CSMC 417

Computer Networks

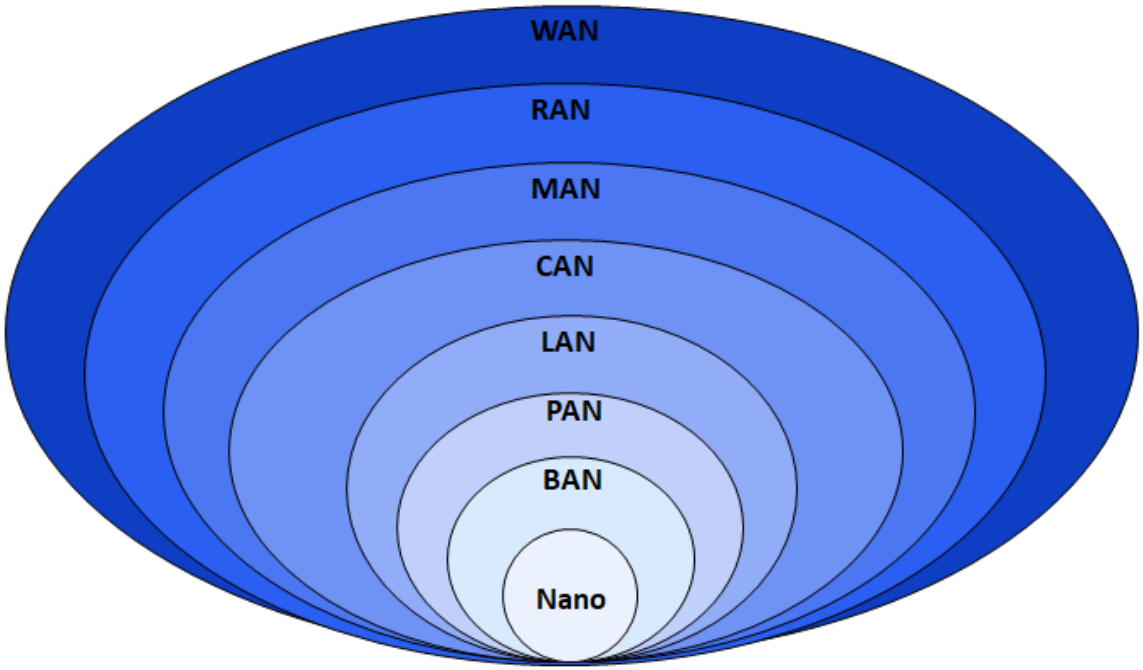
Prof. Ashok K Agrawala

The Medium Access Control Sublayer

Wireless Networking Technologies

Computer Network Types by Spatial Scope

- Nanoscale
- Near-field (NFC)
- Body (BAN)
- Personal (PAN)
- Near-me (NAN)
- Local (LAN)
  - Home (HAN)
  - Storage (SAN)
  - Wireless (WLAN)
- Campus (CAN)
- Backbone
- Metropolitan (MAN)
- Wide (WAN)
- Cloud (IAN)
- Internet
- Interplanetary Internet



WikiPedia NFC

Technologies

- IEEE 802.11 -- WiFi
- Bluetooth
- Zigbee
- Z Wave
- UWB
- RFID
- NFC
- Cellular
  - GSM
  - LTE
  - WiMAX

Characteristics

- Frequency
  - ISM
    - 900 MHz
    - 2.4 GHz
    - 5 Ghz
  - Others
- Data Rates
- Range
- Infrastructure

WiFi MAC

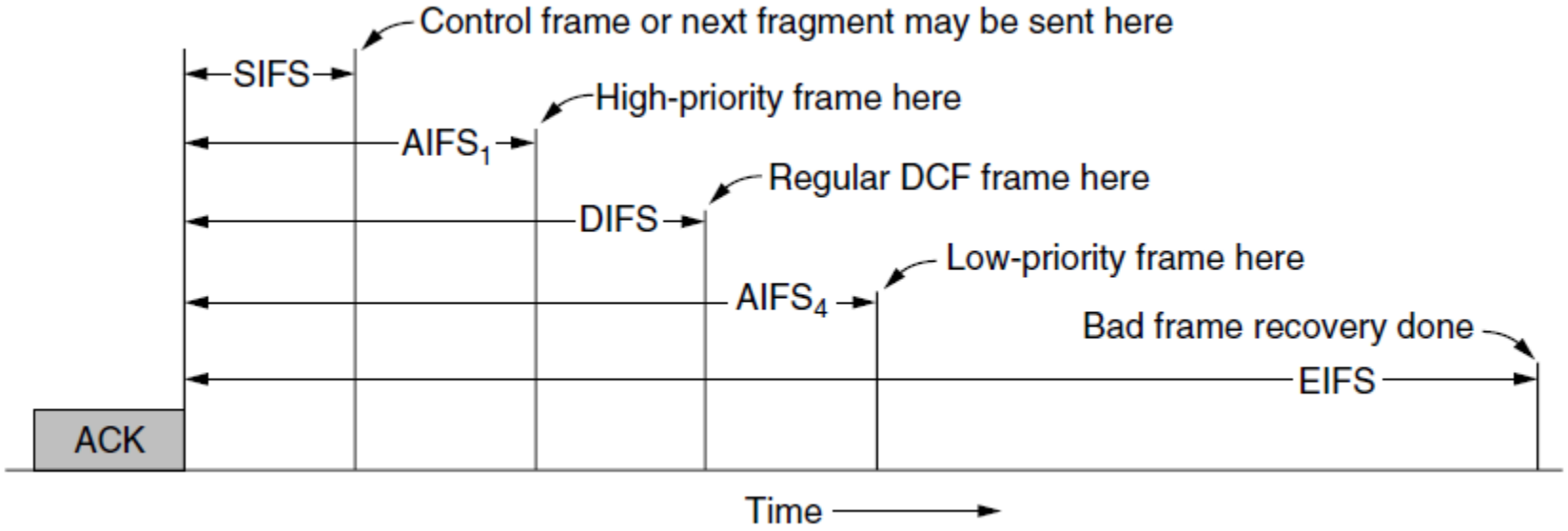
- Retry Counters
  - Short retry counter
  - Long retry counter
  - Lifetime timer
- Basic Access Mechanism
  - CSMA/CA
  - Binary exponential back-off
  - NAV – Network Allocation Vector
- Timing Intervals: SIFS, Slot Time, PIFS, DIFS, EIFS
- DCF Operation
- PCF Operation

Contention and Contention-Free Access

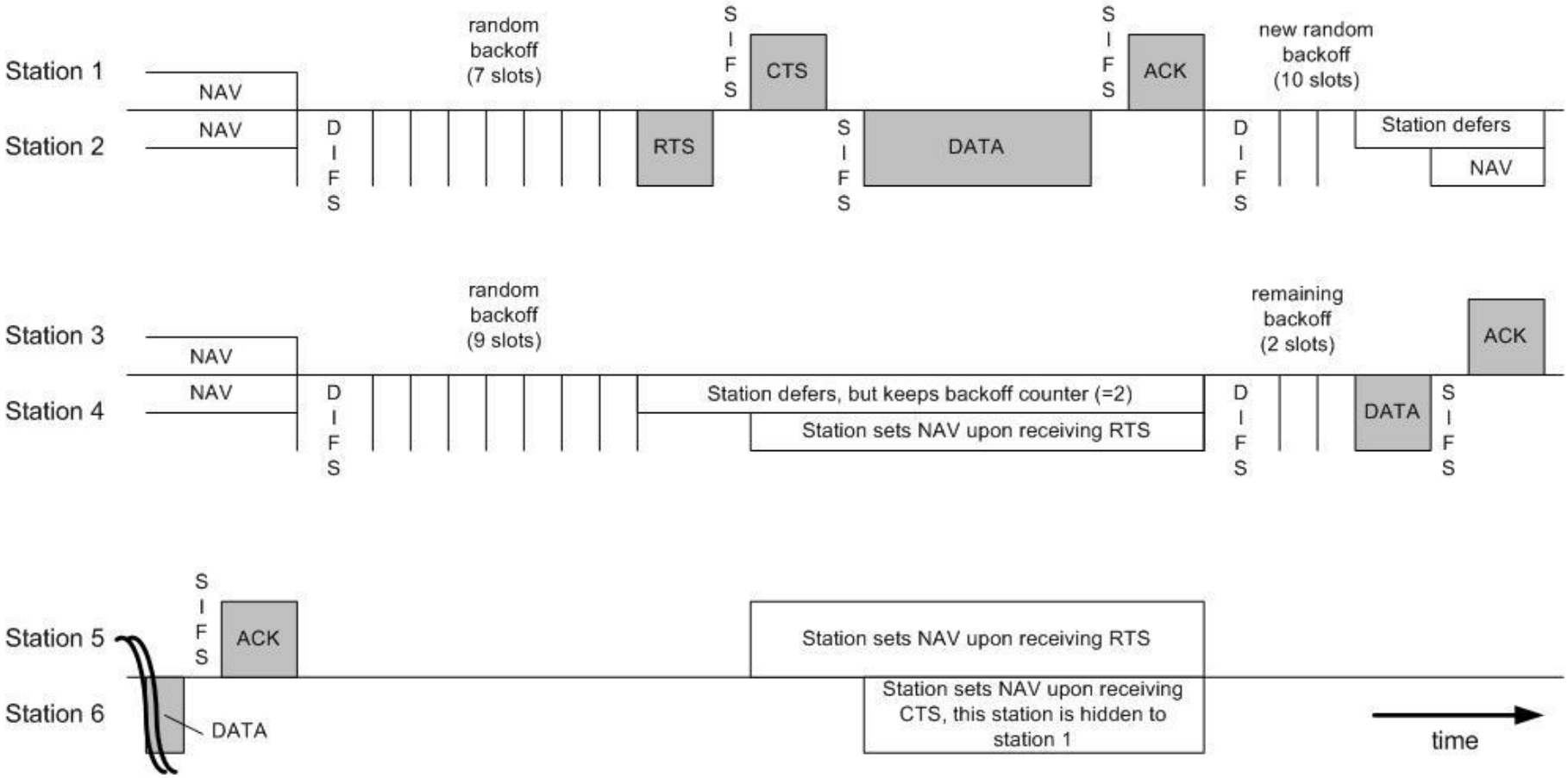
- The original 802.11 standard defined two general approaches for channel access
  - Point Coordinated Function (PCF) for contention-free service
    - an AP controls stations in the Basic Service Set (BSS) to insure that transmissions do not interfere with one another
    - For example, an AP can assign each station a separate frequency
    - In practice, PCF is never used
  - Distributed Coordinated Function (DCF) for contention-based service
    - arranges for each station in a BSS to run a random access protocol
- Wireless networks can experience a hidden station problem
  - where two stations can communicate but a third station can only receive the signal from one of them
- 802.11 networks use CSMA/CA
  - which requires a pair to exchange Ready To Send (RTS) and Clear To Send (CTS) messages before transmitting a packet

WiFi

- Protocol
  - CSMA-CA



DCF Operation

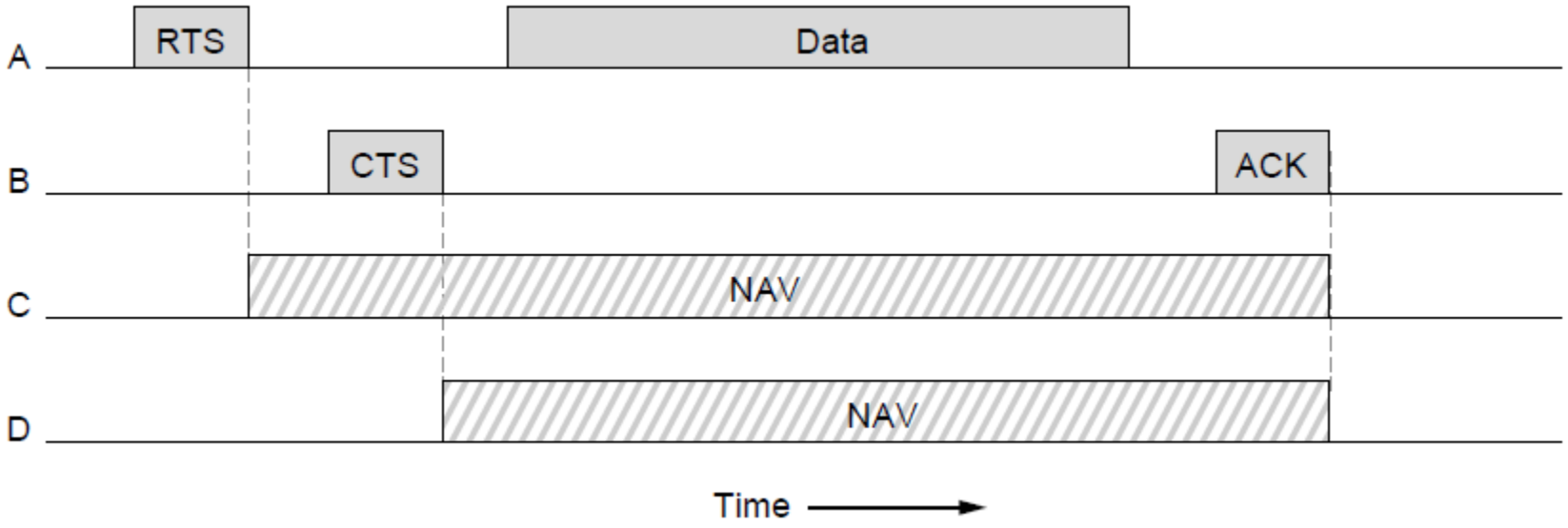


PCF Operation

- Poll – eliminates contention
- PC – Point Coordinator
  - Polling List
  - Over DCF
  - PIFS (less than DIFS ~ 30 μs)
- CFP – Contention Free Period
  - Alternate with DCF
- Periodic Beacon – contains length of CFP
- CF-Poll – Contention Free Poll
- NAV prevents during CFP
- CF-End – resets NAV

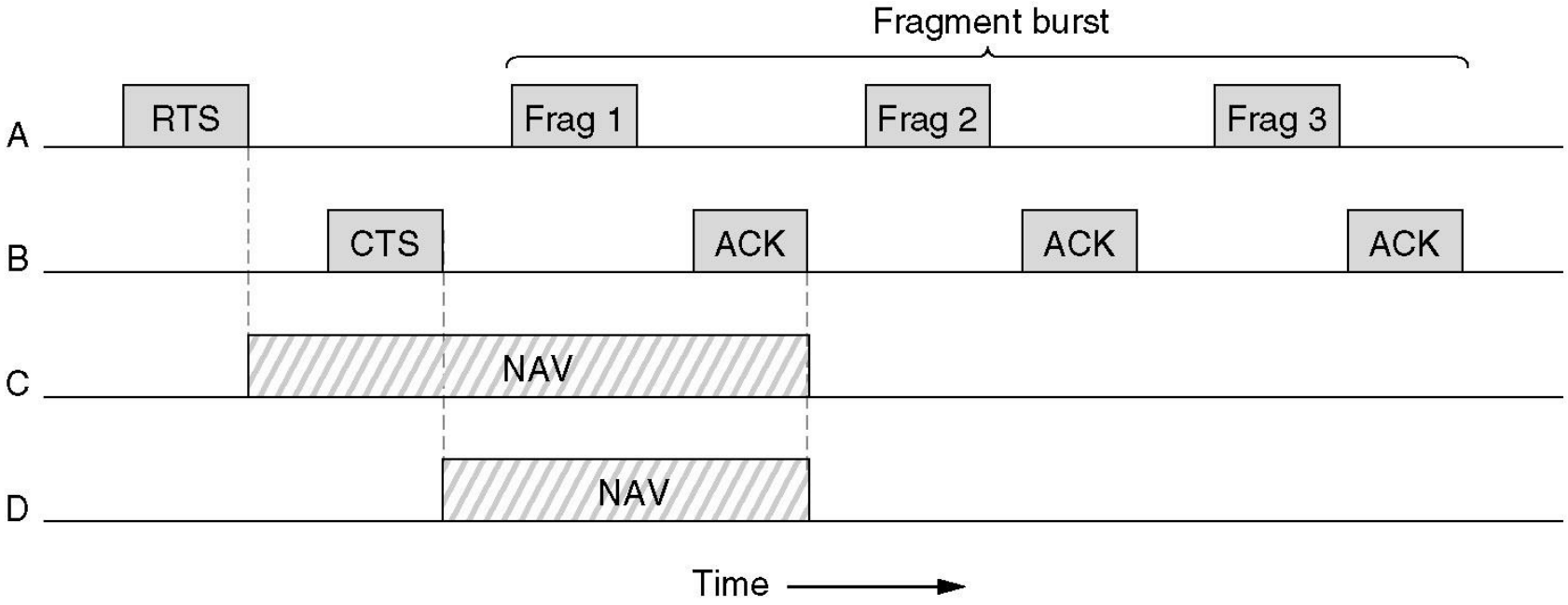
802.11 MAC (2)

Virtual channel sensing with the NAV and optional RTS/CTS (often not used) avoids hidden terminals



The 802.11 MAC Sublayer Protocol (3)

A fragment burst.



Other MAC Operations

- Fragmentation
  - Sequence control field
  - In burst
  - Medium is reserved
  - NAV is updated by ACK

- Privacy
  - WEP bit set when encrypted.
  - Only the frame body.
  - Medium is reserved
  - NAV is updated by ACK
  - Symmetric variable key

- WEP Details
  - Two mechanism
    - Default keys
    - Key mapping
  - WEP header and trailer
    - KEYID in header
    - ICV in trailer
  - *dot11UndecryptableCount*
    - *Indicates an attack.*
  - *dot11ICVErrorCount*
    - *Attack to determine a key is in progress.*

MAC Management

- Interference by users that have no concept of data communication. Ex: Microwave
- Interference by other WLANs
- Security of data
- Mobility
- Power Management

Authentication

- Authentication
  - Prove identity to another station.
  - Open system authentication
  - Shared key authentication
    - A sends
    - B responds with a text
    - A encrypt and send back
    - B decrypts and returns an authentication management frame.
  - May authenticate any number of station.

- Security Problem
  - A rogue AP
    - SSID of ESS
    - Announce its presence with beaconing
    - A active rogue reach higher layer data if unencrypted.

Association

- Association
  - Transparent mobility
  - After authentication
  - Association request to an AP
  - After established, forward data
  - To BSS, if DA is in the BSS.
  - To DS, if DA is outside the BSS.
  - To AP, if DA is in another BSS.
  - To "**portal**", if DC is outside the ESS.
  - **Portal** : transfer point : track mobility. (AP, bridge, or router) transfer 802.1h
  - New AP after reassociation, communicates with the old AP.

Address Filtering

- More than one WLAN
- Three Addresses
- Receiver examine the DA, BSSID

Privacy MAC Function

- WEP Mechanism

Power Management

- Independent BSS
  - Distributed
  - Data frame handshake
  - Wake up every beacon.
  - Awake a period of ATIM after each beacon.
  - Send ACK if receive ATIM frame & awake until the end of next ATIM.
  - Estimate the power saving station, and delay until the next ATIM.
  - Multicast frame : No ACK : optional

Overhead

- Sender
  - Announcement frame
  - Buffer
  - Power consumption in ATIM
- Receiver
  - Awake for every Beacon and ATIM

Power Management

- Infrastructure BSS
  - Centralized in the AP.
  - Greater power saving
  - Mobile Station sleeps for a number of beacon periods.
  - Awake for multicast indicated in DTIM in Beacon.
  - AP buffer, indicate in TIM
  - Mobile requests by PS-Poll

Synchronization

- Timer Synchronization in an Infrastructure BSS
  - Beacon contains TSF
  - Station updates its with the TSF in beacon.

- Timer Synchronization in an IBSS
  - Distributed. Starter of the BSS send TSF zero and increments.
  - Each Station sends a Beacon
  - Station updates if the TSF is bigger.
  - Small number of stations: the fastest timer value
  - Large number of stations: slower timer value due to collision.

- Synchronization with Frequency Hopping PHY Layers
  - Changes in a frequency hopping PHY layer occurs periodically (the dwell period).
  - Change to new channel when the TSF timer value, modulo the dwell period, is zero

Scanning & Joining

- Scanning
  - Passive Scanning : only listens for Beacon and get info of the BSS. Power is saved.
  - Active Scanning: transmit and elicit response from APs. If IBSS, last station that transmitted beacon responds. Time is saved.
- Joining a BSS
  - Syncronization in TSF and frequency : Adopt PHY parameters : The BSSID : WEP : Beacon Period : DTIM

Combining Management Tools

- Combine Power Saving Periods with Scanning
  - Instead of entering power saving mode, perform active scanning.
  - Gather information about its environments.

- Preauthentication
  - Scans and initiate an authentication
  - Reduces the time

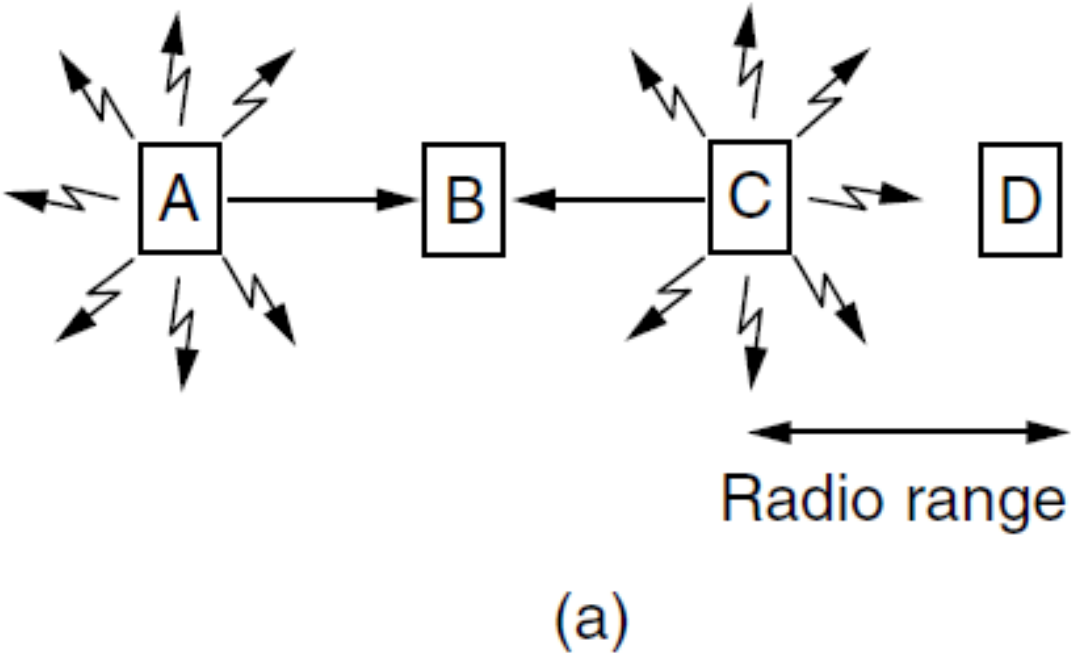
Coordination Among Access Points

- To what extent do APs need to coordinate?
- Many early AP designs were complex
- The access points coordinated to provide seamless mobility similar to the cellular phone system
  - That is, the APs communicated amongst themselves to insure smooth handoff as a wireless computer moved from the region to another
  - Some designs measured signal strength and attempted to move a wireless node to a new AP
    - when the signal received at the new AP exceeded the signal strength at the existing AP

Coordination Among Access Points

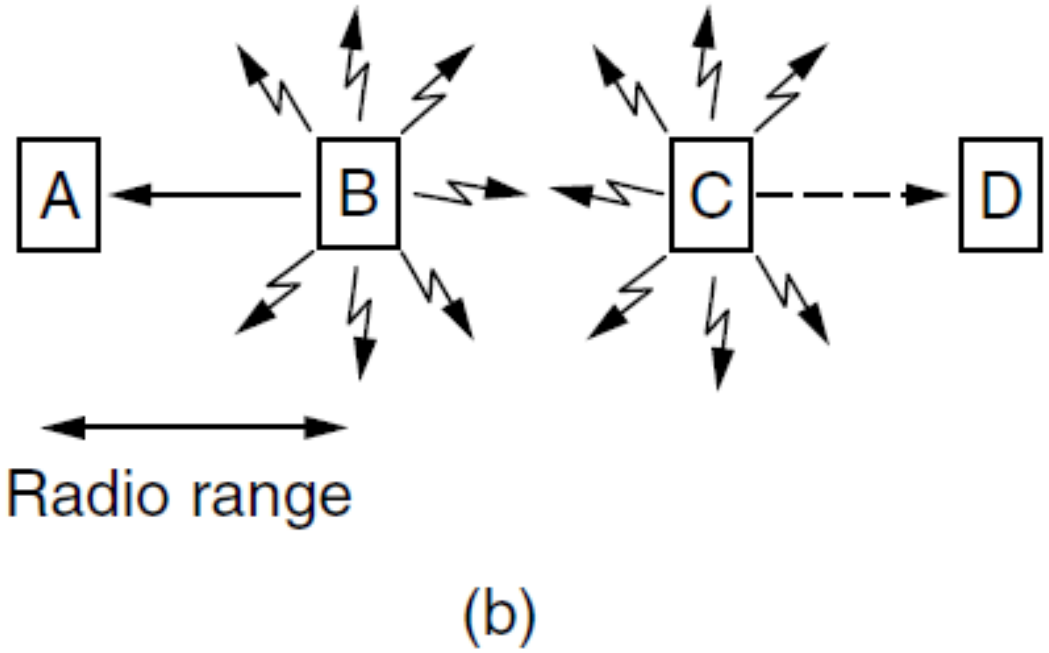
- Some vendors began to offer lower cost, less complex APs that do not coordinate
- The vendors argue that signal strength does not provide a valid measure of mobility
  - a mobile computer can handle changing from one AP to another
  - and that the wired infrastructure connecting APs has sufficient capacity to allow more centralized coordination
- A less complex AP design is appropriate in situations where an installation consists of a single AP

Hidden Terminal



A wireless LAN. (a) A and C are hidden terminals when transmitting to B.

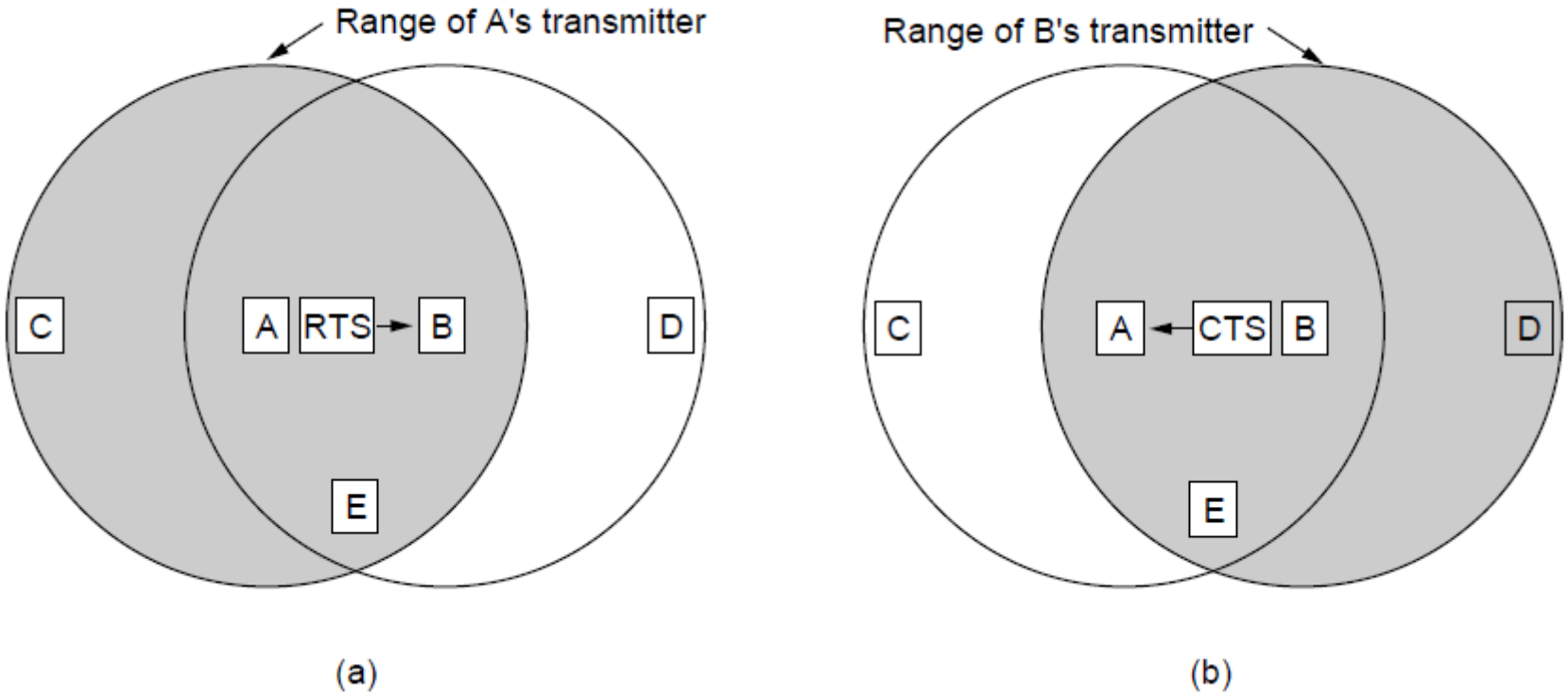
Exposed Terminal



(b)

A wireless LAN. (b) B and C are exposed terminals when transmitting to A and D.

RTS/CTS



The MACA protocol. (a) *A sending an RTS to B. (b) B responding* with a CTS to *A.*

Contention and Contention-Free Access

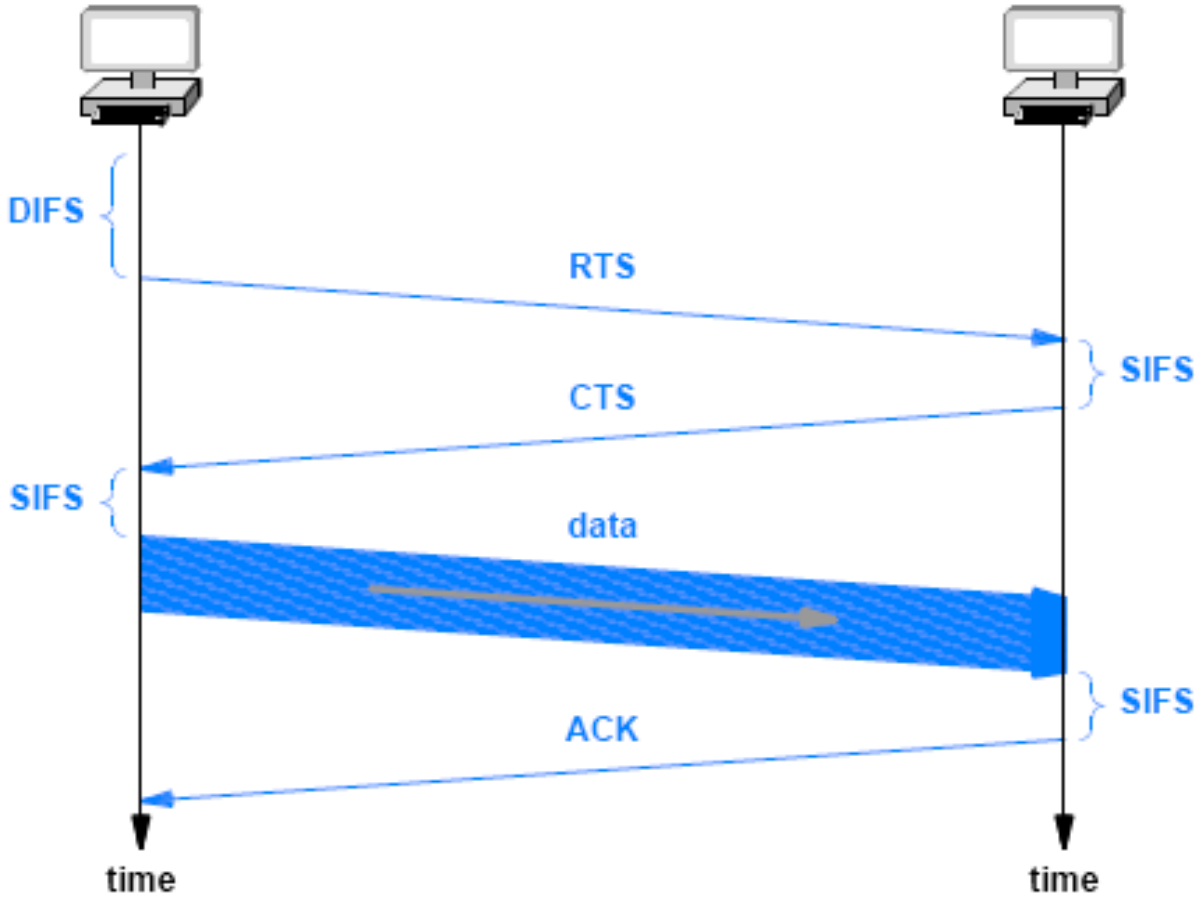
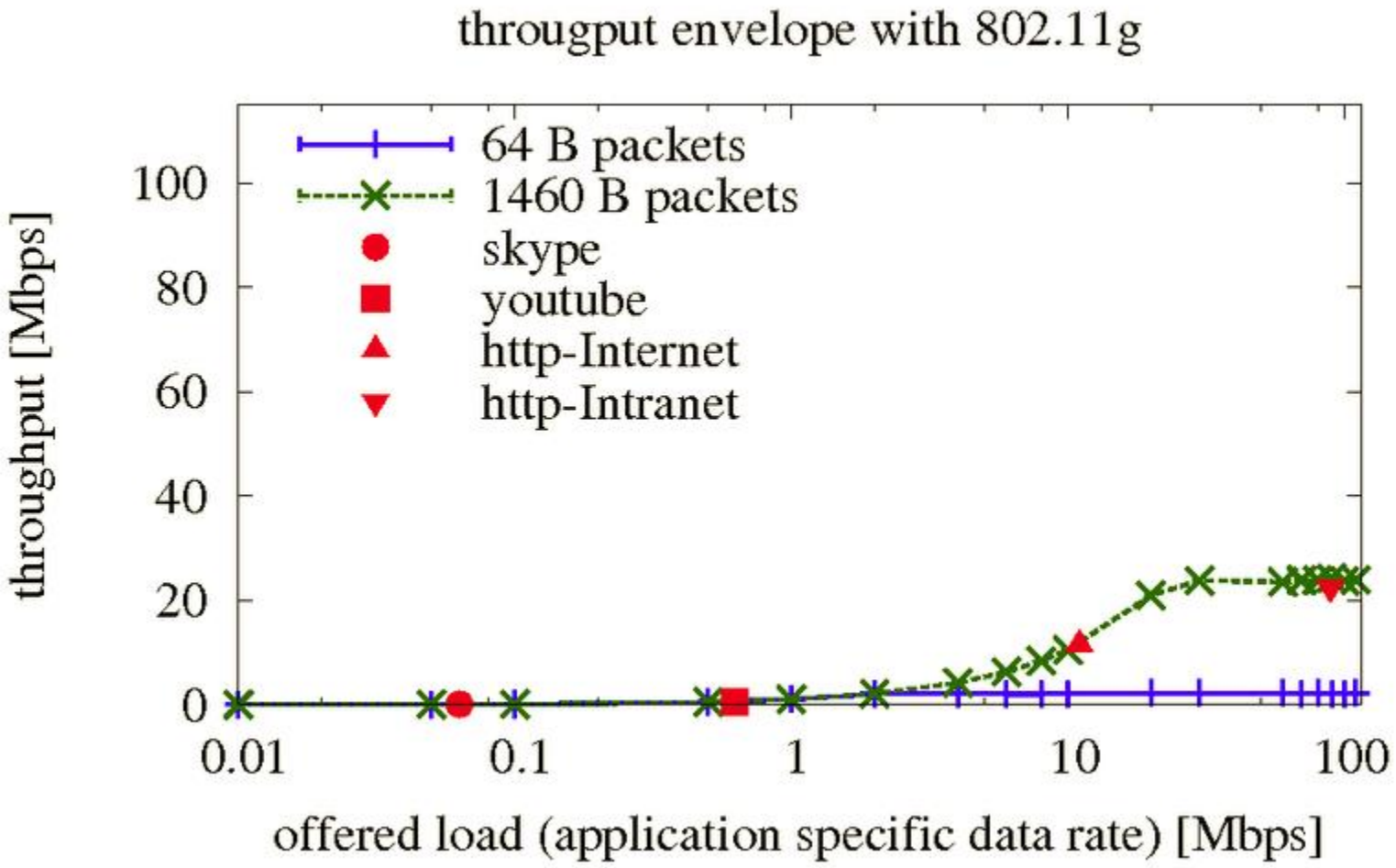
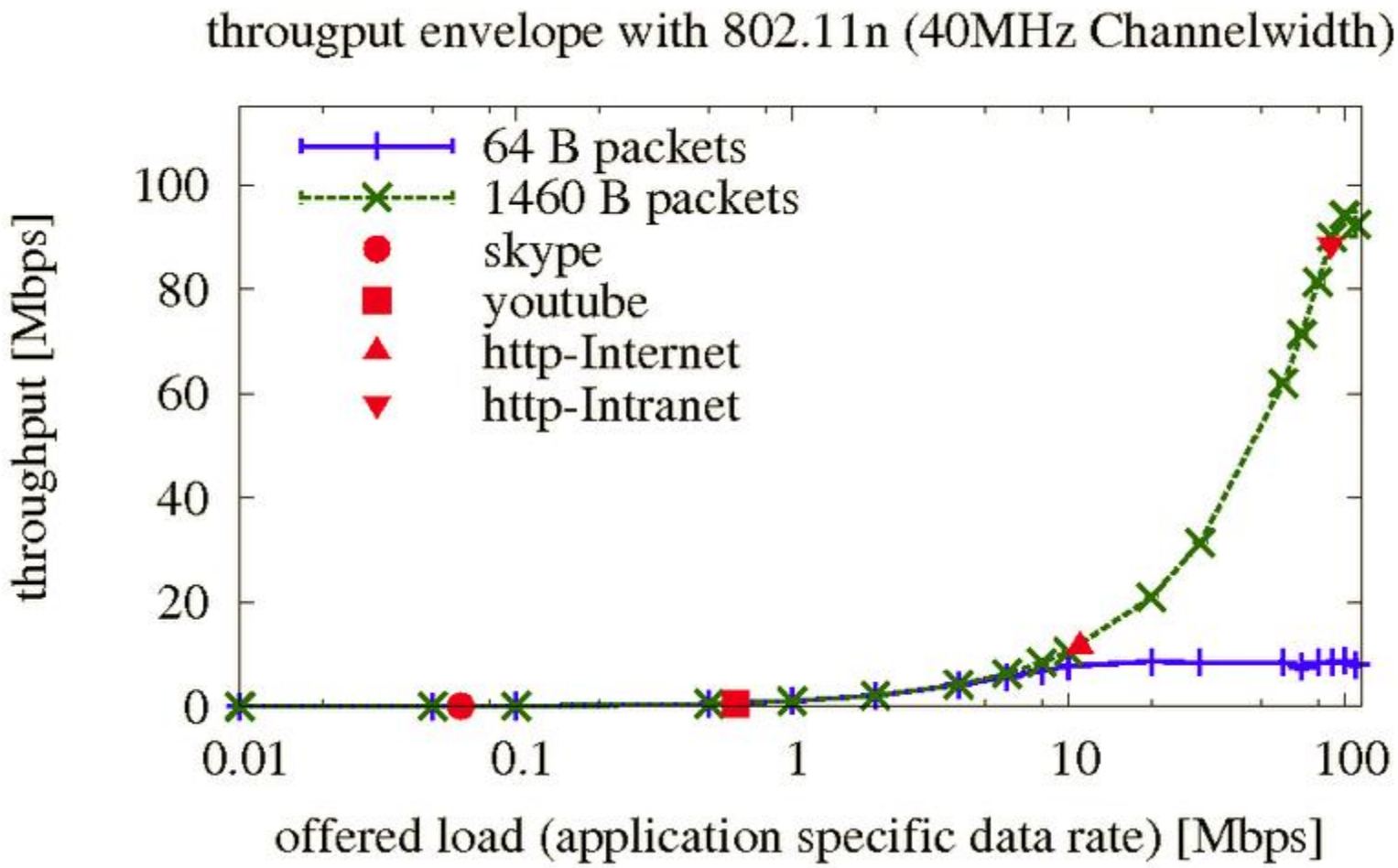


Illustration of CSMA/CA with SIFS and DIFS timing.

Contention and Contention-Free Access

- Physical separation among stations and electrical noise makes it difficult to distinguish between
  - weak signals, interference, and collisions
- Wi-Fi networks do not employ collision detection
  - That is, the hardware does not attempt to sense interference during a transmission
  - Instead, a sender waits for an acknowledgement (ACK) message
  - If no ACK arrives, the sender assumes the transmission was lost
    - and employs a backoff strategy similar to the strategy in wired Ethernet
- In practice, 802.11 networks that have few users and do not experience electrical interference seldom need retransmission
  - However, other 802.11 networks experience frequent packet loss and depend on retransmission


throughput envelope with 802.11g
64 B packets
1460 B packets
skype
youtube
http-Internet
http-Intranet
throughput [Mbps]
0
20
40
60
80
100
0.01
0.1
1
10
100
offered load (application specific data rate) [Mbps]


throughput envelope with 802.11n (40MHz Channelwidth)
64 B packets
1460 B packets
skype
youtube
http-Internet
http-Intranet
throughput [Mbps]
0
20
40
60
80
100
0.01
0.1
1
10
100
offered load (application specific data rate) [Mbps]