

# Wireless Local Area Networks (WLANs) and Wireless Sensor Networks (WSNs) Primer

# Wireless Local Area Networks

- The proliferation of laptop computers and other mobile devices (PDAs and cell phones) created an *obvious* application level demand for wireless local area networking.
- Companies jumped in, quickly developing *incompatible* wireless products in the 1990's.
- Industry decided to entrust standardization to IEEE committee that dealt with wired LANs
  - *namely, the IEEE 802 committee!!*

# IEEE 802 Standards Working Groups

Number	Topic
802.1	Overview and architecture of LANs
802.2 ↓	Logical link control
802.3 *	Ethernet
802.4 ↓	Token bus (was briefly used in manufacturing plants)
802.5	Token ring (IBM's entry into the LAN world)
802.6 ↓	Dual queue dual bus (early metropolitan area network)
802.7 ↓	Technical advisory group on broadband technologies
802.8 †	Technical advisory group on fiber optic technologies
802.9 ↓	Isochronous LANs (for real-time applications)
802.10 ↓	Virtual LANs and security
802.11 *	Wireless LANs
802.12 ↓	Demand priority (Hewlett-Packard's AnyLAN)
802.13	Unlucky number. Nobody wanted it
802.14 ↓	Cable modems (defunct: an industry consortium got there first)
802.15 *	Personal area networks (Bluetooth) <b>802.15.4 ZigBee</b>
802.16 *	Broadband wireless
802.17	Resilient packet ring

Figure 1-38. The important ones are marked with \*. The ones marked with ↓ are hibernating. The one marked with † gave up.

*Tanenbaum slide*

# Classification of Wireless Networks

- ***Base Station*** :: all communication through an ***Access Point (AP)*** {note hub topology}. Other nodes can be fixed or mobile.
- ***Infrastructure Wireless*** :: AP is connected to the wired Internet.
- ***Ad Hoc Wireless*** :: wireless nodes communicate directly with one another.
- ***MANETs (Mobile Ad Hoc Networks)*** :: ad hoc nodes are mobile.

# Wireless LANs

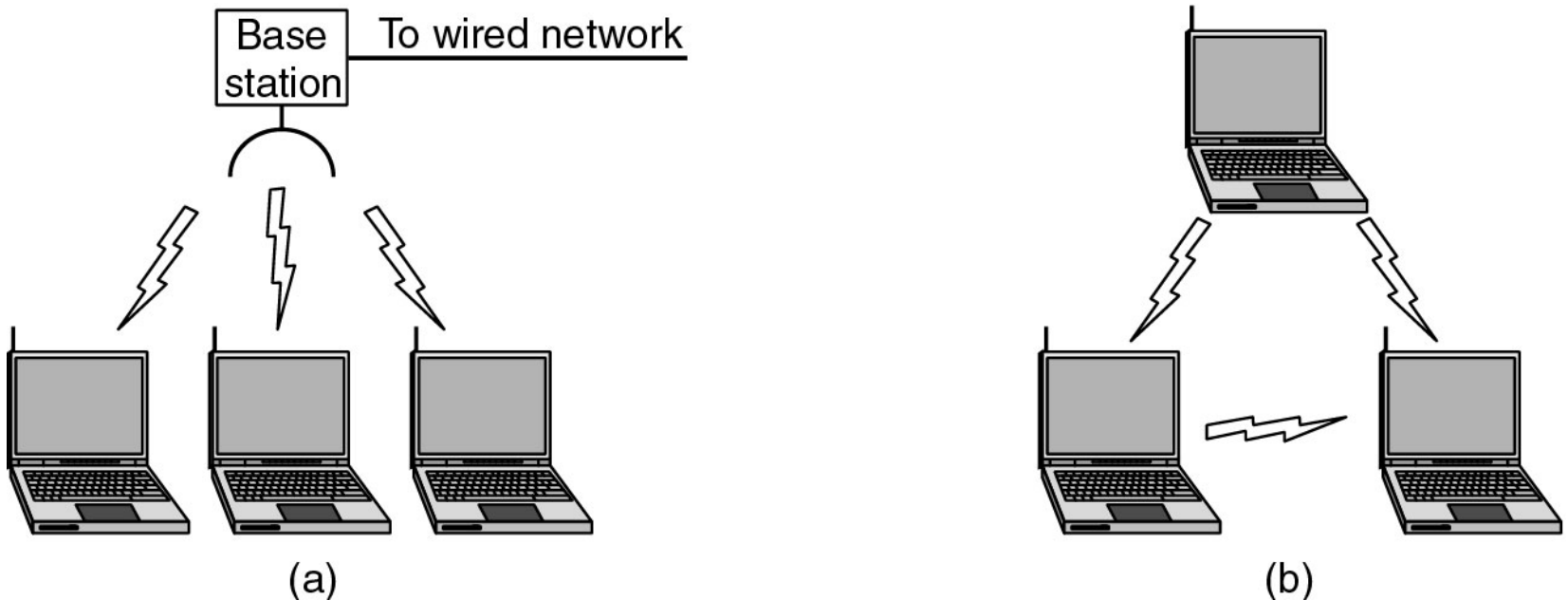


Figure 1-36.(a) Wireless networking with a base station. (b) Ad hoc networking.

# The 802.11 Protocol Stack

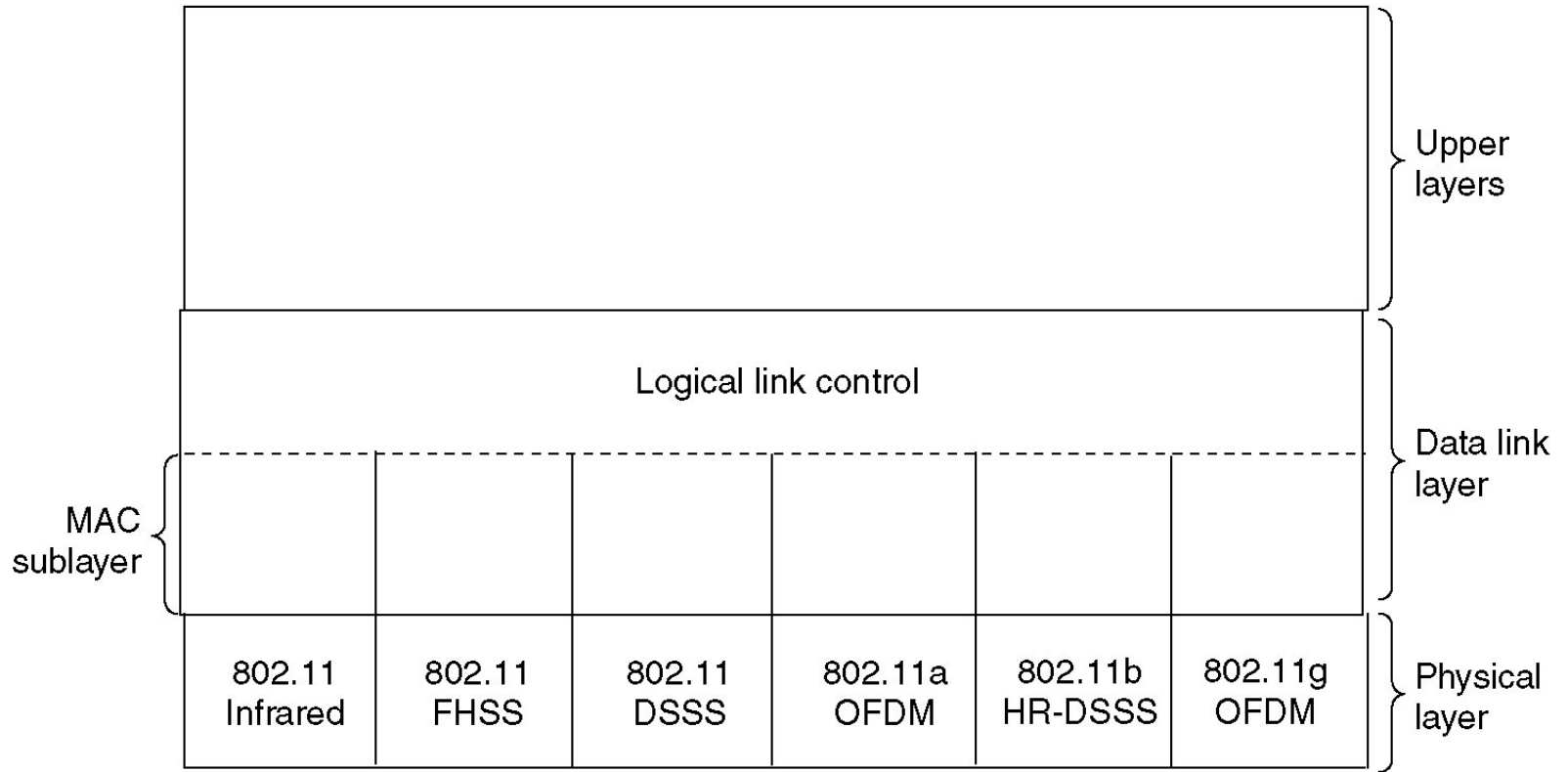


Figure 4-25. Part of the 802.11 protocol stack.

*Note - ordinary 802.11 products are no longer being manufactured.*

Tanenbaum slide

# Wireless Physical Layer

- Physical layer conforms to OSI (five options)
  - 1997: **802.11** infrared, FHSS, DSSS {FHSS and DSSS run in the 2.4GHz band}
  - 1999: **802.11a** OFDM and **802.11b** HR-DSSS
  - 2001: **802.11g** OFDM
- **802.11 Infrared**
  - Two capacities: **1 Mbps or 2 Mbps.**
  - Range is 10 to 20 meters and cannot penetrate walls.
  - Does not work outdoors.
- **802.11 FHSS (Frequency Hopping Spread Spectrum)**
  - **The main issue is *multipath fading.***
  - *[P&D] The idea behind spread spectrum is to spread the signal over a wider frequency to minimize the interference from other devices.*
  - 79 non-overlapping channels, each 1 Mhz wide at low end of 2.4 GHz ISM band.
  - The same pseudo-random number generator used by all stations to start the hopping process.
  - Dwell time: min. time on channel before hopping (400msec).

# Wireless Physical Layer

- **802.11 DSSS (Direct Sequence Spread Spectrum)**
  - *The main idea is to represent each bit in the frame by multiple bits in the transmitted signal (i.e., it sends the XOR of that bit and  $n$  random bits).*
  - Spreads signal over entire spectrum using pseudo-random sequence (similar to CDMA see Tanenbaum sec. 2.6.2).
  - Each bit transmitted using an **11-bit** chipping Barker sequence, PSK at 1Mbaud.
  - This yields a capacity of 1 or 2 Mbps.

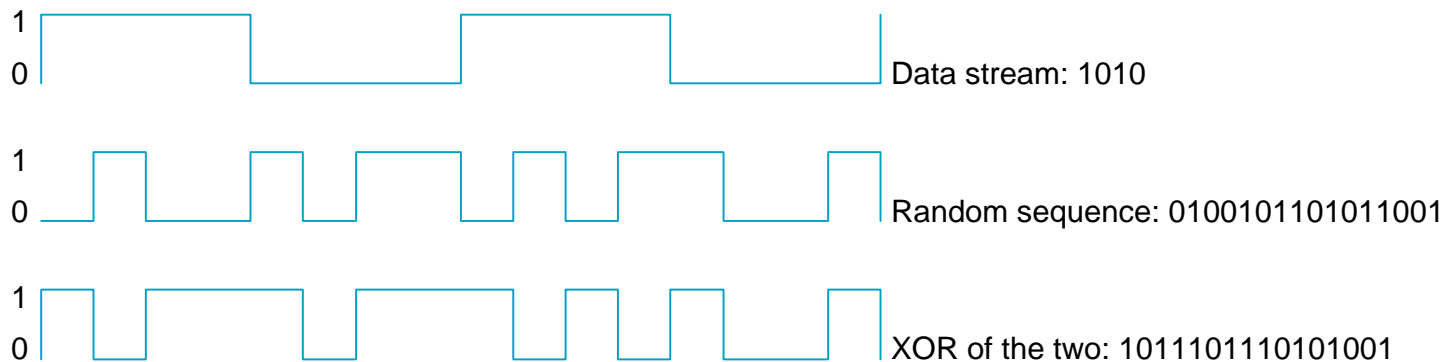


Figure 2.37 Example 4-bit chipping sequence

*P&D slide*



# Wireless Physical Layer

- **802.11a OFDM (Orthogonal Frequency Divisional Multiplexing)**
  - Compatible with European HiperLan2.
  - **54 Mbps** in wider 5.5 GHz band → transmission range is limited.
  - Uses 52 FDM channels (48 for data; 4 for synchronization).
  - Encoding is complex (PSM up to 18 Mbps and QAM above this capacity).
  - E.g., at 54 Mbps 216 data bits encoded into into 288-bit symbols.
  - More difficulty penetrating walls.

# Wireless Physical Layer

- **802.11b HR-DSSS (High Rate Direct Sequence Spread Spectrum)**
  - **11a and 11b** shows a split in the standards committee.
  - **11b** approved and hit the market before **11a**.
  - Up to **11 Mbps** in 2.4 GHz band using 11 million chips/sec.
  - Note in this bandwidth all these protocols have to deal with interference from microwave ovens, cordless phones and garage door openers.
  - Range is 7 times greater than **11a**.
  - **11b and 11a are incompatible!!**

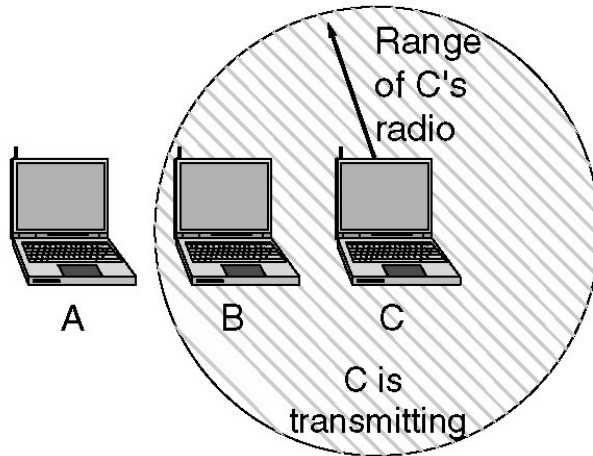
# Wireless Physical Layer

- **802.11g OFDM(Orthogonal Frequency Division Multiplexing)**
  - **An attempt to combine the best of both 802.11a and 802.11b.**
  - Supports bandwidths up to **54 Mbps.**
  - Uses 2.4 GHz frequency for greater range.
  - Is backward compatible with 802.11b.

# 802.11 MAC Sublayer Protocol

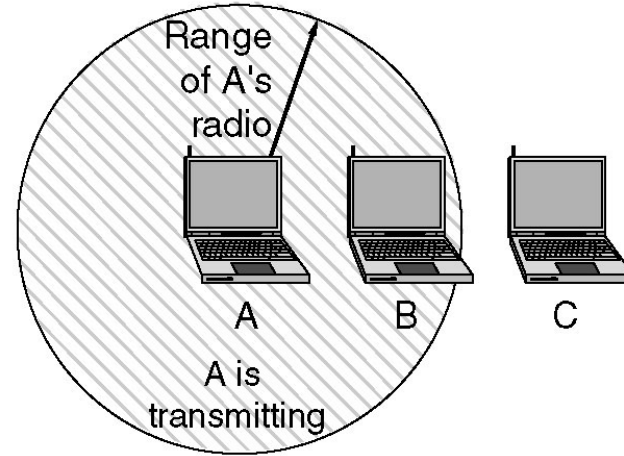
- In 802.11 wireless LANs, “seizing the channel” does not exist as in 802.3 wired Ethernet.
- Two additional problems:
  - Hidden Terminal Problem
  - Exposed Station Problem
- To deal with these two problems 802.11 supports two modes of operation:
  - **DCF (Distributed Coordination Function)**
  - **PCF (Point Coordination Function).**
- **All implementations must support DCF, but PCF is optional.**

A wants to send to B  
but cannot hear that  
B is busy



(a)

B wants to send to C  
but mistakenly thinks  
the transmission will fail



(b)

Figure 4-26.(a)The hidden terminal problem. (b) The exposed station problem.

*Tanenbaum slide*

# The Hidden Terminal Problem

- Wireless stations have transmission ranges and not all stations are within radio range of each other.
- Simple CSMA will not work!
- C transmits to B.
- If A “*senses*” the channel, it will not hear C’s transmission and falsely conclude that A can begin a transmission to B.

# The Exposed Station Problem

- This is the inverse problem.
- B wants to send to C and listens to the channel.
- When B hears A's transmission, B falsely assumes that it cannot send to C.

# Distribute Coordination Function (DCF)

- Uses **CSMA/CA** (**CSMA** with **C**ollision **A**voidance).
  - Uses one of two modes of operation:
    - *virtual carrier sensing*
    - physical carrier sensing
- The two methods are supported:
  1. **MACAW** (**M**ultiple **A**ccess with **C**ollision **A**voidance for **W**ireless) with virtual carrier sensing.
  2. 1-persistent physical carrier sensing.



# Wireless LAN Protocols

[Tan pp.269-270]

- **MACA** protocol solved hidden and exposed terminal problems:
  - Sender broadcasts a Request-to-Send (**RTS**) and the intended receiver sends a Clear-to-Send (**CTS**).
  - Upon receipt of a **CTS**, the sender begins transmission of the frame.
  - RTS, CTS helps determine who else is in range or busy (**C**ollision **A**voidance).
  - Can a collision still occur?

# Wireless LAN Protocols

- **MACAW** added ACKs, Carrier Sense, and BEB done per stream and **not** per station.

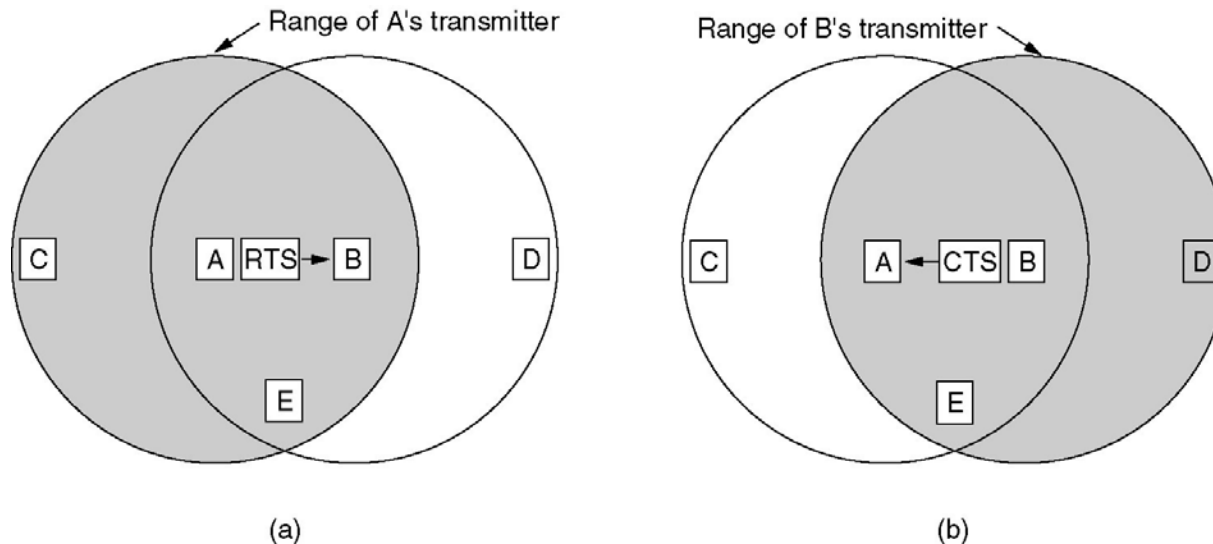


Figure 4-12. (a) A sending an RTS to B.

(b) B responding with a CTS to A.

*Tanenbaum slide*

# Virtual Channel Sensing in CSMA/CA

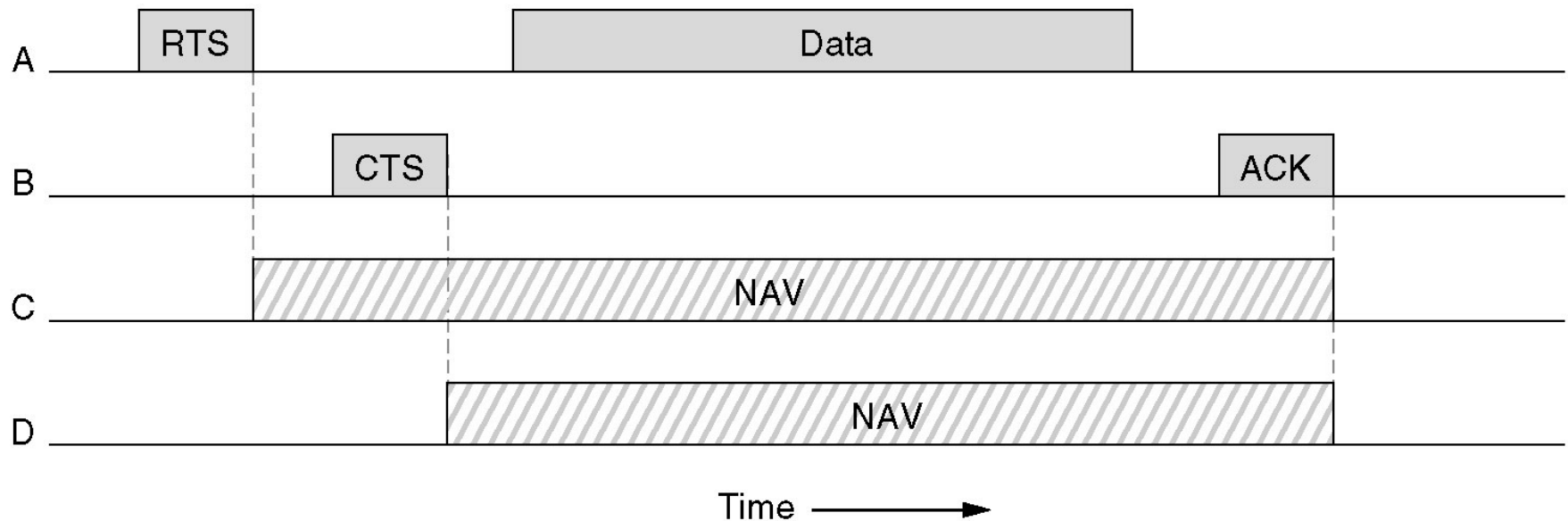


Figure 4-27. The use of virtual channel sensing using CSMA/CA.

- C (in range of A) receives the RTS and based on information in RTS creates a virtual channel busy NAV (Network Allocation Vector).
- D (in range of B) receives the CTS and creates a shorter NAV.

Tanenbaum slide

# Virtual Channel Sensing in CSMA/CA

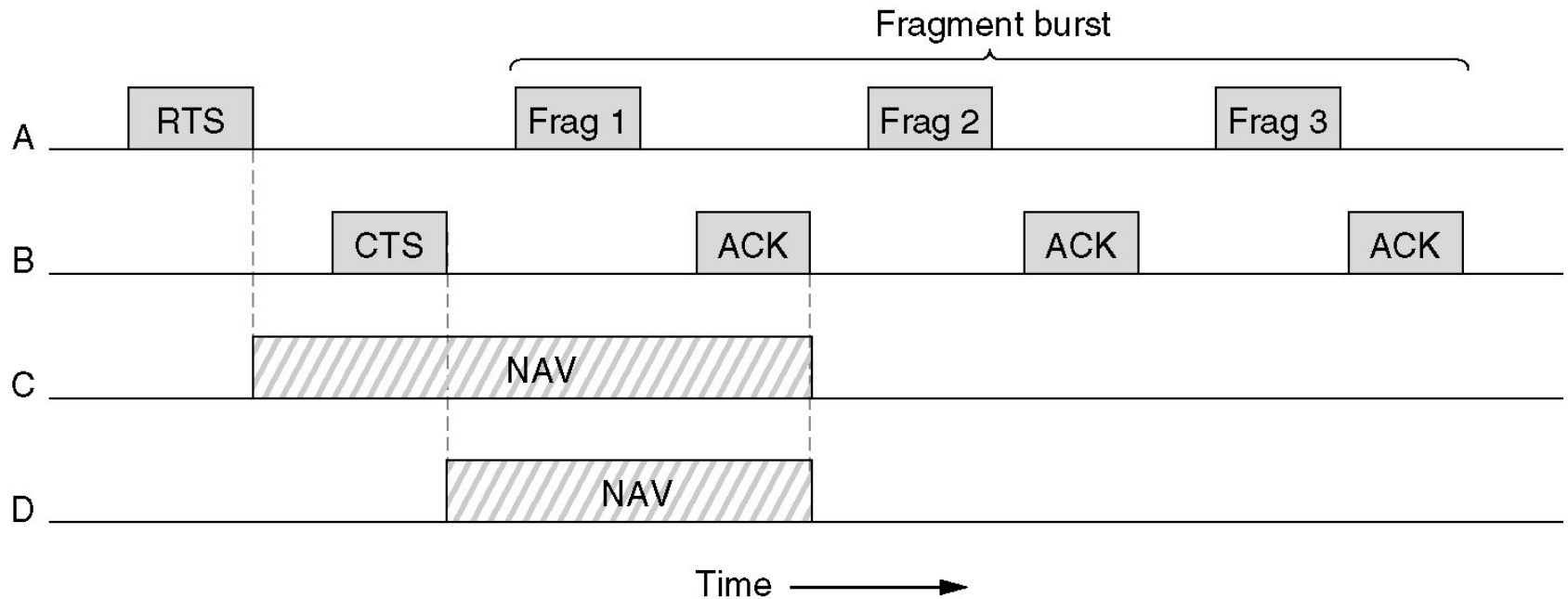
What is the advantage of RTS/CTS?

RTS is 20 bytes, and CTS is 14 bytes.

MPDU can be 2300 bytes.

- “virtual” implies source station sets the *duration field* in data frame or in RTS and CTS frames.
- Stations then adjust their NAV accordingly!

# Figure 4-28 Fragmentation in 802.11



- High wireless error rates → long packets have less probability of being successfully transmitted.
- Solution: MAC layer fragmentation with stop-and-wait protocol on the fragments.

*Tanenbaum slide*

# 1-Persistent Physical Carrier Sensing

- The station **senses** the channel when it wants to send.
- If idle, the station transmits.
  - *A station does not sense the channel while transmitting.*
- If the channel is busy, the station defers until idle and then transmits (**1-persistent**).
- Upon collision, wait a *random time* using binary exponential backoff (**BEB**).

# Point Coordinated Function (PCF)

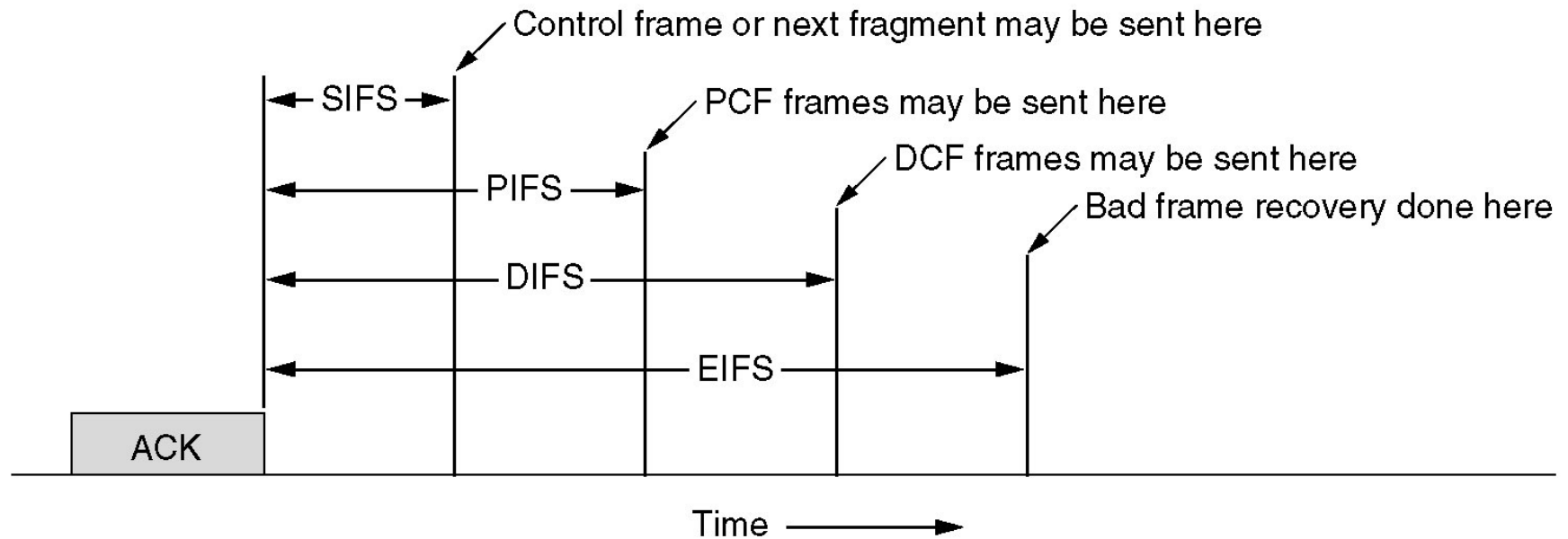
- PCF uses a base station to poll other stations to see if they have frames to send.
- No collisions occur.
- Base station sends *beacon frame* periodically.
- Base station can tell another station to *sleep* to save on batteries and base stations holds frames for sleeping station.

# DCF and PCF Co-Existence

- Distributed and centralized control can co-exist using InterFrame Spacing.
- SIFS (Short IFS) :: is the time waited between packets in an ongoing dialog (RTS,CTS,data, ACK, next frame)
- PIFS (PCF IFS) :: when no SIFS response, base station can issue beacon or poll.
- DIFS (DCF IFS) :: when no PIFS, any station can attempt to acquire the channel.
- EIFS (Extended IFS) :: lowest priority interval used to report bad or unknown frame.



# Figure 4-29. Interframe Spacing in 802.11.



*Tanenbaum slide*

# Basic CSMA/CA

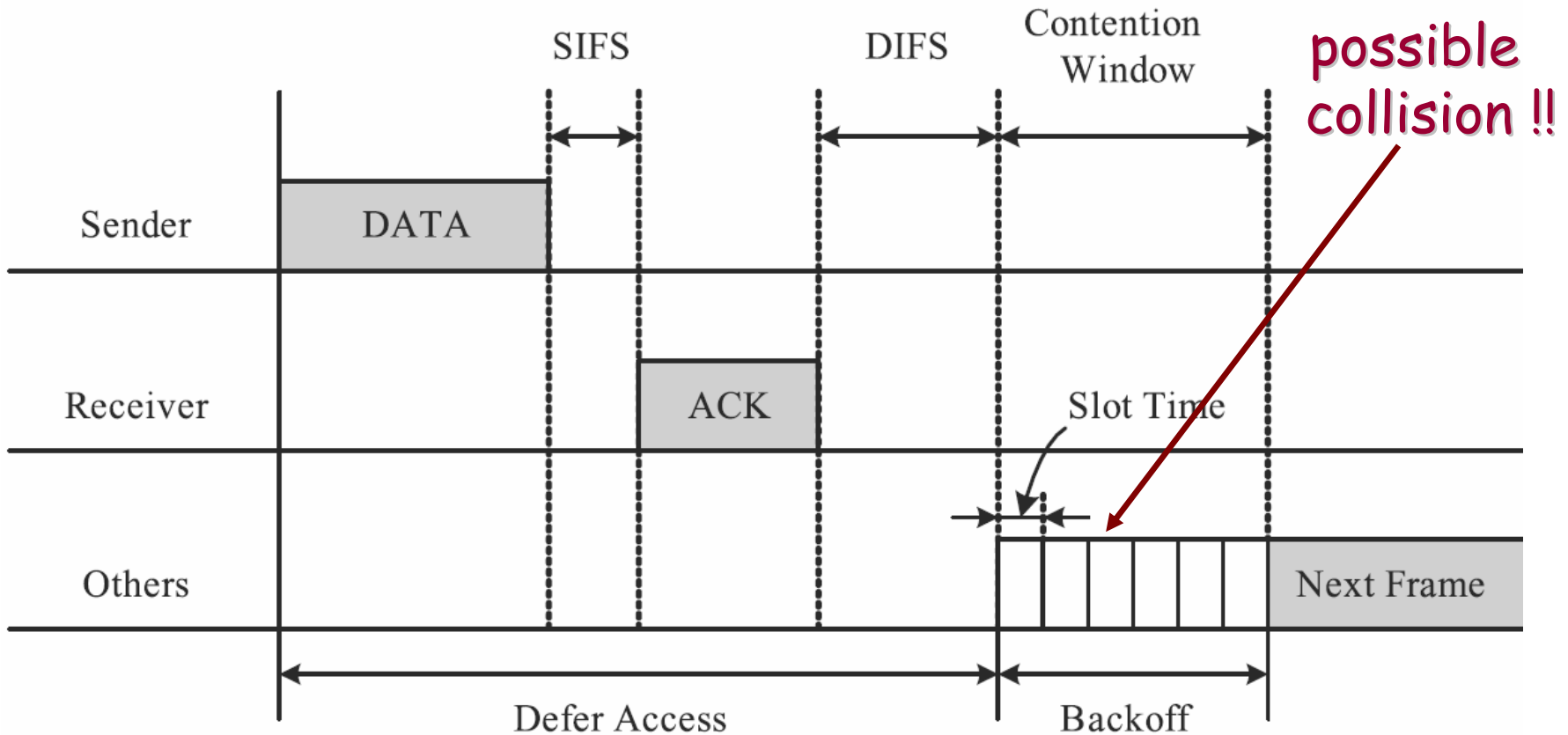


Fig. 1 CSMA/CA protocol of IEEE 802.11 MAC DCF. [N. Kim]

# A Few Wireless Details

- 802.11b and 802.11g use *dynamic rate adaptation* based on frame loss (algorithms internal to wireless card at the AP)
  - e.g. for 802.11b choices are: 11, 5.5, 2 and 1 Mbps
- RTS/CTS may be turned off by default [Research has shown that RTS/CTS degrades performance when hidden terminal is not an issue].
- All APs (or base stations) will periodically send a beacon frame (10 to 100 times a second).
- Beacon frames are also used by DCF to synchronize and handle nodes that want to *sleep*. The AP will buffer frames intended for a sleeping wireless client.
- AP downstream/upstream traffic performance is *asymmetric*.
- Wireless communication quality between two nodes can be asymmetric due to *multipath fading*.

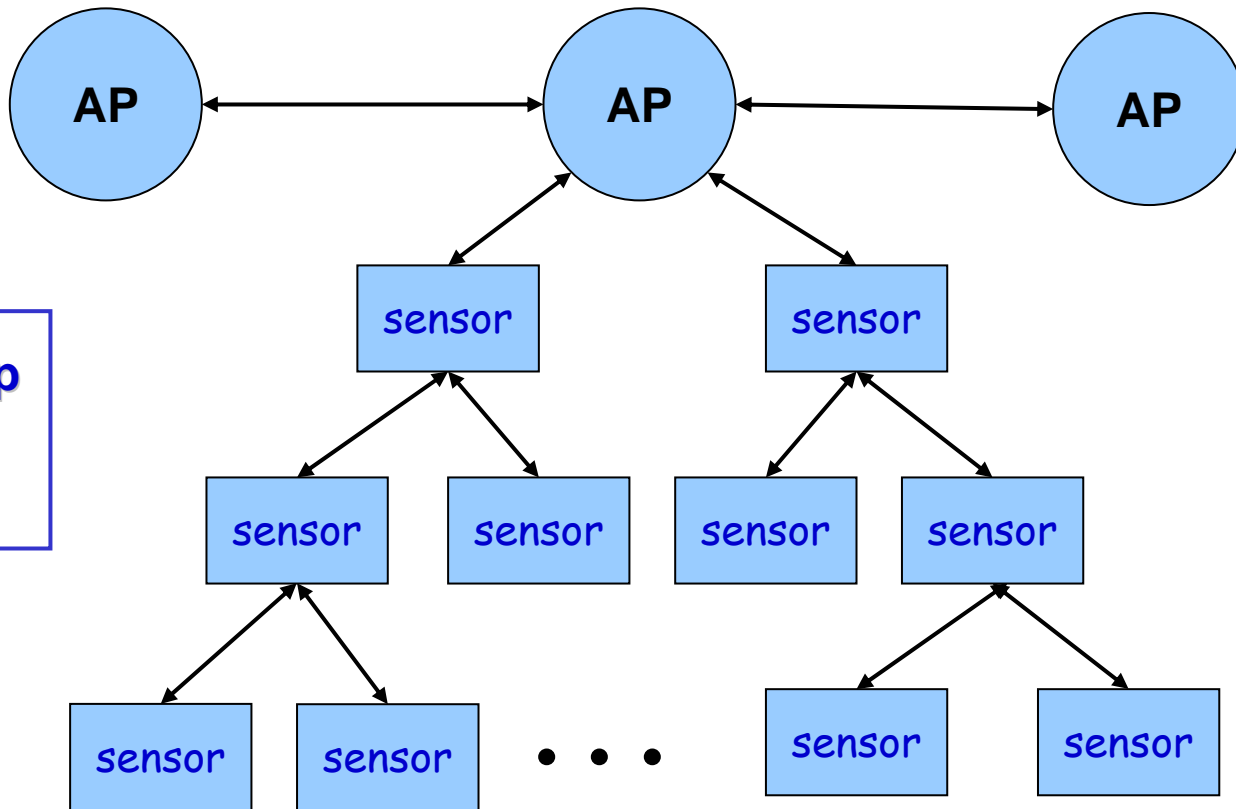
# Wireless Sensor Networks

- Sensors – small devices with low-power transmissions and energy limitations (e.g., battery lifetime is often a **BIG** concern.)
- The main distinction from traditional wireless networks is that the data traffic originates at the sensor node and is sent **upstream** towards the access point (AP) or base station that collects the data.
- While the nature of data collection at the sensor is likely to be **event driven**, for robustness, the generation of sensor packets should be **periodic** if possible.

# Tiered Architecture

- Smaller sensors on the leaves of the tree
  1. Motes, TinyOS
  2. Strong ARM PDA running Linux
    - Battery powered, lifetime is critical.
    - Need to be able to adjust transmission power and permit sensor to go to sleep.
- Second Tier
  - AP, base station or video aggregator
  - Data sent from sensors to more powerful computers for storage and analysis.

# The Berkeley System



Multiple hop  
tree  
topology

# The Berkeley System

