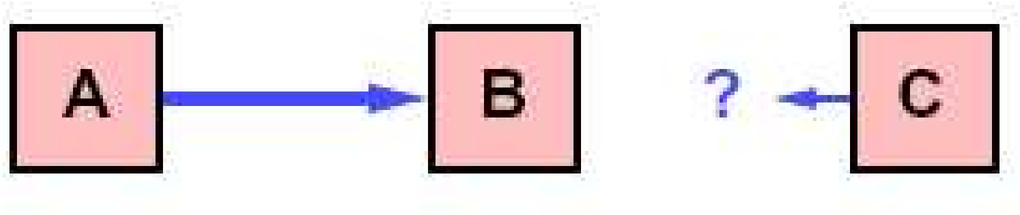


- In any case, all you could hear is yourself any way:
  - The inverse square law
  - Your own signal strength at your own antenna is ***much*** stronger than anybody else’s signal

Issue 2: The Hidden Terminal Problem

Consider the following situation:

- A is sending to B
- C is ***out of range*** of A's transmissions to B
- C wants to send (to anybody)



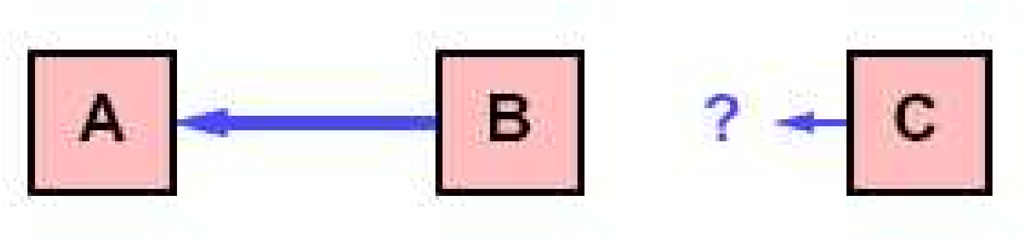
CSMA doesn't work well for wireless here:

- C can't know to wait since it can't hear carrier from A
- B can hear both A and C, thus collision at B
- A is "hidden" to C

Issue 3: The Exposed Terminal Problem

Consider the following situation:

- B is sending to A
- C is ***in range*** of B's transmissions to A
- C wants to send to anybody but B



CSMA doesn't work well for wireless here either:

- C thinks it should wait since it can hear carrier from B
- If A is out of range of C, then C waits needlessly
- C is "exposed" to B

Partial Solution: Virtual Carrier Sense

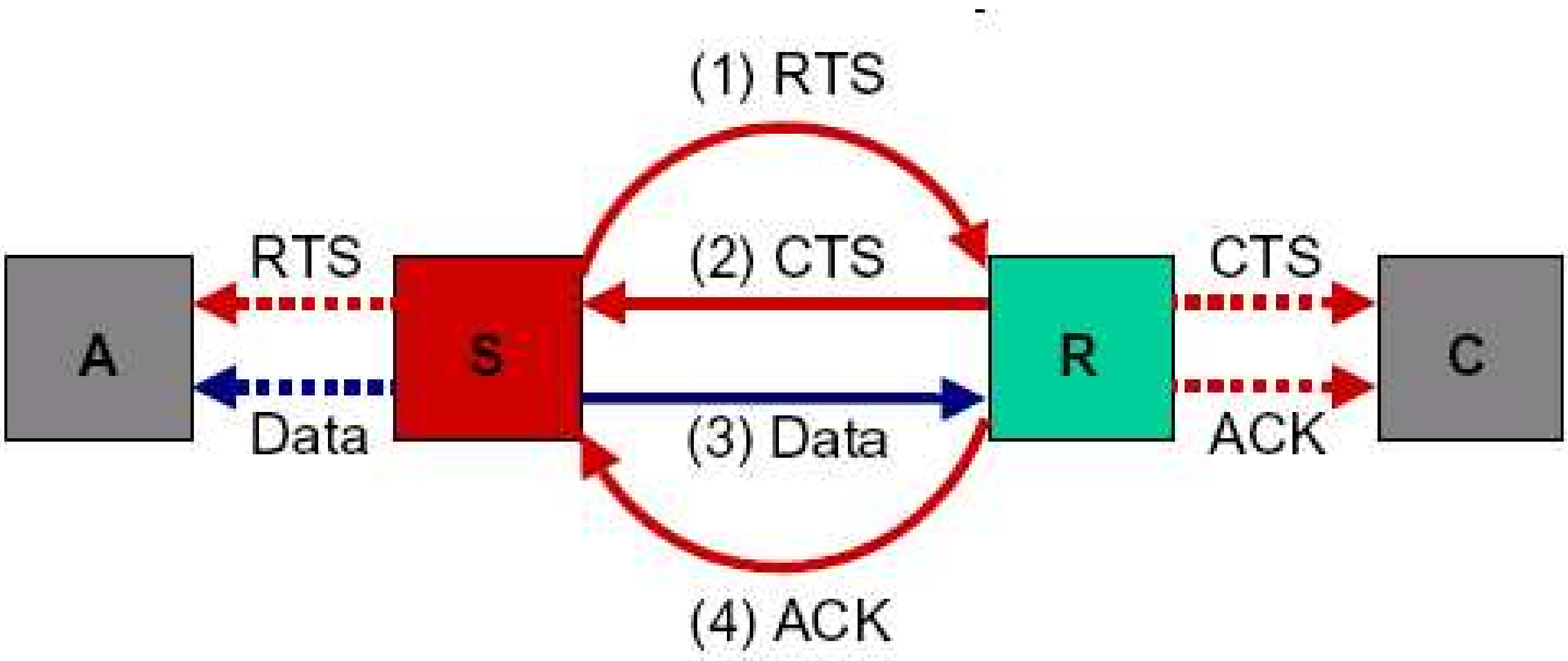
Packet types:

- ***Request-to-Send*** (RTS): Sender sends to receiver before sending a data packet
- ***Clear-to-Send*** (CTS): Receiver replies if ready for data packet to be sent
- ***Acknowledgment*** (ACK): receiver sends if data is received successfully

All packets contain:

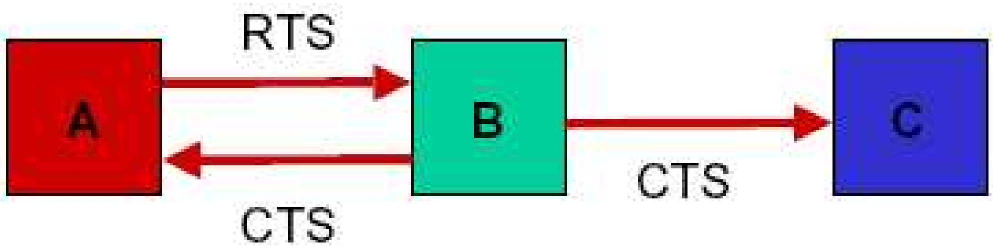
- Address of the ***sender*** of the intended data packet
- Address of the ***receiver*** of the intended data packet
- ***Duration*** of the remainder of the transmission

Virtual Carrier Sense – 2



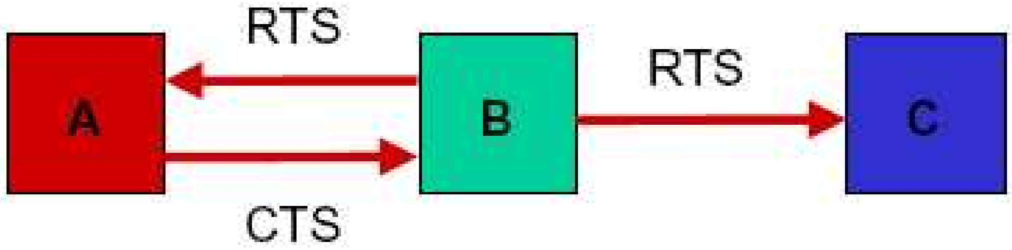
Virtual Carrier Sense - 3

- Hidden terminal problem is avoided:



C waits to send since it hears B’s CTS

- Exposed terminal problem is avoided:



C does not wait to send since it does not hear A’s CTS

Does (and cannot) ***not*** prevent all collisions!

IEEE 802.11 (WiFi)

IEEE 802.11 Usage Model

Host computer sees an “Ethernet interface”

- Just like a wired LAN
- Uses 48-bit 802.3 MAC addresses
- All hosts “in range” of each other see common shared channel
- Supports ARP, broadcast, LAN multicast
- Can directly communicate with neighbors

IEEE 802.11 Modes of Operation

Media Access Control modes

- Distributed Coordination Function (DCF)
- Point Coordination Function (PCF)

Infrastructure mode

- SSID&AP name assigned to each Access Point (AP)
- Cards use AP promiscuous mode to find good AP
- Then filter (in baseband) all packets from other APs

Infrastructureless (ad-hoc) mode

- Nodes communicate directly with each other

802.11 Carrier Sensing

802.11 uses both ***physical*** and ***virtual*** carrier sensing:

- Physical carrier sense provided by PHY
- Virtual carrier sense provided by MAC

Virtual carrier sensing:

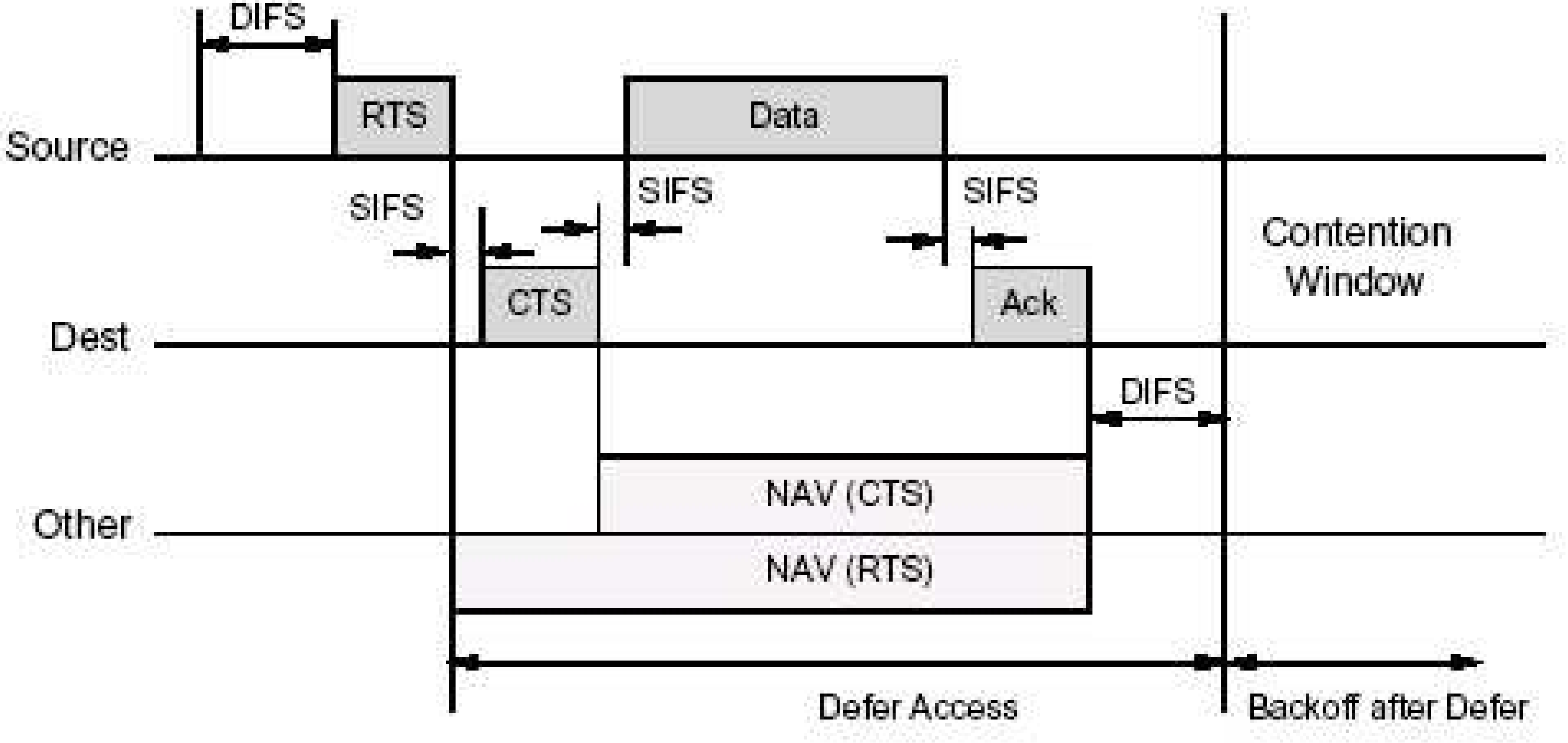
- Maintained by station through ***Network Allocation Vector (NAV)***
- NAV records prediction of future traffic on medium
- Counter that counts down busy time at uniform rate
- Set based on Duration field in received packets (e.g., RTS, CTS)
- When nonzero, virtual carrier sense thinks medium is busy

Carrier sense mechanism combines both mechanisms:

- Medium considered busy whenever either indicates carrier
- Medium also considered busy whenever our own transmitter is on

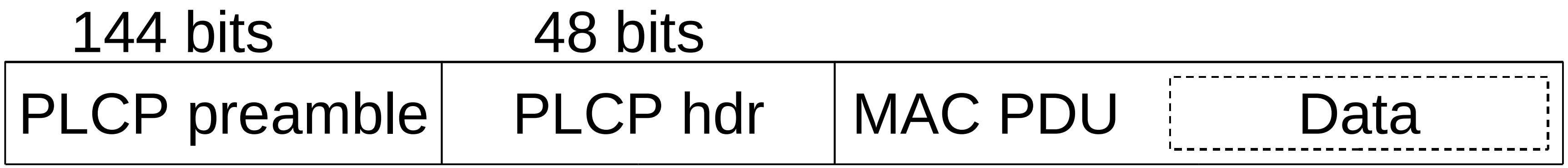
Use of RTS and CTS

Other data senders must wait until entire RTS/CTS/Data/ACK finished



RTS/CTS only used for data packets larger than some threshold --- You can tune this!

Multirate Support in 802.11



144 bits

48 bits

PLCP preamble

PLCP hdr

MAC PDU

Data

To enable sharing the media among many nodes:

- All control information must be transmitted at rate understood by all stations
- After control information, transceivers change to rate agreed on by sender and receiver
- Preamble and header sent at lowest coding rate
  - – 1 Mbps in .11b/g
  - – 6 Mbps in .11a

Using The Infrastructure

Multiple base stations in a “service set”

- Each station associates with one at at time
- Ideally, the “best” (typically: the loudest)

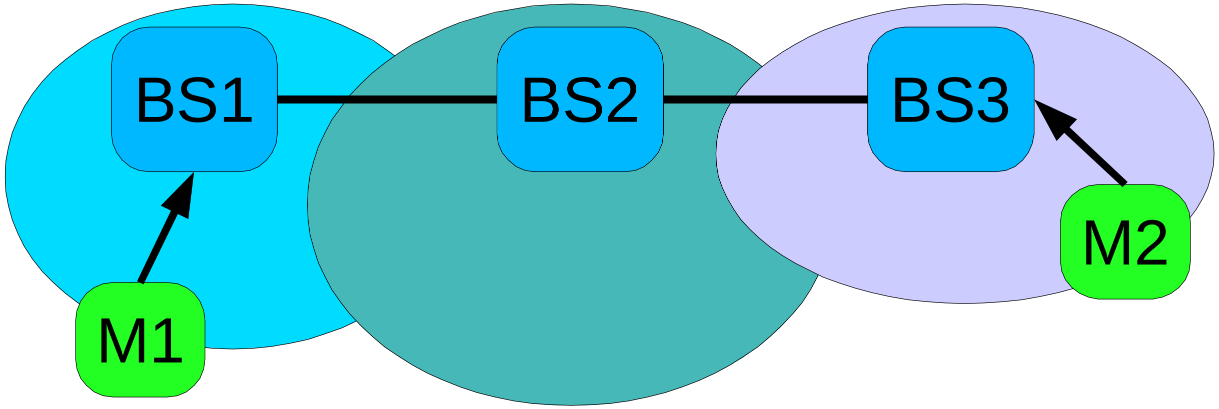
Beacons

- Base stations periodically send out “Here I am”
  - Network name (“SSID”): “CMU”
  - Base station identifier
- May be disabled in home networks to make “war driving” harder

Probe packets

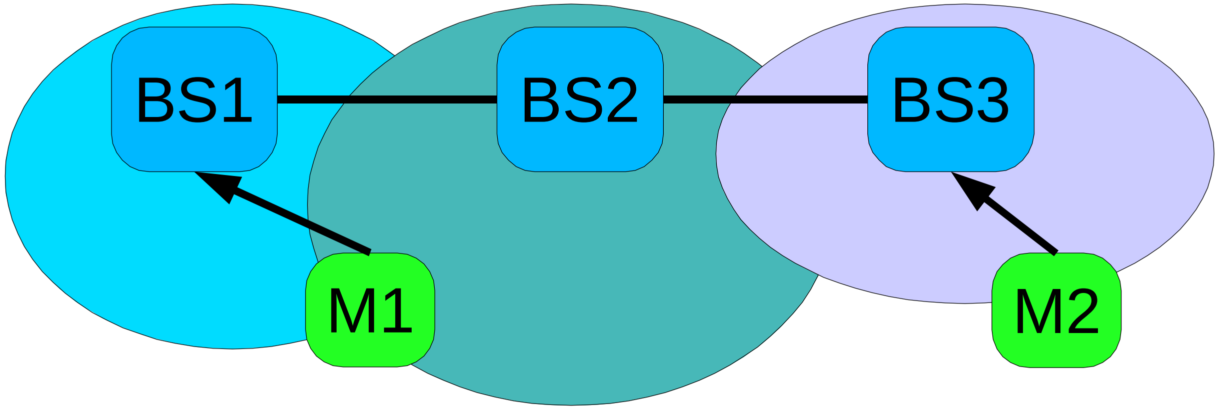
- “Base station ____, are you there?”

Cooperating Base Stations



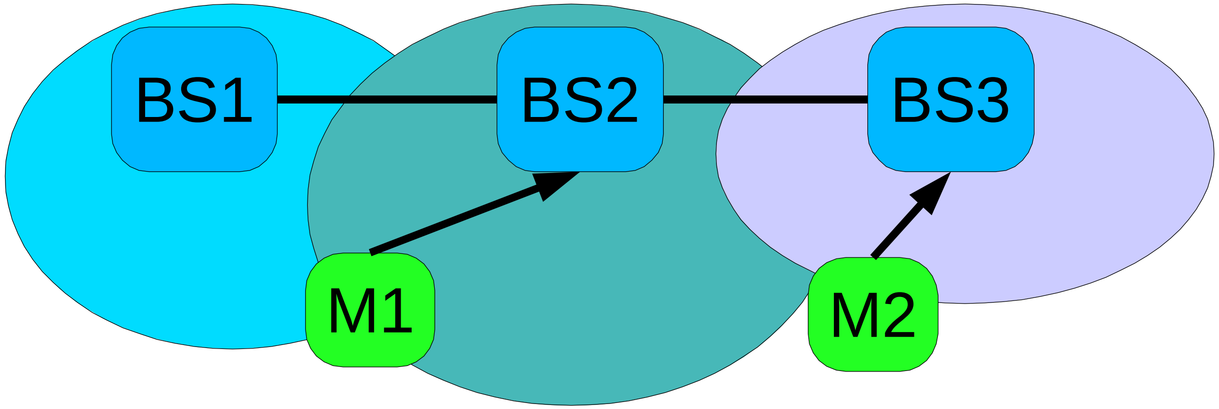
- Periodically sample (passive/active) stations in SS

Cooperating Base Stations



- Periodically sample (passive/active) stations in SS
- If another station looks better to you, move

Cooperating Base Stations

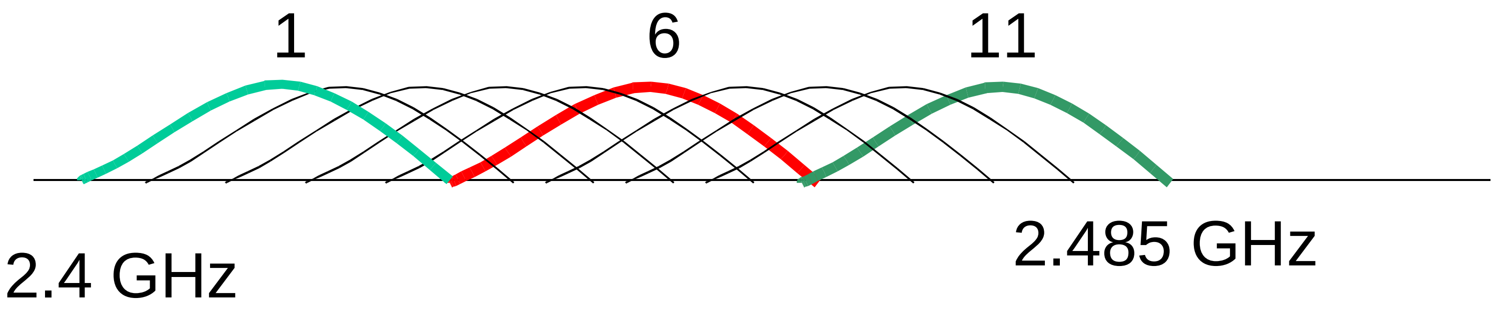


- Periodically sample (passive/active) stations in SS
- If another station looks better to you, move
  - Associating causes new BS to tell others in SS
    - “Joe is over here now”
    - Anybody associated with SS is part of “one big Ethernet” with all others

802.11b

Radio characteristics

- 2.4 GHz ISM band
- Signal is 22 MHz wide
- New limit on output is 4 W EIRP
- Uses 11 chips/bit DSSS – not true CDMA!
  - No need/ability to set a code per card
  - 10.4 dB spreading gain at 2 Mbps
- 11 defined channels in USA
- Only 3 are non-overlapping: 1,6,11



802.11a

Radio characteristics

- 5.1–5.3 GHz NII band
- 8 non-overlapping 20 MHz wide channels
- 40 – 800 mW EIRP (4@40, 4@200, 4@800)
- Uses OFDM – 48 sub-carriers per channel

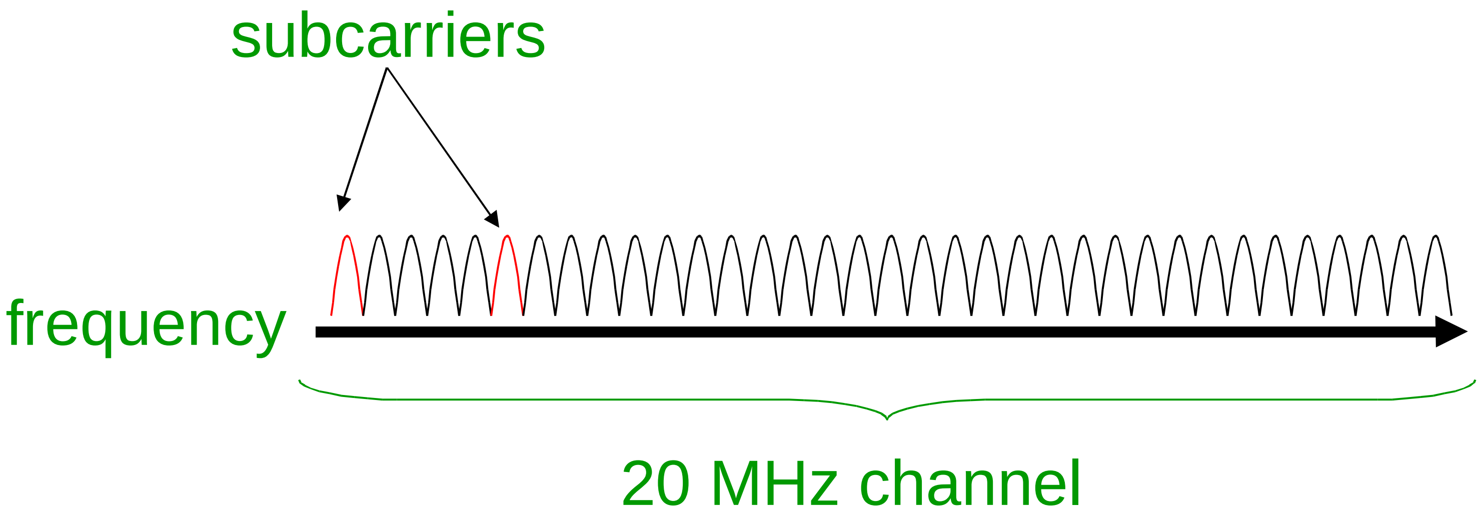
Theoretical: 54Mbps

Real: 20-24 Mbps

OFDM

Orthogonal Frequency Division Multiplexing

- Channel subdivided in subcarriers
- Each subcarrier at a different frequency
- Some see high path loss or noise, some see less
- Send more data over better carriers, less over worse



802.11g

Radio characteristics

- 2.4 GHz ISM band
- Uses OFDM – 52 BPSK sub-carriers

Specification: 54 Mbps

Implementation claims: 108Mbps, 130 Mbps

- Uses multiple channels
- BW severely limited by presence of ***any*** 802.11b nodes

Reality: 20 Mbps to 70 Mbps

Cellular Wide-Area Wireless

Cellular Model of Digital Communication

Completely closed solutions

- Buy it, use it, pay for it
- Variety of bitrates available
- Excellent support for seamless mobility inside service area
- Billing models vary widely (per bit, per QoS, flat with limit)

Generally appears to host computer as point to point link with access server in carrier's network

- Link may require activation before use (like modem link)
- Once activated, generally persistent (like DSL)
- Packet service (host assigned is an IP address)
- Talking with nearby hosts is same as talking across the Internet to remote hosts

Cellular Solutions

1xRRT *(Single Carrier (**1x**) **R**adio **T**ransmission **T**echnology)*

- Theoretical: 144 Kbps, 307 Kbps
- CDMA 3G technology
- Offered by Sprint, Verizon

EDGE

- Theoretical: 384 Kbps
- Real: 130 Kbps peak download, 30 Kbps upload
- GSM 2.5 technology
- Offered by Cingular, ATT Wireless

Cellular Solutions-2

1xEV-DO (1x Evolution Data Optimized)

- CDMA2000 3G Standard (TIA/EIA/IS-856)
- Theoretical: 2.4 Mbps Peak Download Speed
- 1.25 MHz channels in licensed spectrum
- 5-15 Km typical cell radius
- Fully mobile, claims no line-of-sight required
- Clear migration path from IS-95 and 1xRTT
- Over 4 million subscribers worldwide as of Jan 2004

BlueTooth

Bluetooth Overview

Current version 1.2, November 2003

Useful range: typically < 5m

Used in 1000s of different devices

- PDAs
- Phone headsets
- Laptops
- Printers
- Cell phones

Bluetooth Goals

"Cable replacement"

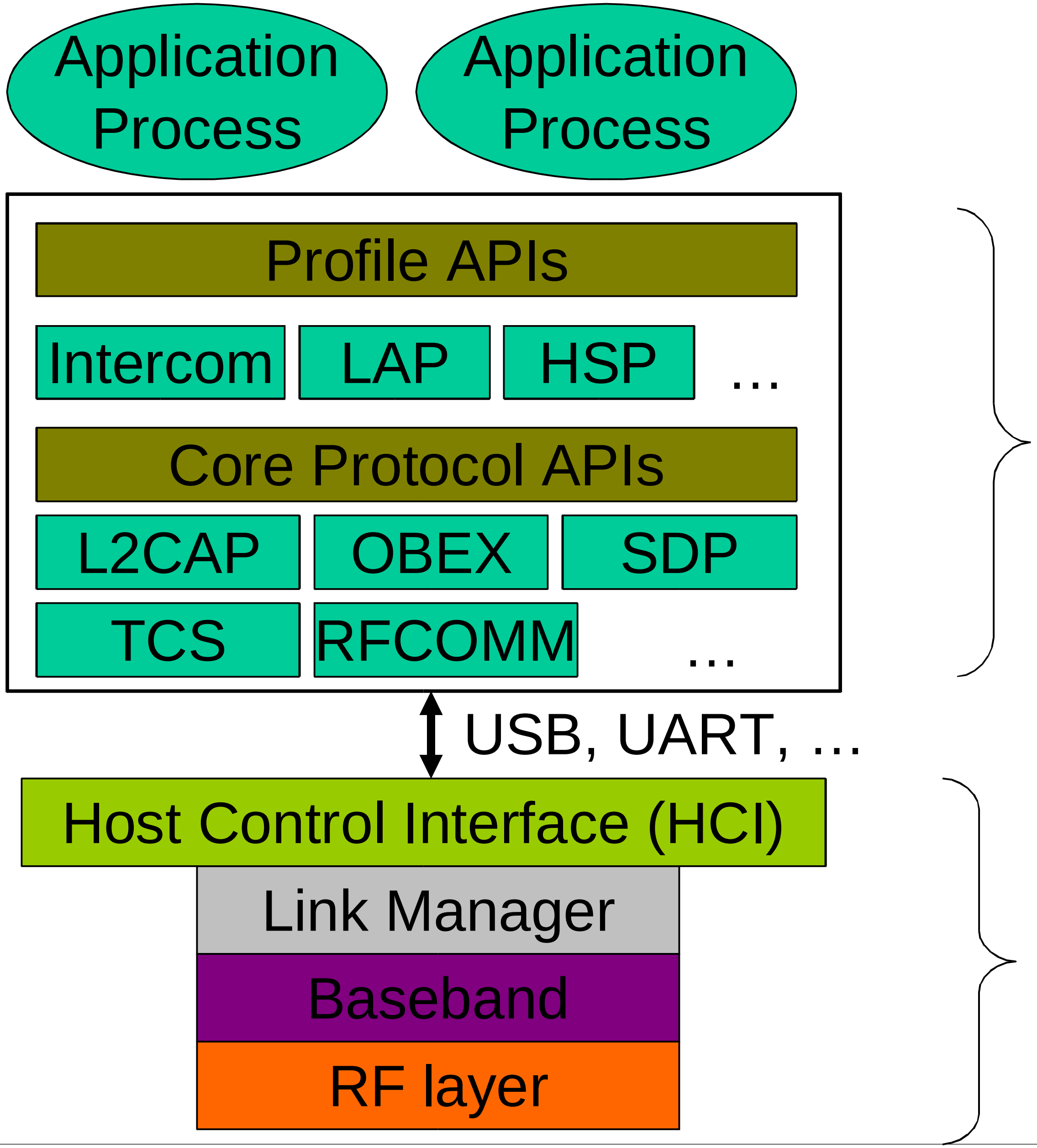
- Synchronize PDA to PC
- Print to a printer in the same room

"Personal Area Networking"

- Phone in pocket, headset on head
- Phone in pocket, car's built-in audio
  - Including: phone rings, radio mutes

"Low price for the right performance"

Bluetooth Architecture



Software - usually in host’s kernel

Hardware - single chip

Overview of RF/Baseband

Frequency-hopping among 79 1MHz channels

- Hops across entire 2.4GHz ISM band
- Adaptive-hopping in v1.2 may reduce conflict with 802.11b/g networks

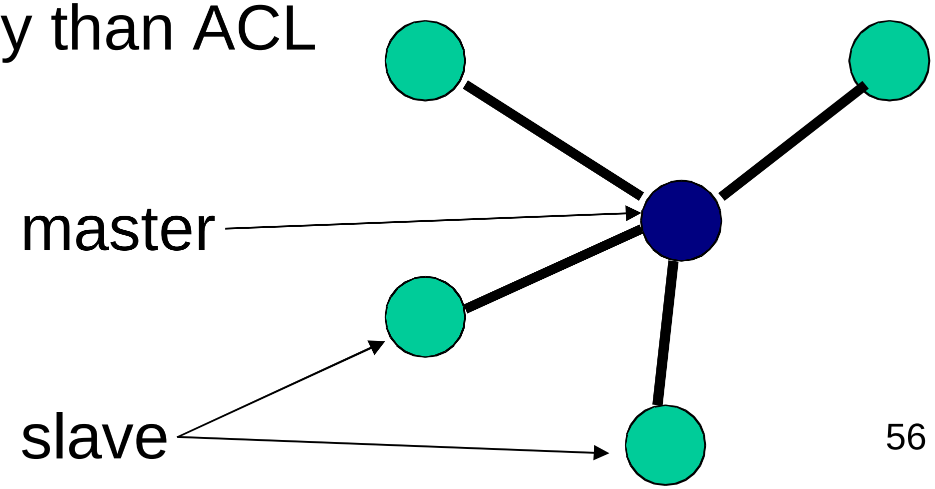
Raw data rate is 1 Mbps

- 625 µs per slot, 1 slot per hop
- 366 bits/slot (30 bytes/slot)
- Uses robust/simple Gaussian Frequency Shift Keying (GFSK)
- Receiver sensitivity generally lower than 802.11 (-70 to -80 dBm compared to -90dBm)

Overview of Link Manager Functions

Connects a master to up to 7 slaves (mostly…)

- Support for both packet and CBR data
  - Asynchronous connection-oriented (ACL)
  - Synchronous connection-oriented (SCO)
- No support for slave-to-slave communication
  - Must relay data through software on host
- Handling voice a primary focus
  - SCO higher priority than ACL



Piconet Construction

Step 1: ***Inquiry***

- Master scans looking for devices in range
- Potential slaves wait to be noticed
- Both master and slaves must be explicitly set to inquiry-master or inquiry-slave state
- Application or profile must assign roles

Step 2: ***Paging***

- Master invites desired slaves to join piconet
- Typically, exchange of authentication (PIN) leads to ***pairing***

Link Performance

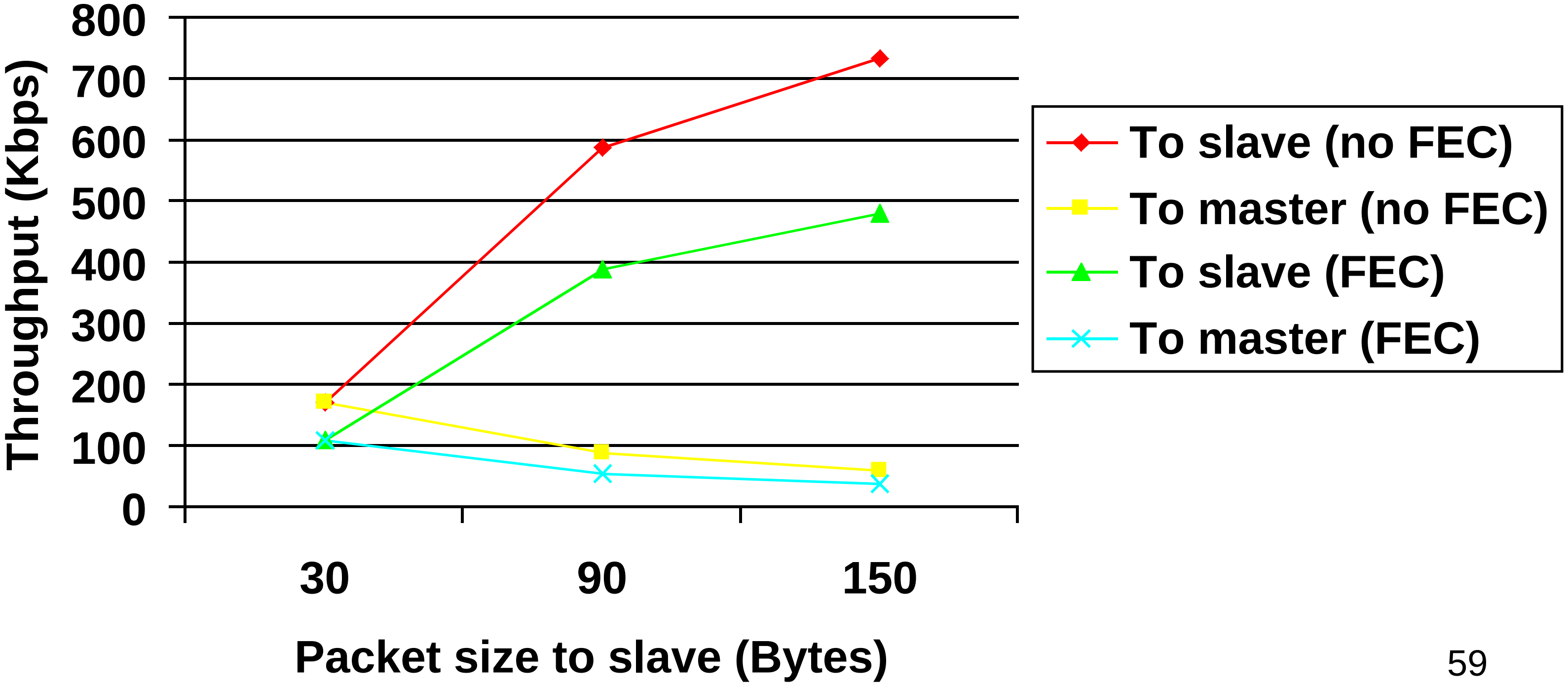
Synchronous Links (SCO)

- Supports 1 to 3 PCM (64kbps) full-duplex voice connections per piconet (POTS quality)
- Speech coder generates 10B/1.25ms
- 3 levels of FEC level available (chosen by user, not LMP)
- HV1 (max FEC) full-duplex SCO uses entire capacity of piconet
  - 10B of speech, 20B of FEC in each packet

Link Performance

Asynchronous Link (ACL)

- Master sends 30, 90 or 150B at a time
- Slave polled for 30 B at a time
- Strongly asymmetric throughput
- Change master if needed!



Overview of Service Model

Core Protocols built on HCI and LMP

- ***SDP*** – service discovery protocol
- ***L2CAP*** – segmentation and reassembly
- ***RFCOMM*** – RS-323 emulation
- ***TCS*** – telephone communication service
- ***OBEX*** – object exchange

Profiles built on top of connection primitives

- Specify parameters for low-level transport
- More than 13 defined
  - Generic access, Intercom, Serial Port, Headset, Dial-up networking, LAN Access,…

Overview of Application APIs

Not specified by Bluetooth = dependent on software stack implementer

BlueZ Stack for Linux is popular

- http://www.bluez.org

Berkeley Sockets API

- HCI raw socket
- L2CAP socket for datagram
- SCO sockets for sequential packets

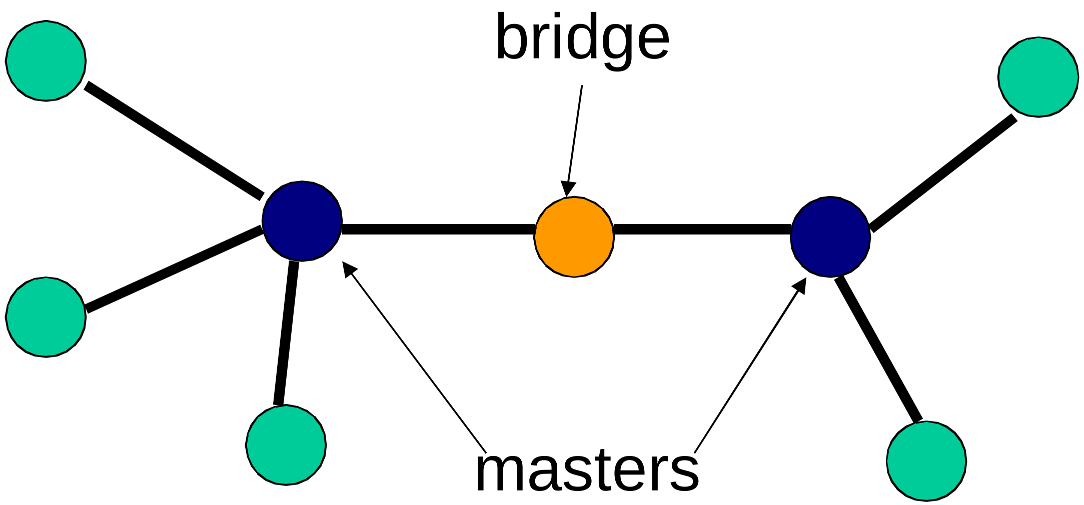
Library API for common tasks

- Bluetooth address processing
- HCI setup/configuration

Scatternets

Building a multi-hop network with Bluetooth

- A master or slave acts as ***bridge node***
- Forwards data between piconets



Scatternets – 2

Connecting multiple piconets together into a scatternet remains a research topic

- ***Bridge node*** must participate in two piconets simultaneously
- Hard real-time requirement to track clock drift of both masters
- Where to implement?
  - Host stack software? (current implementation)
  - Core Bluetooth stack below HCI (???)

ZigBee – IEEE 802.15.4

ZigBee???

What's a “ZigBee”?

- “Wireless Control That Simply Works”
- Low-power, low-data-rate sensor/control nodes
  - Heating/cooling, medical monitoring
  - Inter-smoke-alarm networks
  - Security
  - Curtain open/close
- Plan: many nodes/network, self-organizing

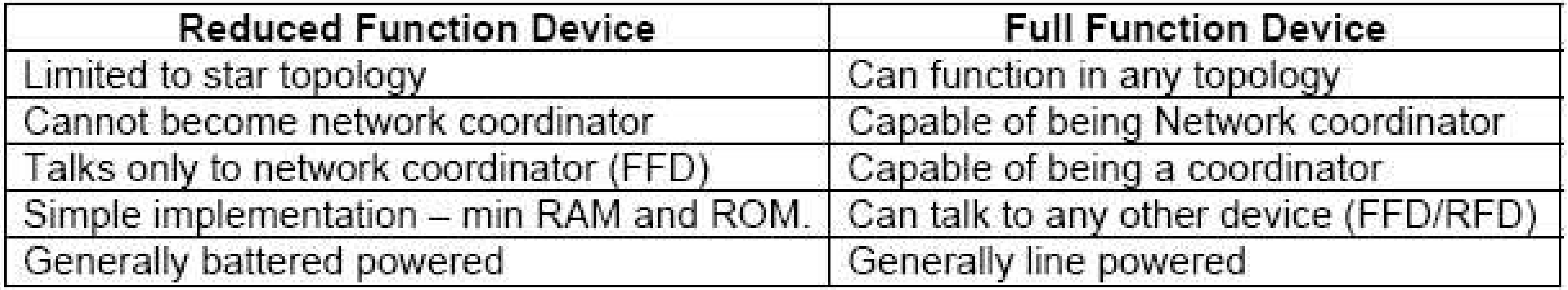
“ZigBee”

What's a “ZigBee”?

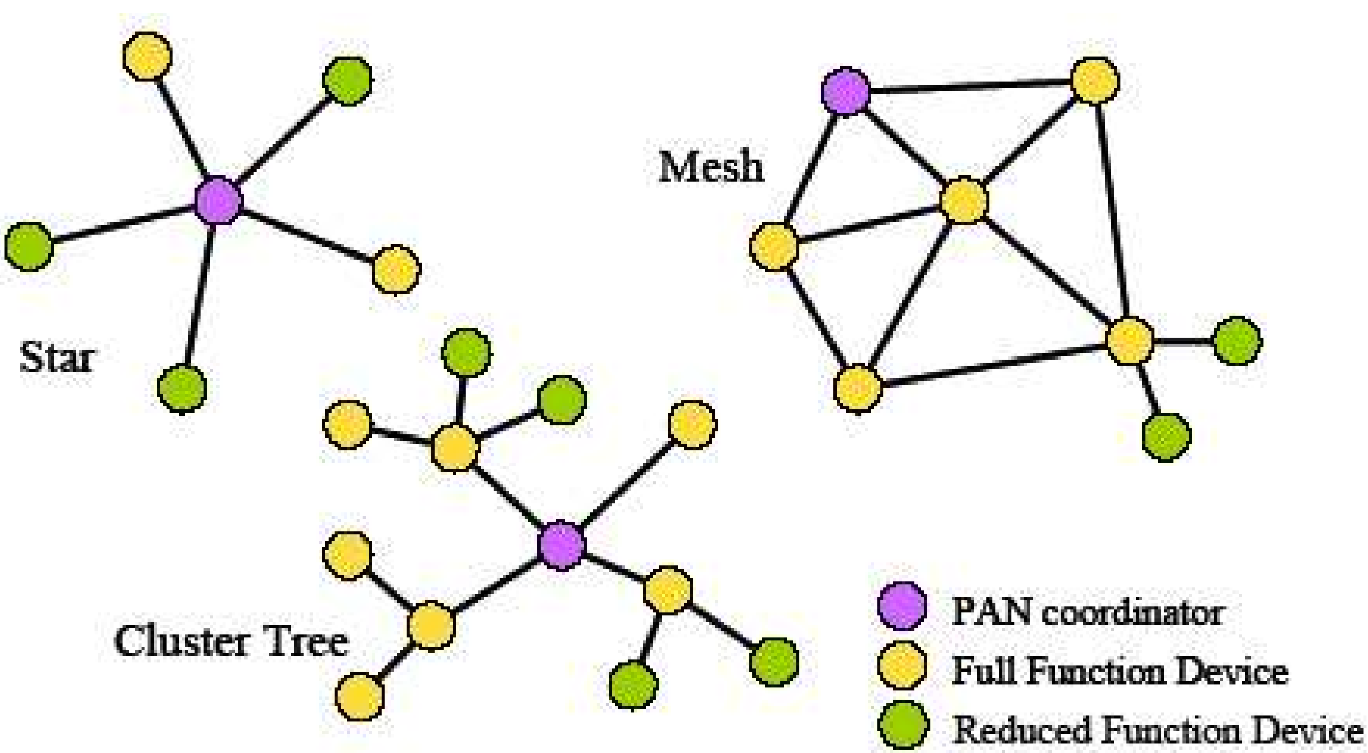
- “The technique that honey bees use to communicate new-found food sources to other members of the colony is referred to as the ZigBee Principle.”
- Uh-huh

Usage Model

Not typically an IP Network



Reduced Function Device	Full Function Device
Limited to star topology	Can function in any topology
Cannot become network coordinator	Capable of being Network coordinator
Talks only to network coordinator (FFD)	Capable of being a coordinator
Simple implementation – min RAM and ROM.	Can talk to any other device (FFD/RFD)
Generally battered powered	Generally line powered



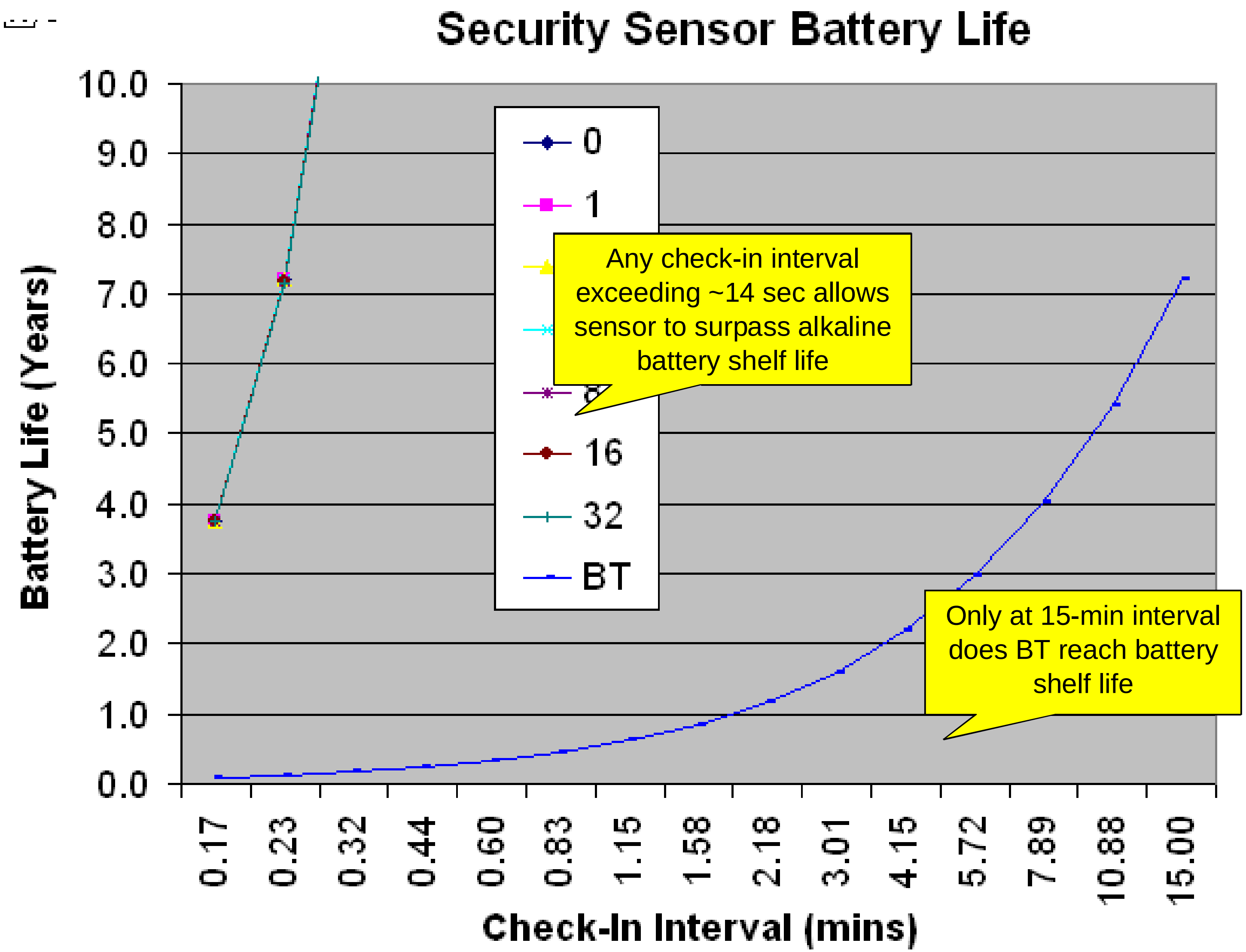
From Craig

Usage Model - 2

Intended for low duty cycle sensor networks

- Node takes 15ms to access channel & send data
- 802.11 node takes < 1ms
- Addresses IEEE 64-bit (not Ethernet style)
- 104 bytes of data per packet
- Up to 2^{64} nodes per network (Bluetooth limited to between 7 and 255)

Bluetooth .vs. ZigBee Power Consumption



Any check-in interval exceeding ~14 sec allows sensor to surpass alkaline battery shelf life

Only at 15-min interval does BT reach battery shelf life

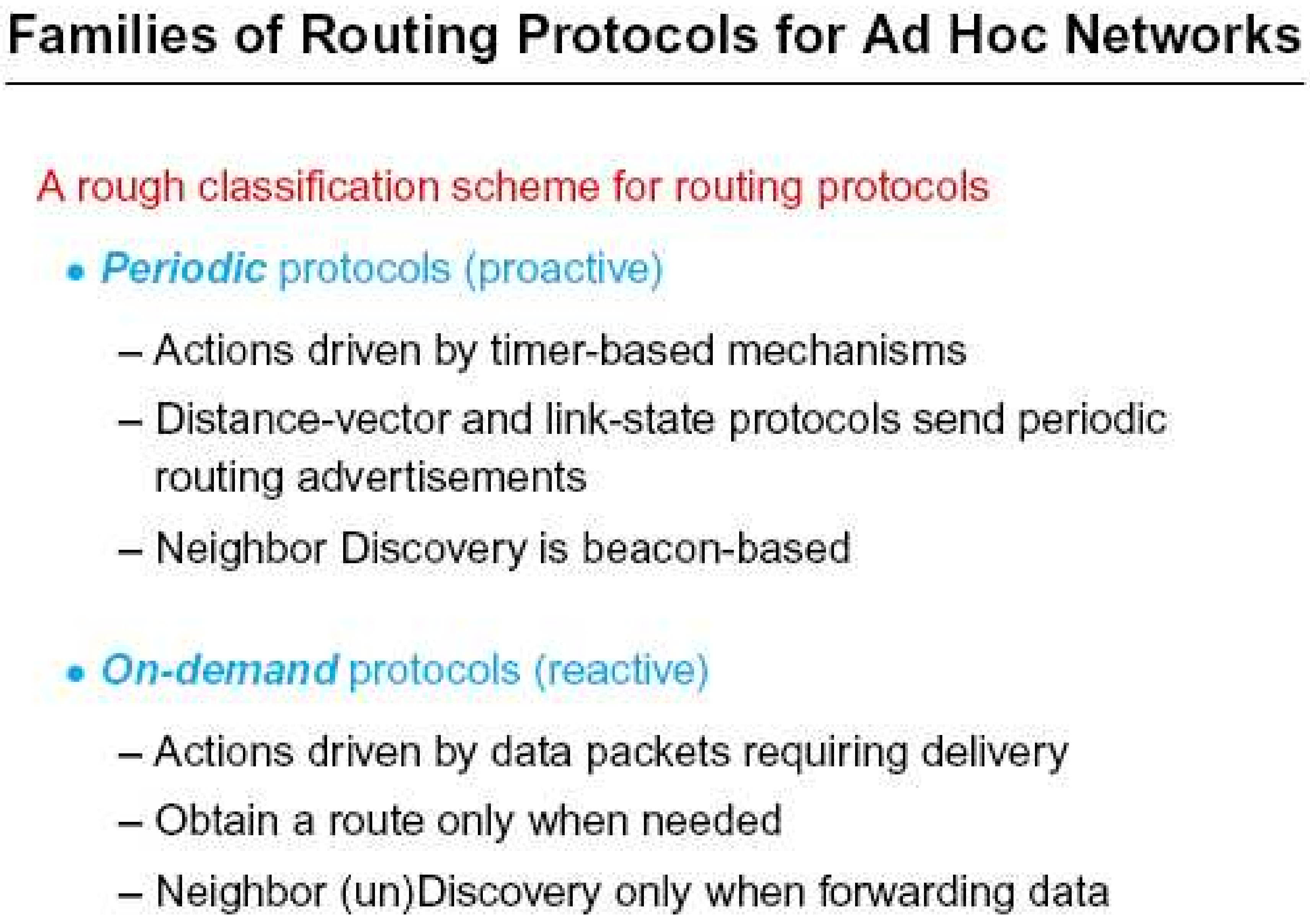
From Adams04

Multi-hop Routing Protocols

Multi-hop Routing Protocols

IETF Mobile Ad Hoc Network Working Group (MANET) protocols:

- Dynamic Source Routing Protocol (DSR)
- Ad Hoc On Demand Distance Vector (AODV)
- Optimized Link State Routing Protocol(OLSR)
- Topology Dissemination Based on Reverse-Path Forwarding (TBRPF)



Families of Routing Protocols for Ad Hoc Networks

A rough classification scheme for routing protocols

- ***Periodic*** protocols (proactive)
  - – Actions driven by timer-based mechanisms
  - – Distance-vector and link-state protocols send periodic routing advertisements
  - – Neighbor Discovery is beacon-based
- ***On-demand*** protocols (reactive)
  - – Actions driven by data packets requiring delivery
  - – Obtain a route only when needed
  - – Neighbor (un)Discovery only when forwarding data

Dynamic Source Routing Protocol (DSR)

David B. Johnson and David A. Maltz (1993 – present)

A completely on-demand protocol based on source routes

Based on source routes

- Packets carry ***source routes*** listing all intermediate hops (can increase data packet size)
- ***No*** routing decisions made by intermediate hops
- Nodes ***ignore*** all topology changes not affecting them
- All routes are trivially ***loop free***
- Node overhearing source routes ***learn network topology***

Dynamic Source Routing Protocol (DSR) - 2

Completely on-demand

- Eliminates ***all*** periodic routing packets
- ***Zero*** overhead when stationary and routes already found
- ***Dynamically*** adjusts overhead to level of topology change

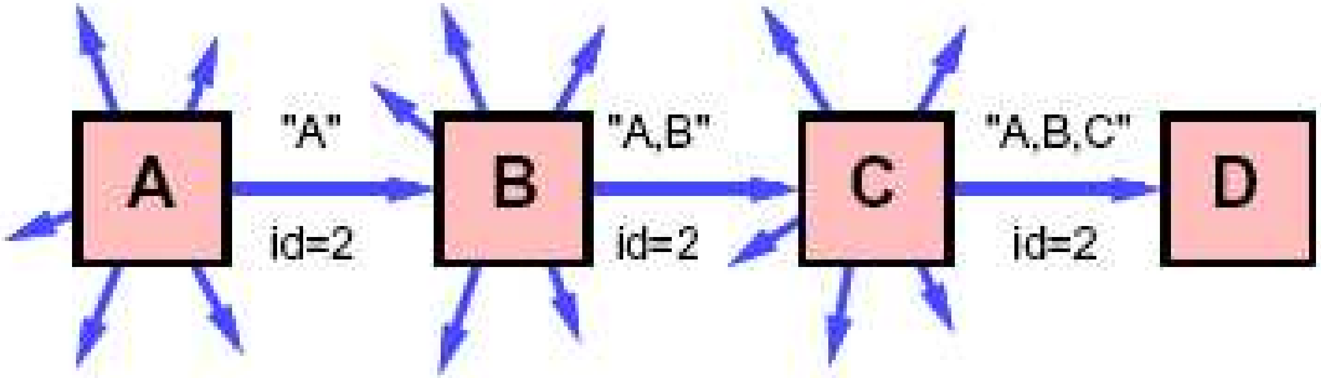
Each node keeps a ***Route Cache*** of known routes

- ***Agressively*** used to reduce cost of Route Discovery
- Nodes can answer Route Discoveries using cached routes
- Caching philosophy is ***optimistic***: stale data cleared as needed
- Can store multiple routes to same node

Route Discovery in DSR

To discover a route to some destination:

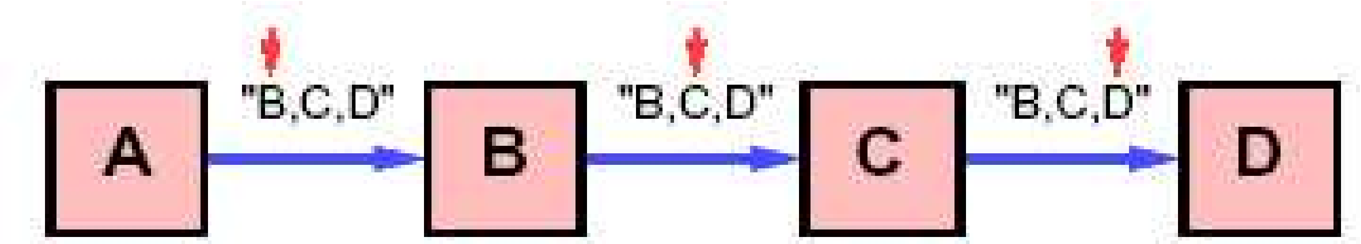
- Ask neighbors for route with ***nonpropagating*** Route Request
- Flood fill a ***propagating*** Route Request
- Target returns each discovered path as Route Reply
- Nodes with a cached route generally reply themselves
- Nodes overhearing the Request or Reply learn the routes



Route Maintenance in DSR

Each forwarding nodes verifies receipt by next hop

- Listen for link-level per-hop acknowledgement, or
- Listen for that node sending packet to its next hop (passive acknowledgement), or
- Set bit in packet to request explicit acknowledgement



When problem detected:

- Send Route Error to original sender, describing broken link
- Salvage packet with alternate route, if already known
- Sender removes link from cache, performs new discovery if needed

DSR Summary and Comments

Summary

- DSR is a purely on-demand protocol
- Uses source routes – permits lots of control
- Route caches used to reduce overhead

Comments

- Provides internetworking support and QoS (not described today)
- Relatively low overhead protocol
- Searching for unreachable nodes is expensive
  - Must search repeatedly in case they become reachable

Summary

“Wireless” isn't one thing

- Few nodes or many
- Short range or long
- High-speed or low
- Infrastructure, ad-hoc, cooperating group

Open issues at all levels

- Error coding, control
- Power management
- Security
- Routing, organization

Summary – 2

Know the main issues

- Fuzzy boundaries
- Noise/errors
- Hidden-terminal/exposed-terminal
- What to do about “carrier sensing”
- Infrastructure, ad-hoc, cooperating group

References (802.11)

- **IEEE 802.11 Standards** http://standards.ieee.org/getieee802/802.11.html
- **Direct Sequence Spread Spectrum - Physical Layer Specification, IEEE 802.11**, Jan Boer - Chair DS PHY, Lucent Technologies WCND Utrecht, http://grouper.ieee.org/groups/802/11/Tutorial/ds.pdf
- **Anatomy of IEEE 802.11b Wireless**, Joel Conover http://www.networkcomputing.com/1115/1115ws2.html
- **Link-level Measurements from an 802.11b Mesh Network**, Daniel Aguayo, John Bicket, Sanjit Biswas, Glenn Judd, Robert Morris, *SIGCOMM'04*

References – Bluetooth

General:

- https://www.bluetooth.org/spec/
- http://www.winlab.rutgers.edu/~pravin/bluetooth/
- **Bluetooth: Technology for Short-Range Wireless Apps**. Pravin Bhagwat. *IEEE Internet Computing, Vol. 5, No. 3, May-June 2001*

Implementation:

- **Bluetooth programming for Linux** Marcel Holtmann, Andreas Vedral http://www.holtmann.org/papers/bluetooth/wtc2003_slides.pdf
- **BCM2035 Single Chip Bluetooth solution Datasheet** **http://www.broadcom.com/collateral/pb/2035-PB01-R.pdf**

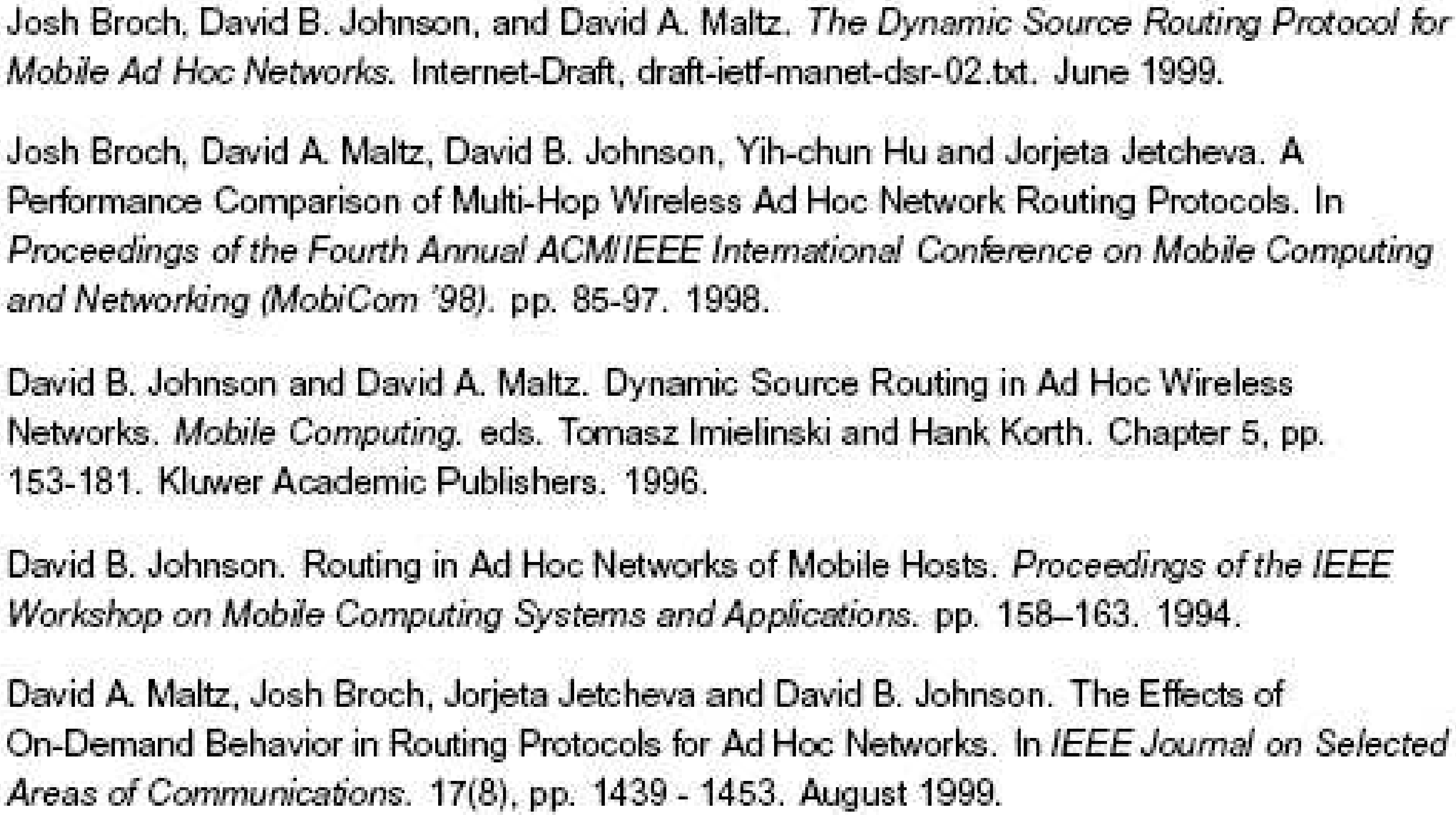
Scatternets:

- **A routing vector method (RVM) for routing in Bluetooth scatternets**. Pravin Bhagwat, Adrian Segall. *The Sixth IEEE International Workshop on Mobile Multimedia Communications (MOMUC'99), Nov 1999.*
- **Distributed topology construction of Bluetooth personal area networks**. T. Salonidis, P. Bhagwat, L. Tassiulas, R. LaMaire. *Infocom 2001.*
- **Scatternet - Part 1, Baseband vs. Host Stack Implementation** *Ericsson Technology Licensing, June 2004.*

References – ZigBee

- http://zigbee.org/
  - **Designing with 802.15.4 and ZigBee,** Jon Adams, 2004. http://zigbee.org/resources/documents/IWAS_presentation_Mar04_Designing_with_802154_and_zigbee.ppt
  - **Zigbee: “Wireless Control That Simply Works”,** William C. Craig. http://zigbee.org/resources/documents/2004_ZigBee_CDC-P810_Craig_Paper.pdf
  - **Home networking with IEEE 802.15.4: a developing standard for low-rate wireless personal area networks**
    Callaway, E.; Gorday, P.; Hester, L.; Gutierrez, J.A.; Naeve, M.; Heile, B.; Bahl, V. C*ommunications Magazine, IEEE ,* 40(8), Aug. pp.70 – 77, 2002.

References – DSR



Josh Broch, David B. Johnson, and David A. Maltz. *The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks.* Internet-Draft, draft-ietf-manet-dsr-02.txt. June 1999.

Josh Broch, David A. Maltz, David B. Johnson, Yih-chun Hu and Jorjeta Jetcheva. A Performance Comparison of Multi-Hop Wireless Ad Hoc Network Routing Protocols. In *Proceedings of the Fourth Annual ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom '98).* pp. 85-97. 1998.

David B. Johnson and David A. Maltz. Dynamic Source Routing in Ad Hoc Wireless Networks. *Mobile Computing.* eds. Tomasz Imielinski and Hank Korth. Chapter 5, pp. 153-181. Kluwer Academic Publishers. 1996.

David B. Johnson. Routing in Ad Hoc Networks of Mobile Hosts. *Proceedings of the IEEE Workshop on Mobile Computing Systems and Applications.* pp. 158–163. 1994.

David A. Maltz, Josh Broch, Jorjeta Jetcheva and David B. Johnson. The Effects of On-Demand Behavior in Routing Protocols for Ad Hoc Networks. In *IEEE Journal on Selected Areas of Communications.* 17(8), pp. 1439 - 1453. August 1999.