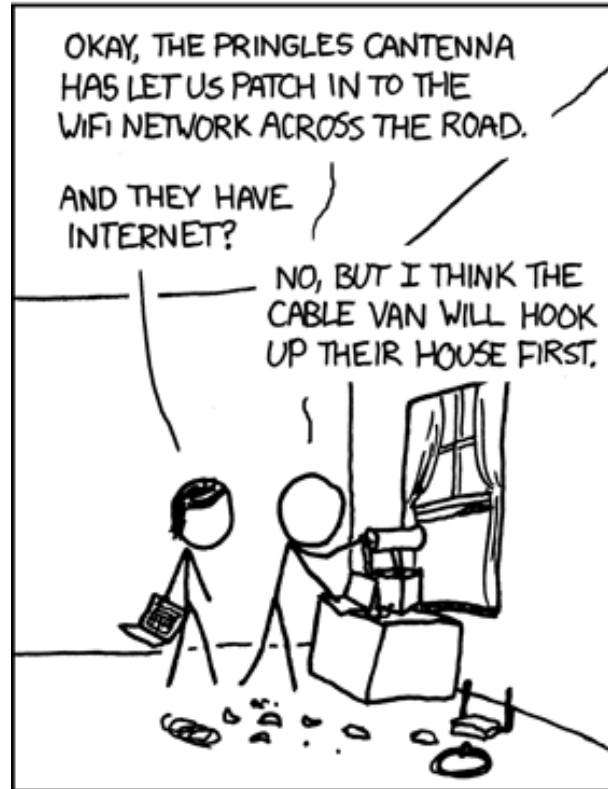


# Wireless LANs, 802.11

THERE ARE FEW FORCES MORE POWERFUL THAN GEEKS DESPERATELY TRYING TO GET INTERNET IN A NEW APARTMENT.



<http://xkcd.com/466/>

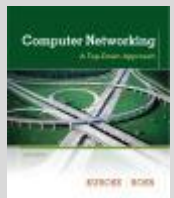
*Computer Networking: A Top Down Approach*

6<sup>th</sup> edition

Jim Kurose, Keith Ross

Addison-Wesley

Some materials copyright 1996-2012  
J.F Kurose and K.W. Ross, All Rights Reserved



# Wireless and mobile networks

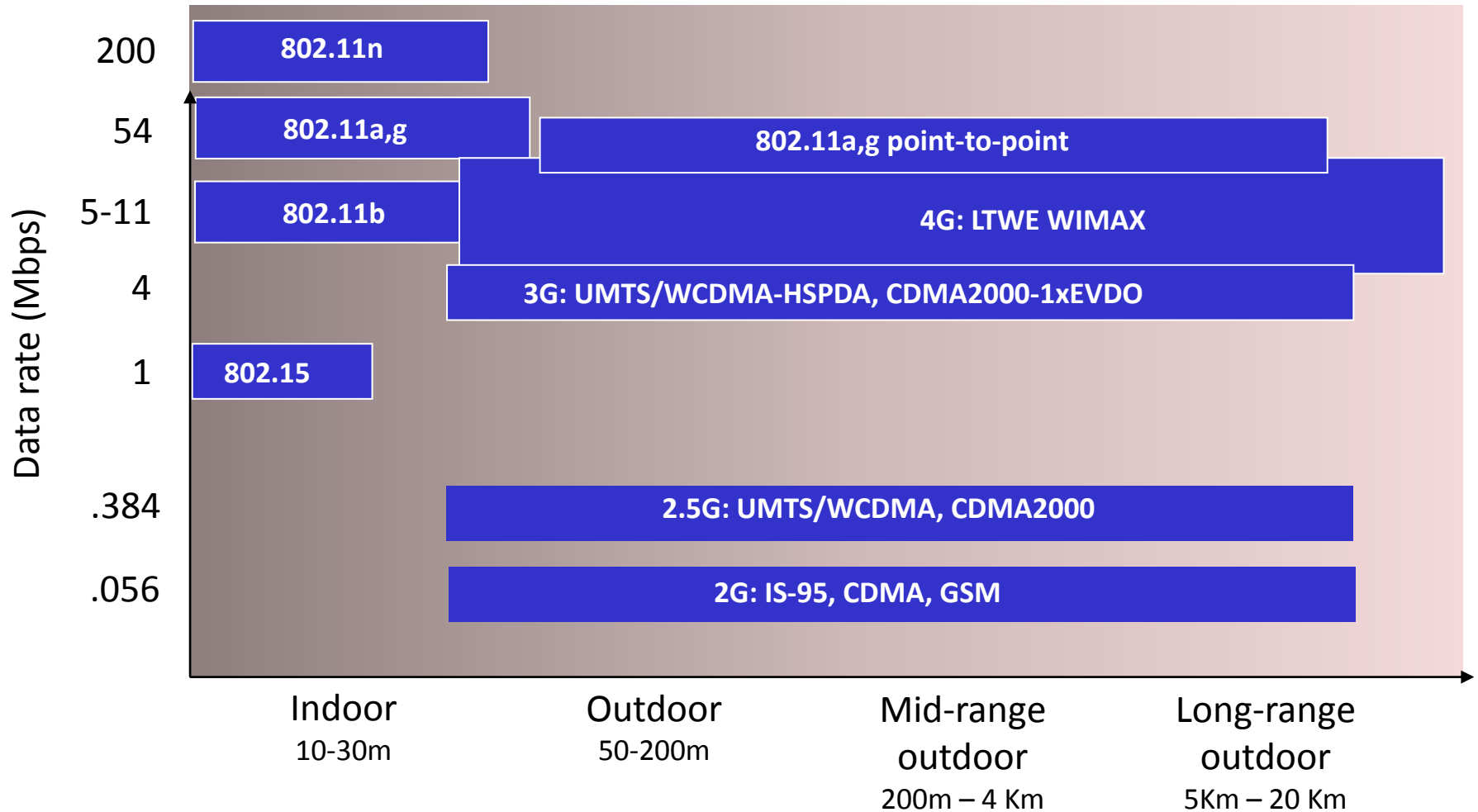
## Background:

- ❖ # 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

# Wireless

- Shared medium using wireless
  - Bit errors more prevalent than wired
  - Limits on transmit power
    - Battery life, government regulation
  - Difficult to transmit and listen for collisions
  - Undirected signal
    - Interference
    - Security

# Wireless technologies

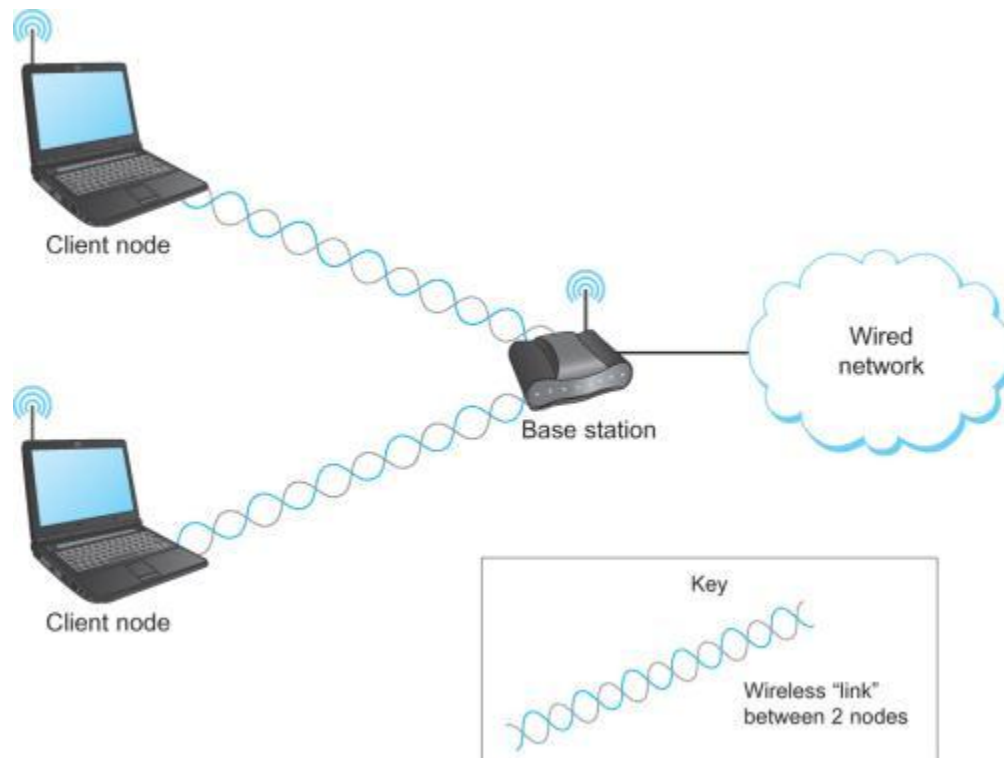


# Wireless technologies

	Link length	Data rate	Uses
RFID	10 m	Very low	Smart cards, pet implants, passports, library books
Bluetooth 802.15.1	10 m	2 Mbps	Link peripheral to computer (e.g. headset, mouse, keyboard).
Wi-Fi 802.11	100 m	11-600 Mbps	Link computer to a wired base station.
3G Cellular	10 km	Hundreds of kbps (per connection)	Link mobile device to wired tower.
Wi-MAX 802.16	50 km	144 Mbps	Last-mile broadband to home. Mobile broadband.

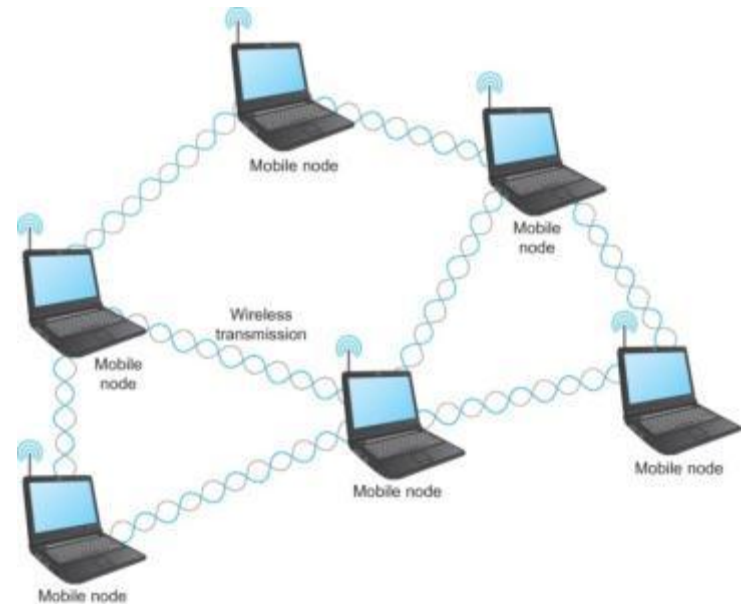
# Wireless topology

- Base station topology
  - Typically all clients talk to base station
  - No direct communication between clients
  - *Infrastructure mode*



# Wireless topology

- Ad hoc / mesh topology
  - Nodes are peers
  - No special base station
  - Advantages:
    - More **fault tolerant**
    - **Extends range**
  - Disadvantages:
    - **Nodes are more complex**
    - Nodes may be asked to **expend limited resources** (e.g. power)



One Laptop per Child, uses  
802.11s mesh draft standard.

# Wireless link characteristics

*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)

– *Multipath propagation:*

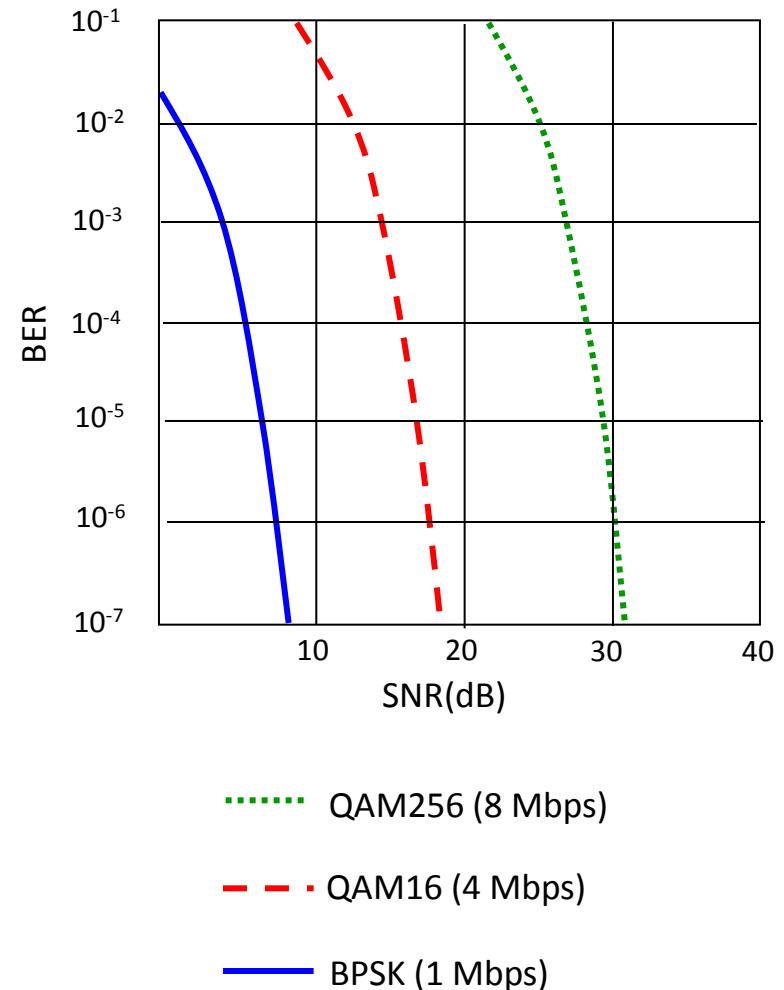
- Radio signal reflects off objects ground, arriving at destination at slightly different times

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



# Wireless link characteristics

- SNR: signal-to-noise ratio
  - Larger SNR, easier to extract signal from noise
- *SNR versus BER tradeoffs*
  - *Given physical layer:* Increase power, increase SNR, decrease BER
  - *Given SNR:* Choose physical layer that meets BER requirement, giving highest throughput
    - SNR may change with mobility: dynamically adapt physical layer (modulation technique, rate)

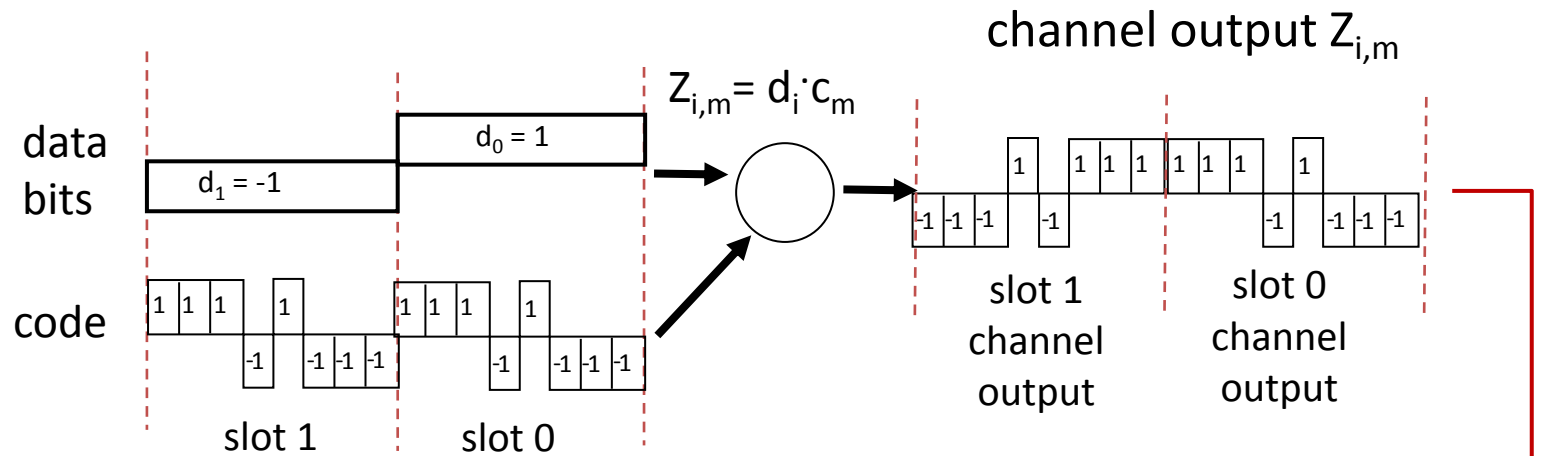


# Code Division Multiple Access (CDMA)

- 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

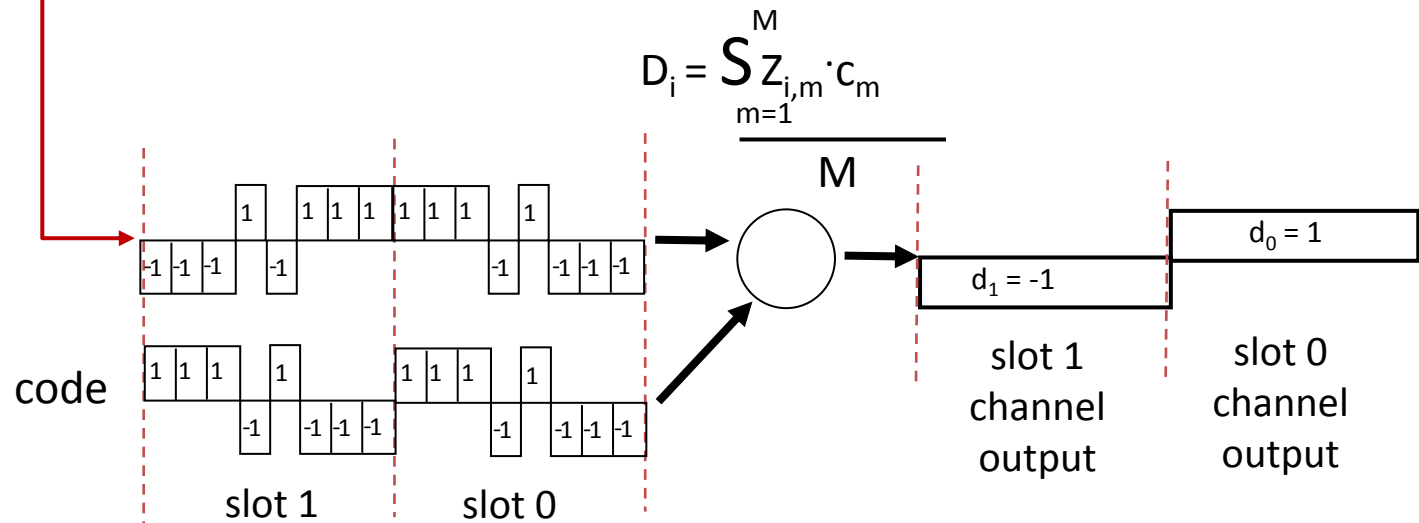
# CDMA encode/decode

sender



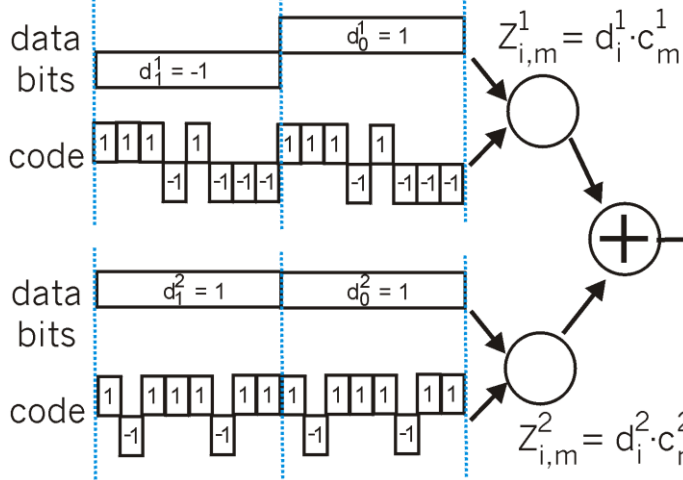
received input

receiver



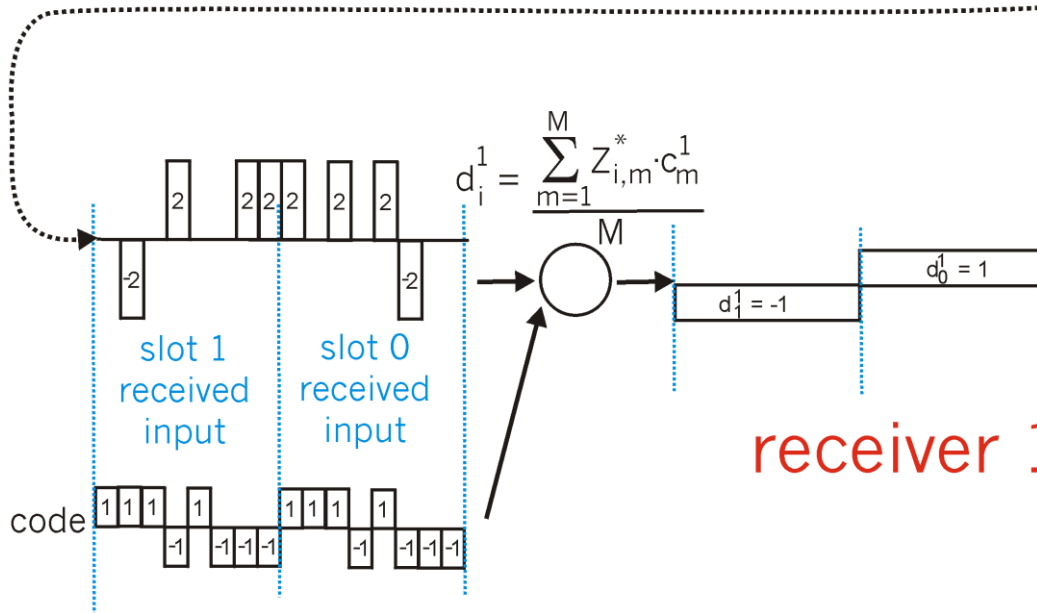
# CDMA: two-sender interference

senders



channel,  $Z_{i,m}^*$

*Channel sums together transmissions by sender 1 and 2*



*Using same code as sender 1, receiver recovers sender 1's original data from summed channel data!*

# 802.11 Wi-Fi

Standard	Released	Max bit rate (shared)	Frequency band	Indoor range
802.11	1997	2 Mbps	2.4 GHz	20 m
802.11a	1999	54 Mbps	5 GHz	35 m
802.11b	1999	11 Mbps	2.4 GHz	38 m
802.11g	2003	54 Mbps	2.4 GHz	38 m
802.11n	2009	600 Mbps	2.4 GHz 5 GHz	70 m

- Operate in **license exempt** bands
- **More absorption at high frequencies** (5 GHz)
- All **support lower bit rates**
  - Switch between modulation techniques & error correction codes
- 802.11n, **multiple antennas**
  - **MIMO** (Multiple Input Multiple Output)

# 802.11 collision avoidance

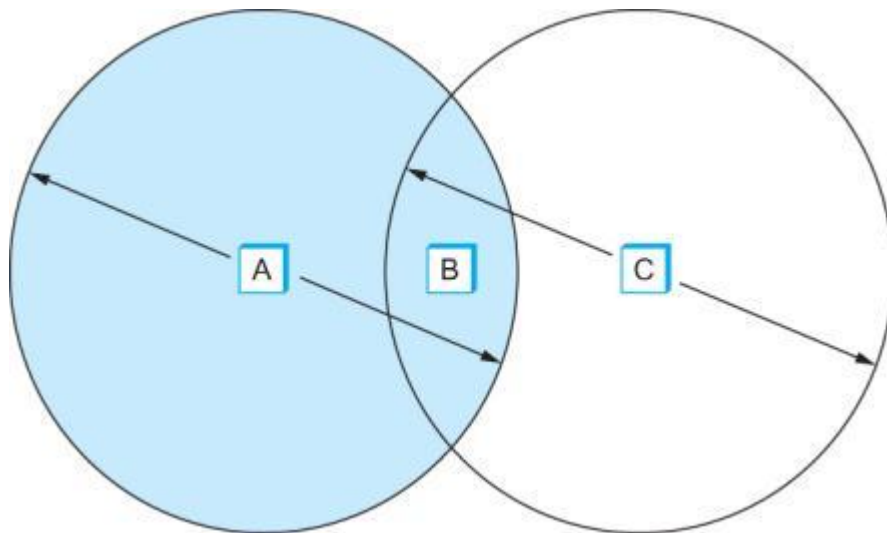
- Collision avoidance

- Can't transmit and listen for collision

- Transmission power swamps receiving circuit
    - Collision detection (CD) as in Ethernet not possible

- Not everyone can hear everything

- Hidden node problem:



A and C both want to send to B.

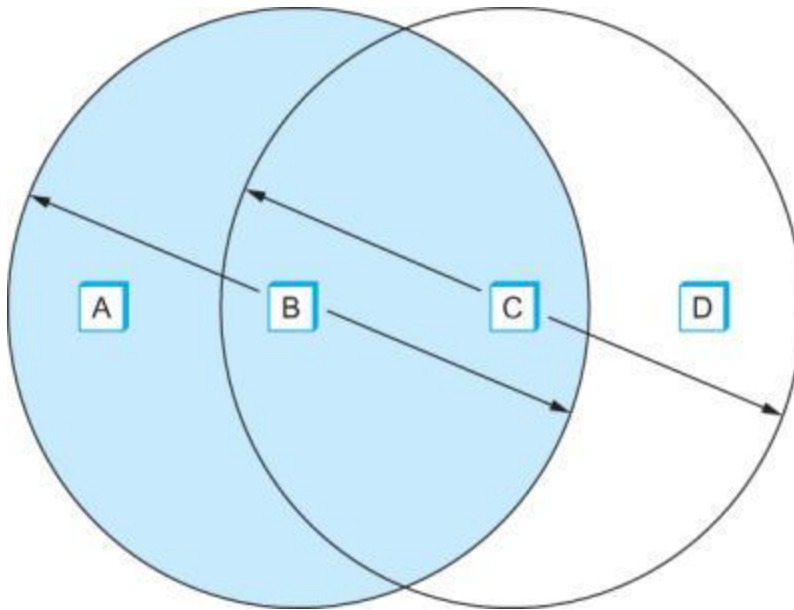
A and C can't hear each other so can't detect their transmissions collided.

# 802.11 collision avoidance

- Collision avoidance

- Lack of global info about who is in range of who

- Exposed node problem:



C wants to send to D.

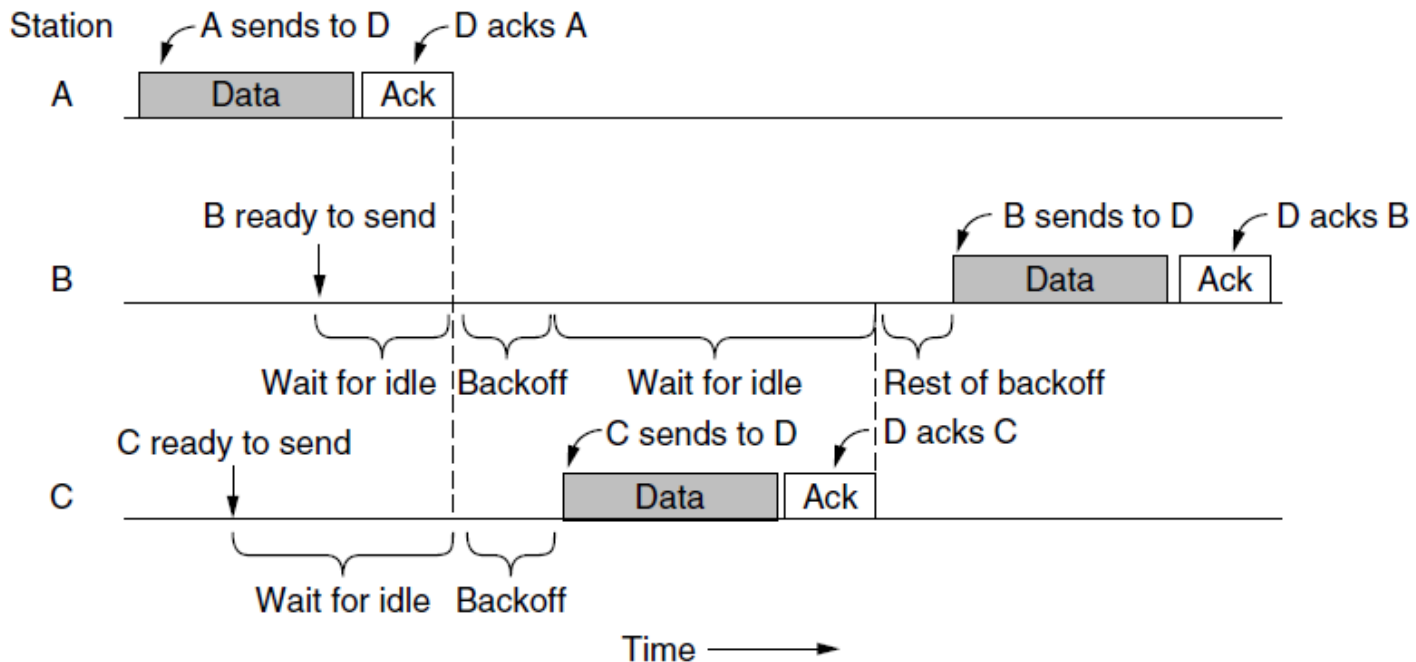
But C can hear B transmitting to A.  
But D cannot hear B,  
and A cannot hear C.

So C could safely transmit to D.

# CSMA w/ Collision Avoidance

- CSMA/CA

- Don't send if you hear transmission
- If you sent recently, don't be greedy
  - Use random backoff
- **Explicit ACK** from receiver to sender
  - Exponential backoff if bad/missing ACK





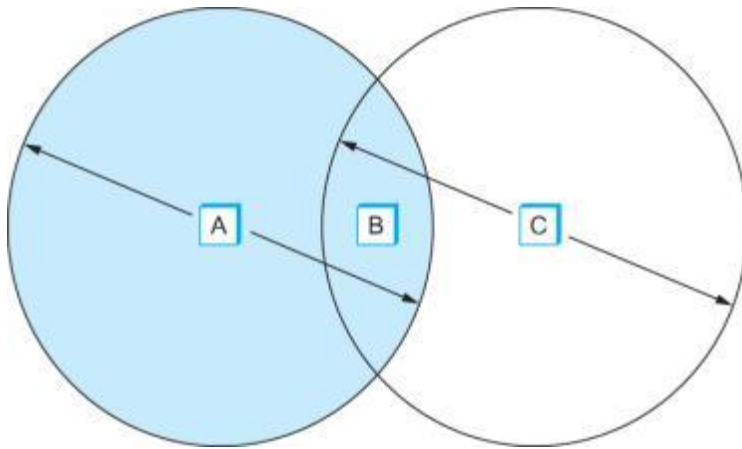
# Ready to Send-Clear to Send

- Ready to Send-Clear to Send
  - Optional RTS-CTS protocol:
    - Exchange control frames before transmission
    - Informs nearby nodes about planned transmission
    - Request to Send (RTS)
      - Transmitter: "I want to send a frame of this length"
    - Clear to Send (CTS)
      - Receiver: "Okay, you're the man, send the data"
    - One-side usually an access point
      - Clients can hear either the RTS or CTS
      - Other clients stay off the air until after ACK

# Ready to Send-Clear to Send

- RTS-CTS

- Helps address hidden node problem:



A wants to send to B.

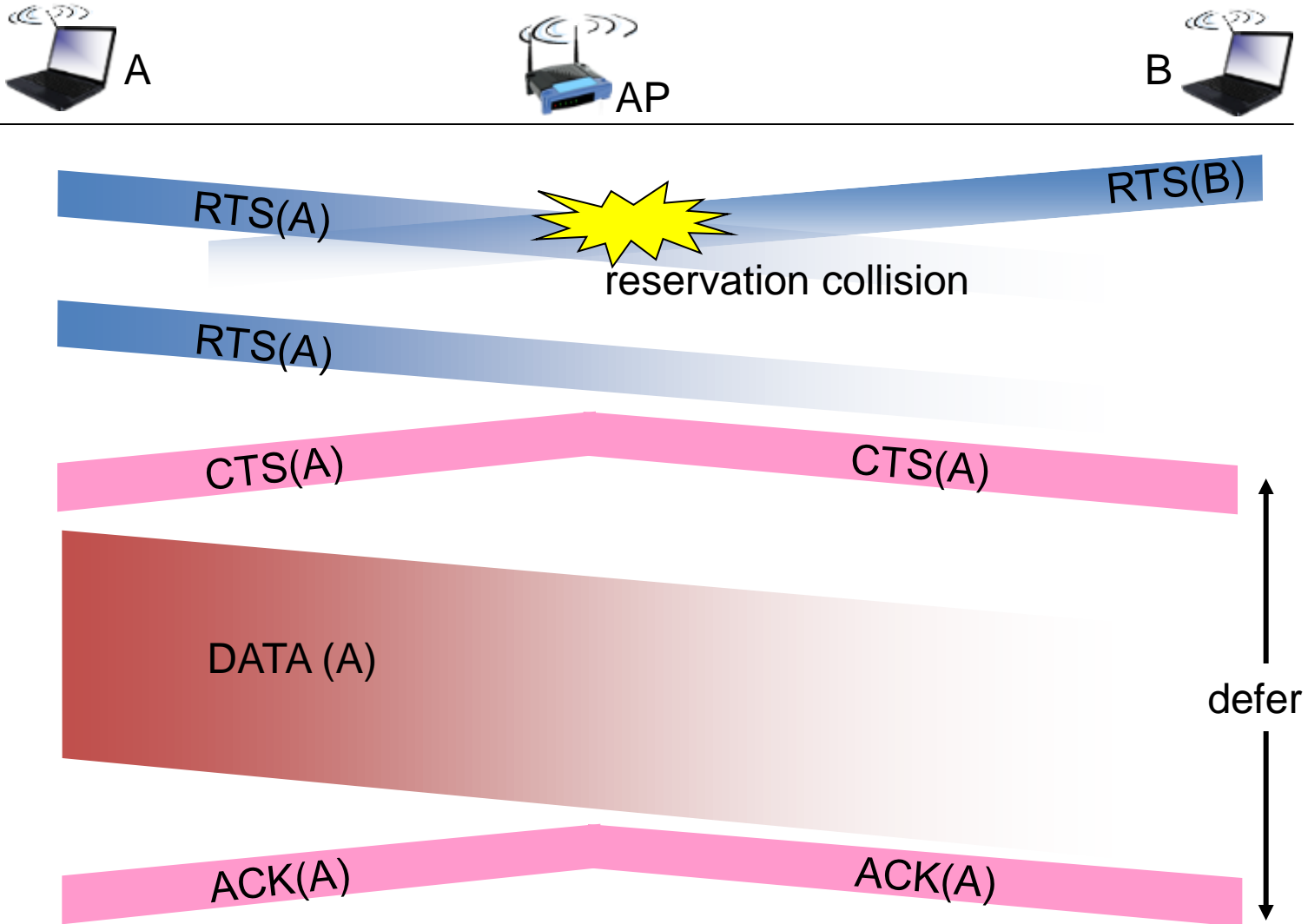
A issues RTS.

B hears RTS, responds with CTS.

C wants to send to B.

But heard the recent CTS broadcast from B.  
C waits until after length of A's  
communication (obtained from the CTS).

# Collision avoidance: RTS-CTS



# Ready to Send-Clear to Send

- RTS-CTS

- Good in theory, not used much in practice
- Slows down:
  - Short frames and transmissions from access point (AP)

## Why RTS-CTS is not your ideal wireless LAN multiple access protocol

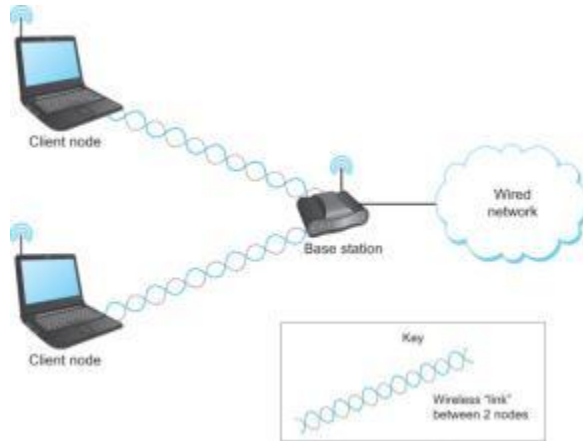
João Luís Sobrinho, Roland de Haan, José Manuel Brázio  
Instituto de Telecomunicações, IST  
Lisboa, Portugal  
Email: {joao.sobrinho, r.dehaan, jose.brazio}@lx.it.pt

**Abstract**—Although Request-To-Send Clear-To-Send (RTS-CTS) has been introduced as a uniform improvement over Carrier Sense Multiple Access (CSMA) in a wireless LAN environment it is not. As it tries to solve the hidden-stations problem of CSMA, it creates new problems derived from the interaction among its control and data packets. In this paper, we systematically identify and classify the sequences of events where CSMA and RTS-CTS depart from an ideal behavior, and we define a reference configuration and an analytical model on the basis of which a comparative study of protocol performance is made. The results show that RTS-CTS falls short of an ideal protocol, in some cases performing even worse than CSMA. This is especially noticeable in situations where the interaction between control packets in RTS-CTS prevents transmissions that under CSMA could occur concurrently and successfully.

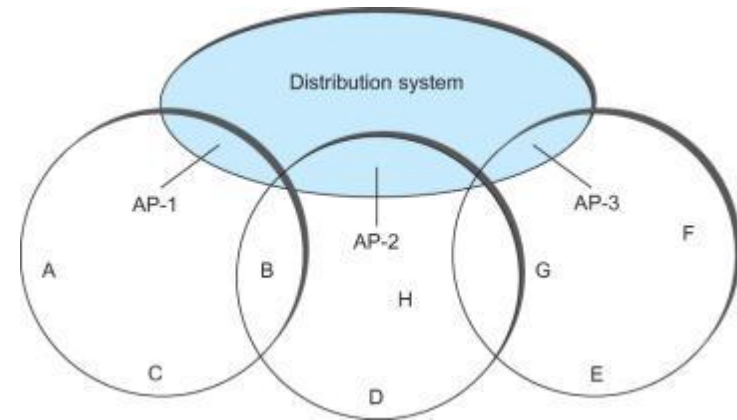
where CSMA and RTS-CTS deviate from the ideal behavior, and we define a reference configuration and an analytical model on the basis of which we make a comparative study of protocol performance. The configuration considered consists of a wireless LAN comprising two interfering cells and subject to several traffic scenarios. The analytical model builds on the work of [8] and [9] and, in contrast to most existing analytical work on RTS-CTS, accurately describes the space and time dependencies between the transmission activity at different stations in the network.

The paper is organized as follows. In Section II, we state the operation of an ideal protocol and closely examine the shortcomings of CSMA and RTS-CTS. Next, in Section III, we

# 802.11 distribution system



Simple distribution system. One access point (AP) and multiple clients.



Distribution system with multiple APs. Clients can switch between APs.

- **Distribution system**

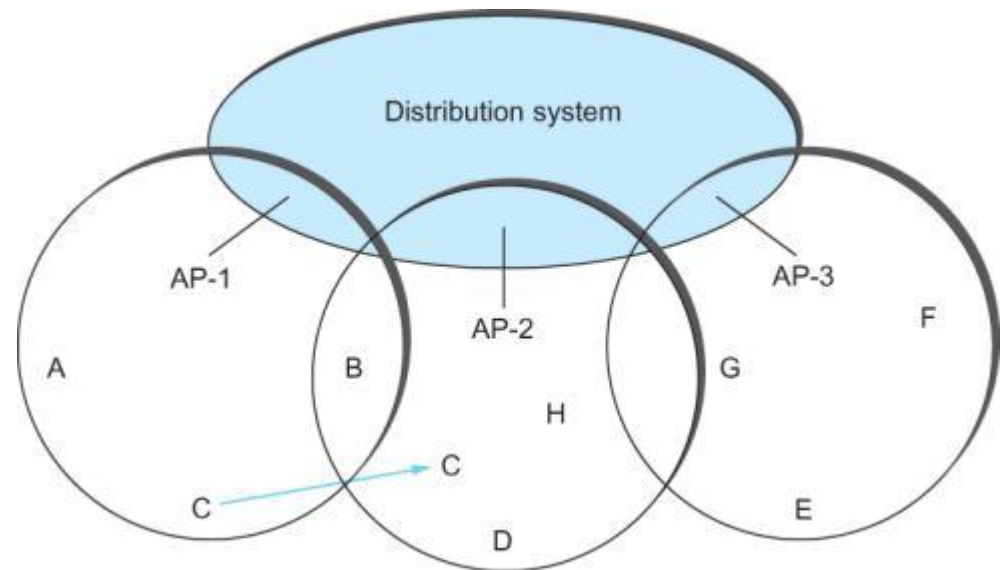
- Operating at same link layer as Wi-Fi

- Not using higher layer protocols (e.g. network layer)

- Each client associates with one AP

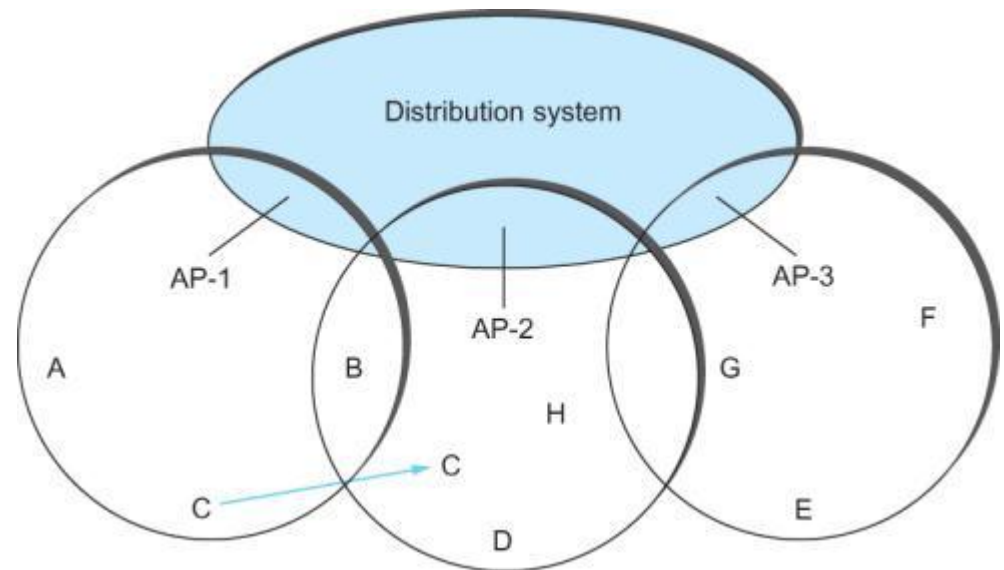
# 802.11 finding an AP

- Passive scanning
  - APs periodically send **beacon frame**
    - Advertise access point's capabilities
    - Transmission rate, etc.
  - Node can respond with **association request**



# 802.11 finding an AP

- Active scanning
  - Node sends a **probe frame**
  - All APs that hear probe, send a **probe response**
  - **Node decides AP it likes best**
  - Node sends AP **association request**
  - AP sends **association response**



# Node communication

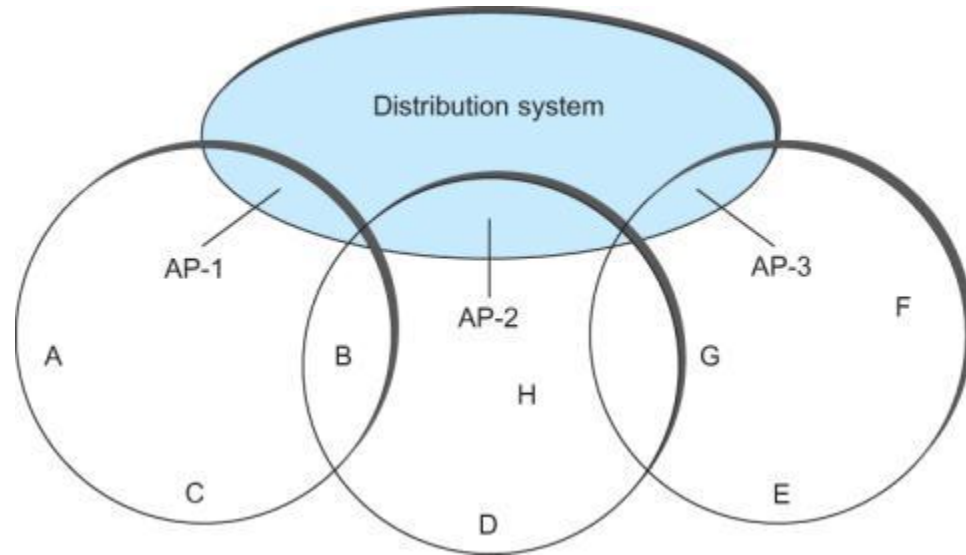
- Node-to-node communication

- Simple case:

- A wants to talk to C
    - Send via AP-1

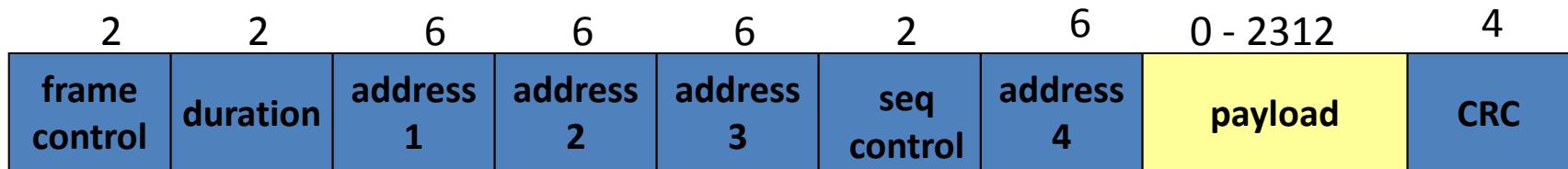
- Complex case:

- A wants to talk to F
    - Send to AP-1
    - Goes through distribution system
    - AP-3 sends to F





# 802.11 frame format



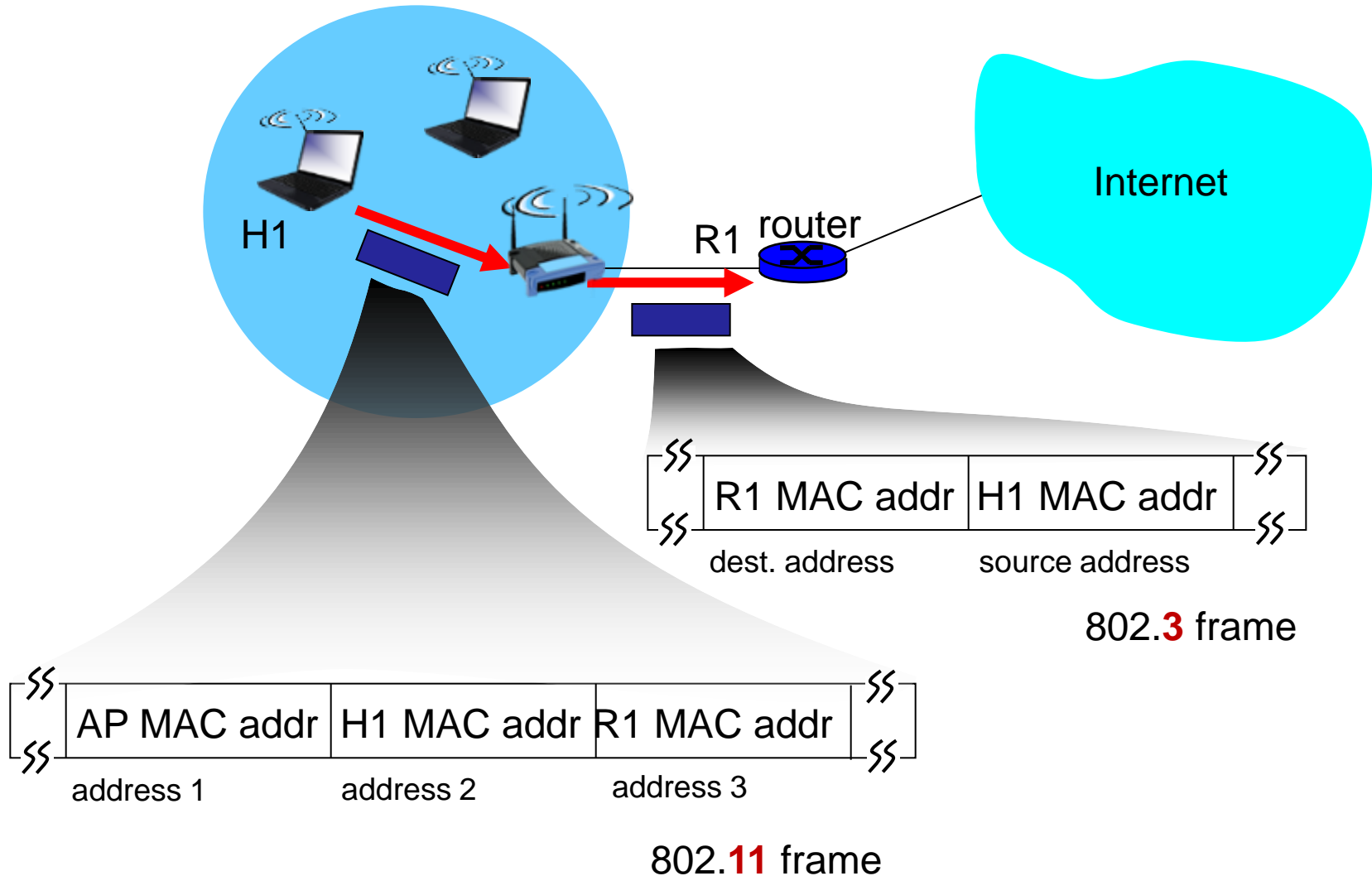
**Address 1:** MAC address of wireless host or AP to receive this frame

**Address 2:** MAC address of wireless host or AP transmitting this frame

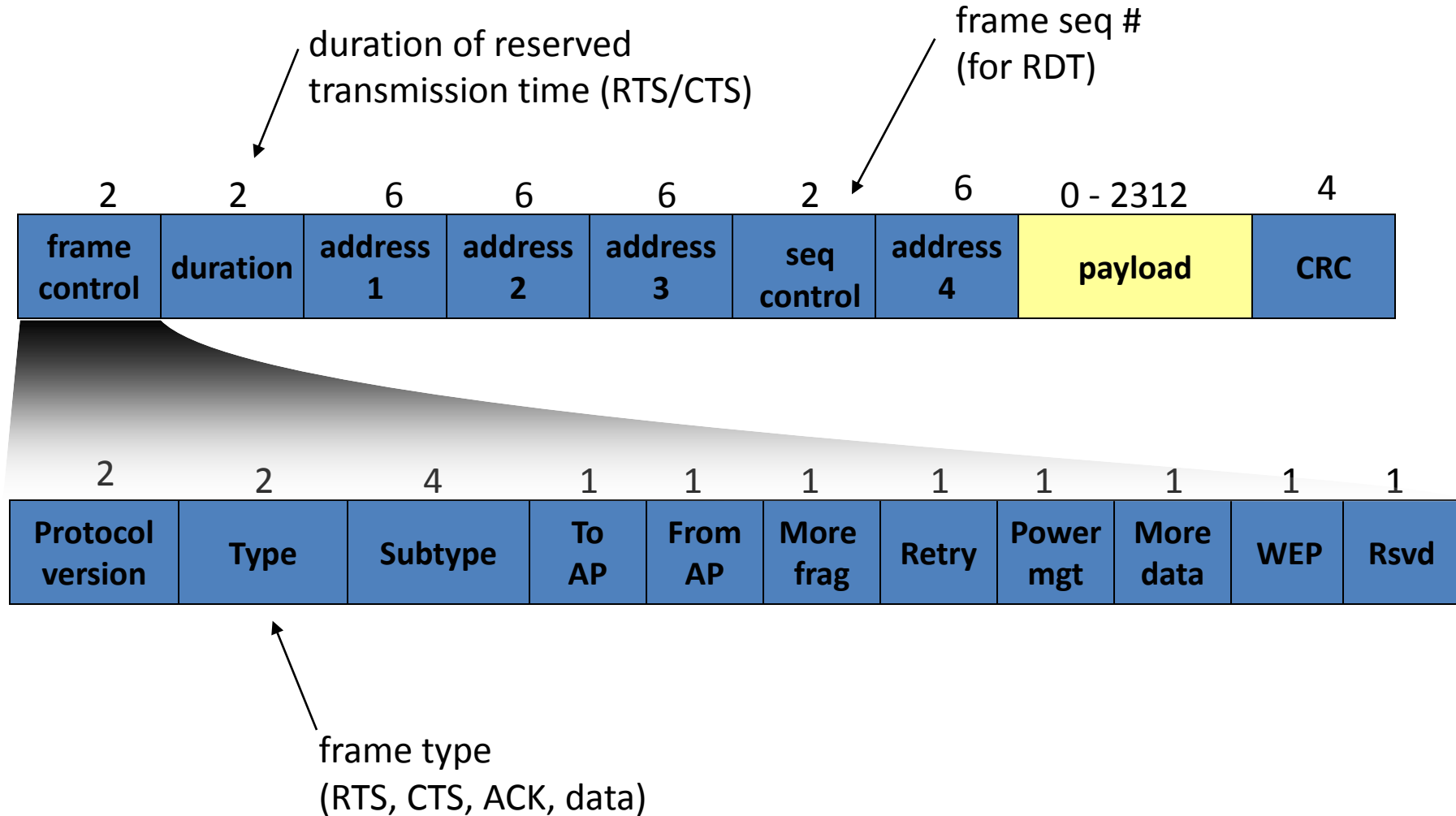
**Address 3:** MAC address of router interface to which AP is attached

**Address 4:** used only in ad hoc mode

# 802.11 frame addressing



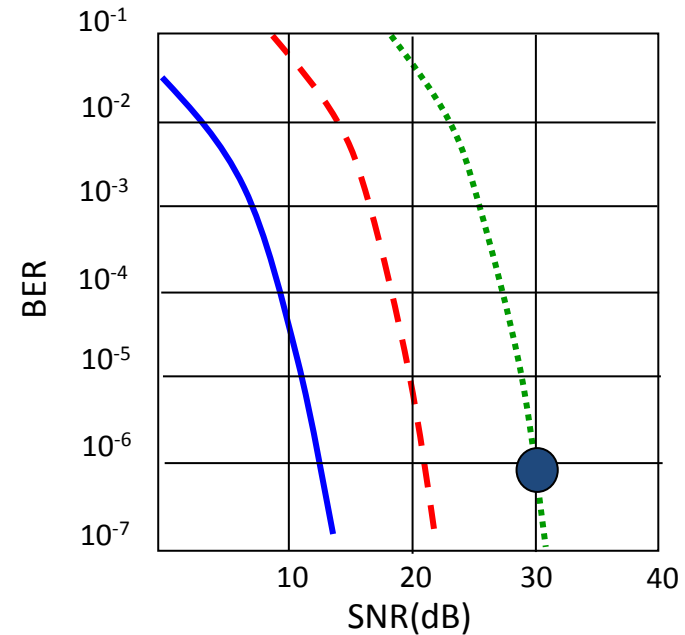
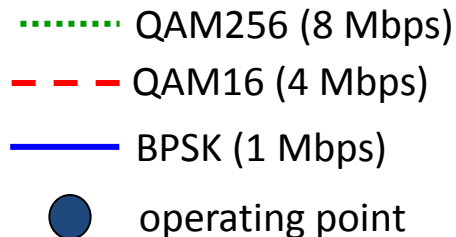
# 802.11 frame format (more)



# 802.11 advanced features

## *Rate adaptation*

- ❖ Base station, mobile dynamically change transmission rate (physical layer modulation technique) as mobile moves, SNR varies



1. SNR decreases, BER increase as node moves away from base station
2. When BER becomes too high, switch to lower transmission rate but with lower BER

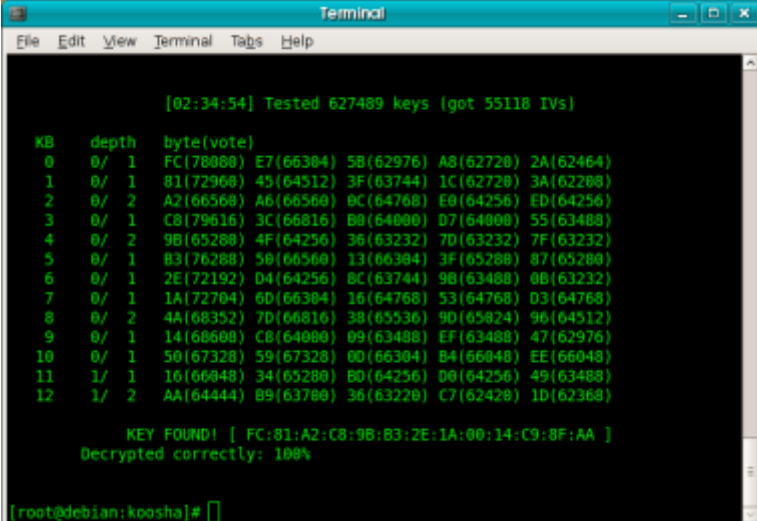
# 802.11 advanced features

## *Power management:*

- ❖ Node-to-AP: "I am going to sleep until next beacon frame"
  - AP knows not to transmit frames to this node
  - Node wakes up before next beacon frame
- ❖ Beacon frame: contains list of mobiles with AP-to-mobile frames waiting to be sent
  - Node will stay awake if AP-to-mobile frames to be sent
  - Otherwise sleep again until next beacon frame

# 802.11 encryption

- Any client in range can sniff frames
- Encryption schemes:
  - WEP (Wired Equivalent Privacy)
    - Encryption in original 802.11 standard (1999)
    - RC4 stream cipher
    - Shared and static 40 bit-secret, 104-bit secret "WEP2"
    - Random 24-bit initialization vector (IV)
    - Only protect wireless hop
  - 2001 exploit published
    - Cracking software freely available



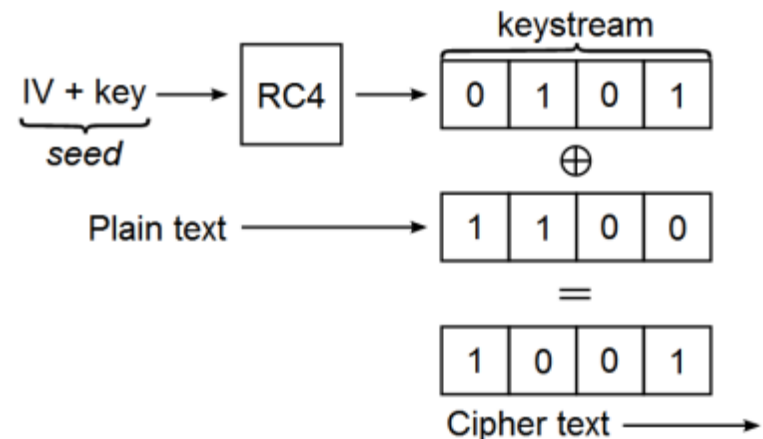
```
Terminal
File Edit View Terminal Tabs Help

[02:34:54] Tested 627489 keys (got 55118 IVs)

KB  depth  byte(vote)
0   0/ 1    FC(78008) E7(66304) 5B(62976) A8(62720) 2A(62464)
1   0/ 1    81(72968) 45(64512) 3F(63744) 1C(62720) 3A(62208)
2   0/ 2    A2(66568) A6(66560) 0C(64768) E0(64256) ED(64256)
3   0/ 1    C8(79616) 3C(66816) B0(64000) D7(64000) 55(63488)
4   0/ 2    9B(65280) 4F(64256) 36(63232) 7D(63232) 7F(63232)
5   0/ 1    83(76288) 50(66560) 13(66304) 3F(65280) 87(65280)
6   0/ 1    2E(72192) D4(64256) 0C(63744) 90(63488) 0B(63232)
7   0/ 1    1A(72704) 6D(66304) 16(64768) 53(64768) D3(64768)
8   0/ 2    4A(68352) 7D(66816) 38(65536) 90(65024) 96(64512)
9   0/ 1    14(68608) C8(64000) 09(63488) EF(63488) 47(62976)
10  0/ 1    50(67328) 59(67328) 00(66304) B4(66048) EE(66048)
11  1/ 1    16(66048) 34(65280) 8D(64256) 00(64256) 49(63488)
12  1/ 2    AA(64444) B9(63780) 36(63220) C7(62420) 1D(62368)

KEY FOUND! [ FC:81:A2:C8:9B:B3:2E:1A:00:14:C9:8F:AA ]
Decrypted correctly: 100%

[root@debian:koosha]#
```



# Breaking 104 bit WEP in less than 60 seconds

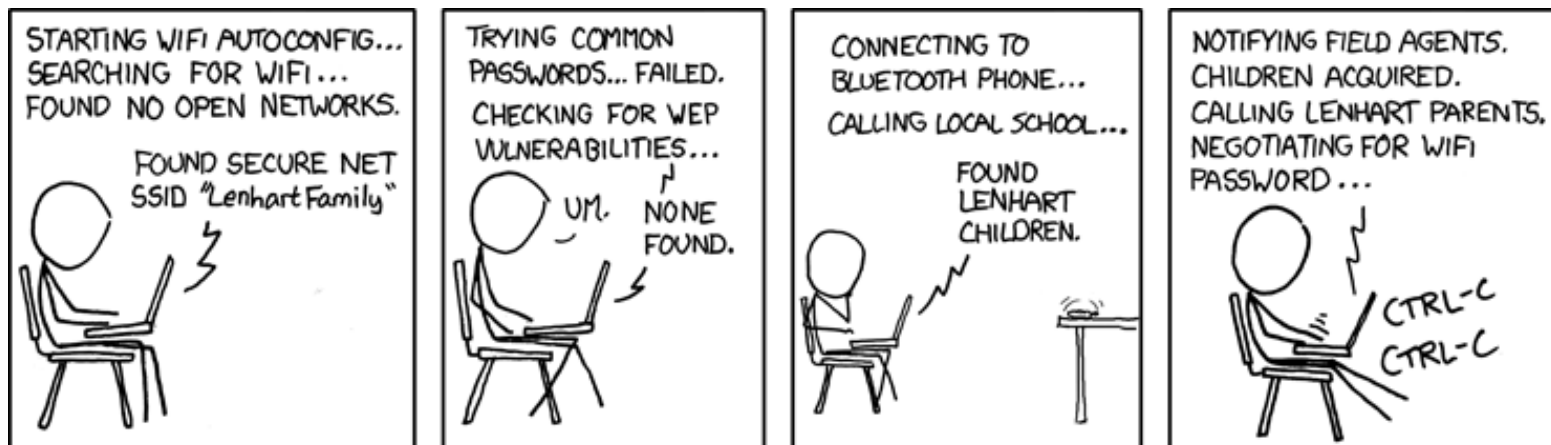
Erik Tews, Ralf-Philipp Weinmann, and Andrei Pyshkin \*  
<e\_tews,weinmann,pyshkin@cdc.informatik.tu-darmstadt.de>

TU Darmstadt, FB Informatik  
Hochschulstrasse 10, 64289 Darmstadt, Germany

**Abstract.** We demonstrate an active attack on the WEP protocol that is able to recover a 104-bit WEP key using less than 40,000 frames with a success probability of 50%. In order to succeed in 95% of all cases, 85,000 packets are needed. The IV of these packets can be randomly chosen. This is an improvement in the number of required frames by more than an order of magnitude over the best known key-recovery attacks for WEP. On a IEEE 802.11g network, the number of frames required can be obtained by re-injection in less than a minute. The required computational effort is approximately  $2^{20}$  RC4 key setups, which on current desktop and laptop CPUs is negligible.

# 802.11 encryption

- WPA (802.11i)
  - WPA interim subset of 802.11i
  - WPA2 (WiFi Protected Access 2)
    - Initial authentication via pre-shared key
    - New key generated for a particular session
    - 128-bit key, 48-bit IV
    - Enterprise version using 802.1x authentication



<http://xkcd.com/416/>



# Summary

- Wireless LANS
  - Shared medium, error-prone
  - Infrastructure vs. ad hoc
  - Code division multiple access (CDMA)
  - Hidden node and exposed node problems
- 802.11
  - Most popular short-haul wireless technology
    - Many flavors: a, b, g, n
  - CSMA with Collision Avoidance (CA)
    - Optional CTS/RTS mechanism
  - Encryption