Wireless MAC Protocols
ECE 299.02 Spring 2007
Wired Vs Wireless Media Access

Both are on shared media.
Then, what’s really the problem?
Wired – Collision Detection

- Tx can transmit and sense at the same time
  - If (Transmitted_Signal != Sensed_Signal) → Sender knows it’s a Collision

- Channel Condition ~ identical at Tx and Rx
Collision Detection

- What is the aim of collision detection?

It's a transmitter's job:

To determine if the packet was successfully received without explicitly asking the receiver.
Wireless Media Disperse Energy

Distance

Signal power

SINR threshold

Sensitivity threshold

Distance
Wireless Media Disperse Energy

Will CSMA work in this case? How many yes, how many no?
Wireless Media Disperse Energy

Will CSMA work in this case?

Will CSMA/CD work?
Collision Detection Difficult

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

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

\[
SoI_B^A = \frac{P^A}{d_{AB}^\alpha} \quad \Rightarrow \quad SINR_B^A = \frac{P^A}{d_{AB}^\alpha} \quad N + \frac{P^C}{d_{CB}^\alpha}
\]

\[
I_B^C = \frac{P^C}{d_{CB}^\alpha}
\]
Red signal >> Blue signal

Red < Blue = collision

Distance

Signal power

SINR threshold

Sensitivity threshold

Distance

10
Important: C has not heard A, but can interfere at receiver B

C is the hidden terminal to A

Signal power

SINR threshold

Sensitivity threshold

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

Y is the exposed terminal to A
So, what do you do?
in a multi-hop ad hoc network?
A Project Idea!

- A node decides to intelligently choose a Carrier sensing threshold (T)

- The node senses channel
  - If signal > T, then node does not transmit
  - If signal < T, then don’t transmit

- Possible to guarantee no collisions?
A Project Idea!

Distance

Signal power

SINR threshold

Sensitivity threshold

Distance

X
A

B

C

D
Will this solve the wireless MAC problem?

Do not transmit in this region

Distance

Signal power

SINR threshold

Sensitivity threshold

X

A

B

C

D

T
Whatever the answer ...

This is an example of a good class project

If you came up with the idea,
Showed that it’s a new idea,
And evaluated it to demo how it performs
Today’s Discussions

- IEEE 802.11 overview - some raw data
  - Architecture
  - PHY specifications – Spread Spectrum radios: FH & DS
  - MAC specifications – DCF and PCF
  - Synchronization, Power management, Roaming, Scanning
  - Security

- Deliberations on 802.11 (DCF) MAC
  - Hidden terminal & Exposed terminal issues
  - Carrier sensing

- Some other ideas & open challenges
  - Could be interesting for the project
IEEE 802.11 – An overview
IEEE 802.11 in OSI Model

OSI Reference Model

Application Layer
Presentation Layer
Session Layer
Transport Layer
Network Layer
Data Link Layer
Logical Link Control (LLC) 802.2
Medium Access Control (MAC)
Physical Layer

Wireless
To develop a **MAC** and **PHY** spec for wireless connectivity for fixed, portable and moving stations in a local area.
Applications

Single Hop
- Home networks
- Enterprise networks (e.g., offices, labs, etc.)
- Outdoor areas (e.g., cities, parks, etc.)

Multi-hops
- Adhoc network of small groups (e.g., aircrafts)
- Balloon networks (SpaceData Inc.)
- Mesh networks (e.g., routers on lamp-posts)
802.11 Architecture - Two modes

BSS (Infrastructure Mode)

ESS

IBSS (Ad-Hoc Mode)
Two kinds of radios based on
- "Spread Spectrum"
- "Diffused Infrared"

Spread Spectrum radios based on
- Frequency hopping (FH)
- Direct sequence (DS)

Radio works in 2.4GHz ISM band --- license-free by FCC (USA), ETSI (Europe), and MKK (Japan)
- 1 Mbps and 2Mbps operation using FH
- 1, 2, 5.5, and 11Mbps operation using DSSS (FCC)
Why Spread Spectrum?

- $C = B \times \log_2 (1+S/N)$ . . . [Shannon]
- To achieve the same channel capacity $C$
  - Large $S/N$, small $B$
  - Small $S/N$, large $B$
  - Increase $S/N$ is inefficient due to the logarithmic relationship

![Diagram showing signal, noise, and bandwidth](image)

e.g. $B = 30$ KHz

![Diagram showing wider bandwidth for larger $B$](image)

e.g. $B = 1.25$ MHz
Spread Spectrum

Methods for spreading the bandwidth of the transmitted signal over a frequency band (spectrum) which is wider than the minimum bandwidth required to transmit the signal.

- Reduce effect of jamming
  - Military scenarios
- Reduce effect of other interferences
- More “secure”
  - Signal “merged” in noise and interference
Frequency Hopping SS (FHSS)

- 2.4GHz band divided into 75 1MHz subchannels
- Sender and receive agree on a hopping pattern (pseudo random series). 22 hopping patterns defined
- Different hopping sequences enable co-existence of multiple BSSs
- Robust against narrow-band interferences

One possible pattern:

```
f f f f f f f f f f
```
Simple radio design with FHSS
Data rates ~ 2 Mbps

Invented by Hedy Lamarr (Hollywood film star) in 1940, at age of 27, with musician George Antheil
Direct Sequence SS

- **Direct sequence (DS):** most prevalent
  - Signal is spread by a wide bandwidth pseudorandom sequence (code sequence)
  - Signals appear as wideband noise to unintended receivers

- Not for intra-cell multiple access
  - Nodes in the same cell use same code sequence
IEEE 802.11b DSSS

- ISM unlicensed frequency band (2.4GHz)
- Channel bandwidth: \( f_{\text{high}} - f_{\text{low}} = 22 \text{ MHz} \)
- 1MHz guard band
- Direct sequence spread spectrum in each channel
- 3 non-overlapping channels

<table>
<thead>
<tr>
<th>Channel</th>
<th>( f_{\text{low}} )</th>
<th>( f_{\text{high}} )</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2.401</td>
<td>2.423</td>
</tr>
<tr>
<td>2</td>
<td>2.404</td>
<td>2.428</td>
</tr>
<tr>
<td>3</td>
<td>2.411</td>
<td>2.433</td>
</tr>
<tr>
<td>4</td>
<td>2.416</td>
<td>2.438</td>
</tr>
<tr>
<td>5</td>
<td>2.421</td>
<td>2.443</td>
</tr>
<tr>
<td>6</td>
<td>2.426</td>
<td>2.448</td>
</tr>
<tr>
<td>7</td>
<td>2.431</td>
<td>2.453</td>
</tr>
<tr>
<td>8</td>
<td>2.436</td>
<td>2.458</td>
</tr>
<tr>
<td>9</td>
<td>2.441</td>
<td>2.463</td>
</tr>
<tr>
<td>10</td>
<td>2.446</td>
<td>2.468</td>
</tr>
<tr>
<td>11</td>
<td>2.451</td>
<td>2.473</td>
</tr>
</tbody>
</table>
Diffused Infrared

- Wavelength range from 850 – 950 nm
- For indoor use only
- Line-of-sight and reflected transmission
- 1 – 2 Mbps
PHY Sublayers

- Physical layer convergence protocol (PLCP)
  - Provides common interface for MAC
    - Offers carrier sense status & CCA (Clear channel assessment)
    - Performs channel synchronization / training

- Physical medium dependent sublayer (PMD)
  - Functions based on underlying channel quality and characteristics
    - E.g., Takes care of the wireless encoding
PLCP (802.11b)

- **Long preamble**: 192us
- **Short preamble**: 96us (VoIP, video)
PLCP (802.11b)

Note:

To send even one bit payload reliably, you will have to form a packet with the PLCP preamble and the PLCP header.

This constraints protocol design

You cannot arbitrarily exchange control messages.

What are the control messages in IEEE 802.11?
IEEE 802.11 MAC
802.11 MAC (DCF)

- CSMA/CA based protocol
  - Listen before you talk
  - CA = Collision avoidance (prevention is better than cure !!)

- Robust for interference
  - Explicit acknowledgment requested from receiver
    - for unicast frames
  - Only CSMA/CA for Broadcast frames

- Optional RTS/CTS offers Virtual Carrier Sensing
  - RTS/CTS includes duration of immediate dialog
  - Addresses hidden terminal problems
802.11 MAC (DCF)
Physical Carrier Sense & Backoff
MAC Management Layer

- **Synchronization**
  - Finding and staying with a WLAN
    - Uses TSF timers and beacons

- **Power Management**
  - Sleeping without missing any messages
    - Periodic sleep, frame buffering, traffic indication map

- **Association and Reassociation**
  - Joining a network
  - Roaming, moving from one AP to another
  - Scanning
Synchronization

- **Timing Synchronization Function (TSF)**
  - Enables synchronous waking/sleeping
  - Enables switching from DCF to PCF
  - Enables frequency hopping in FHSS PHY
    - Transmitter and receiver has identical dwell interval at each center frequency

- **Achieving TSF**
  - All stations maintain a local timer.
  - AP periodically broadcasts beacons containing timestamps, management info, roaming info, etc.
    - Not necessary to hear every beacon
  - Beacon synchronizes entire BSS
    - Applicable in infrastructure mode ONLY
  - Distributed TSF (for Independent BSS) more difficult
Power management

- Battery powered devices require power efficiency
  - LAN protocols assume idle nodes are always ON and thus ready to receive.
  - Idle-receive state key source of power wastage

- Devices need to power off during idle periods
  - Yet maintain an active session – tradeoff power Vs throughput

- Achieving power conservation
  - Allow idle stations to go to sleep periodically
  - APs buffer packets for sleeping stations
  - AP announces which stations have frames buffered when all stations are awake – called Traffic Indication Map (TIM)
    - TSF assures AP and Power Save stations are synchronized
    - TSF timer keeps running when stations are sleeping

- Independent BSS also have Power Management
  - Similar in concept, distributed approach
Roaming & Scanning

- Stations switch (roam) to different AP
  - When channel quality with current AP is poor

- Scanning function used to find better AP
  - Passive Scanning → Listen for beacon from different Aps
  - Active Scanning → Exchange explicit beacons to determine best AP

- Station sends Reassociation Request to new AP
  - If Reassociation Response successful → Roaming

- If AP accepts Reassociation Request
  - AP indicates Reassociation to the Distribution System
  - Distribution System information is updated
  - Normally old AP is notified through Distribution System
MAC management frame

- Beacon
  - Timestamp, Beacon Interval, Capabilities, ESSID, Supported Rates, parameters
  - Traffic Indication Map
- Probe
  - ESSID, Capabilities, Supported Rates
- Probe Response
  - Timestamp, Beacon Interval, Capabilities, ESSID, Supported Rates, parameters
  - Same for Beacon except for TIM
- Association Request
  - Capability, Listen Interval, ESSID, Supported Rates
- Association Response
  - Capability, Status Code, Station ID, Supported Rates
MAC Management Frame

- **Reassociation Request**
  - Capability, Listen Interval, ESSID, Supported Rates, Current AP Address

- **Reassociation Response**
  - Capability, Status Code, Station ID, Supported Rates

- **Disassociation**
  - Reason code

- **Authentication**
  - Algorithm, Sequence, Status, Challenge Text

- **Deauthentication Reason**
Security

- Range of attacks huge in wireless
  - Easy entry into the network
  - Jamming, selfish behavior, spatial overhearing

- Securing the network harder than wired networks
  - Especially in distributed environments

- WEP → symmetric 40 or 128-bit encryption
- WPA: Wi-Fi protected access
  - Temporal key integrity protocol (TKIP) – better
  - User authentication

- IEEE 802.11i – Efforts toward higher security
The deliberations for 802.11
(Hidden and Exposed Terminals, Carrier Sensing)
Hidden Terminal Problem

Why such an important problem with CSMA?
- Node X can carrier sense, and defer transmission
- Probability of simultaneous transmission negligible
Hidden Terminal Problem

How about increasing carrier sense range??

- E will defer on sensing carrier → no collision !!!
Hidden Terminal Problem

- But what if barriers/obstructions??
  - E doesn’t hear C → Carrier sensing does not help

This motivates the notion of channel reservation through RTS/CTS
RTS/CTS

- Does it solve hidden terminals?
  - What should be the carrier sensing zone?
    - Same as communication zone?

E does not receive CTS successfully → Can later initiate transmission to D. Hidden terminal problem remains.
RTS/CTS + Larger CS Zone

Now can HT problem be solved?

But what if barriers/obstructions? E will not carrier sense. Thus can cause hidden terminal problem again.
Exposed Terminal

- B should be able to transmit to A
  - RTS prevents this
Exposed Terminal

- B should be able to transmit to A
  - Carrier sensing makes the situation worse
Thoughts!

- 802.11 does not solve HT/ET completely
  - Only alleviates the problem through RTS/CTS and recommends larger CS zone

- Large CS zone aggravates exposed terminals
  - Spatial reuse reduces → A tradeoff
  - RTS/CTS packets also consume bandwidth
  - Moreover, backing off mechanism is also wasteful

The search for the best MAC protocol is still on. However, 802.11 is being optimized too. Thus, wireless MAC research still alive
MACA-BI [GerlaUCLA]

- RTS/CTS/ACK are control overhead
  - Needed to reduce it

- Rx predicts trasmission from the Tx
  - Traffic estimation (???)

- If Rx thinks Tx has pending packets for Rx
  - Rx transmits RTR to Tx
  - Tx replies with Data

- Improves MACA with no RTS/ACK
  - improvement but not too much
DBTMA [HaasCornell98]

- **Rx Busy tone**
  - RTS → CTS
  - Signal X

- **Tx Busy tone**
  - CTS → RTS
  - Signal X
Implicit MACKnowldgment

- APs typically backlogged with traffic
  - Persistent traffic → possibility of optimization

- We propose an implicit ACK optimization
  - Piggyback the CTS with ACK for previous dialog

![Diagram showing IEEE 802.11 protocol with Implicit ACK]

**Gain**

Implicit ACK For Previous Packet
Hybrid Channel Access

The optimization timeline

802.11

Implicit ACK

Hybrid Channel Access

Backoff

Backoff

Backoff

Backoff

RTS

CTS

Data

ACK

RTS

CTS +ACK

Data

RTS

Poll +ACK

Data
Seedex [KumarUIUC03]

- Forget channel reservation and backoff
- Instead, let nodes pick sequence of time slots

- Decides to probably transmit in some, else listen
- Transmit slots chosen using a random seed
- Publishes the seed to 2-hop neighbors

- When PT slots arrive, nodes transmit with
  - Probability “p”
  - “p” chosen as a function of overlapping neighbors
Hot Research Topics

- Power control increases spatial reuse
  - Whisper in the room so that many people can talk

- Rate control based on channel quality

- Exploit channel diversity
  - Utilize multiple channels to parallelize dialogs

- Exploit spatial diversity
  - Use directional antennas to interfere over smaller region (next class)

... and many more topics
Questions ?
PLCP

- PLCP has two structures.
  - All 802.11b systems have to support Long preamble.
  - Short preamble option is provided to improve efficiency when transmitting voice, VoIP, streaming video.

- PLCP Frame format
  - PLCP preamble
    - SFD: start frame delimiter
  - PLCP header
PLCP Header

- 8-bit signal or data rate (DR) indicates how fast data will be transmitted
- 8-bit service field reserved for future
- 16-bit length field indicating the length of the ensuing MAC PDU (MAC sublayer’s Protocol Data Unit)
- 16-bit Cyclic Redundancy Code
Power management approach

- Allow idle stations to go to sleep
  - station’s power save mode stored in AP
- APs buffer packets for sleeping stations.
  - AP announces which stations have frames buffered
  - Traffic Indication Map (TIM) sent with every Beacon
- Power Saving stations wake up periodically
  - listen for Beacons
- TSF assures AP and Power Save stations are synchronized
  - stations will wake up to hear a Beacon
  - TSF timer keeps running when stations are sleeping
  - synchronization allows extreme low power operation
- Independent BSS also have Power Management
  - similar in concept, distributed approach
Scanning

- Scanning required for many functions.
  - finding and joining a network
  - finding a new AP while roaming
  - initializing an Independent BSS (ad hoc) network
- 802.11 MAC uses a common mechanism for all PHY.
  - single or multi channel
  - passive or active scanning
- Passive Scanning
  - Find networks simply by listening for Beacons
- Active Scanning
  - On each channel Send a Probe, Wait for a Probe Response
- Beacon or Probe Response contains information necessary to join new network.
Active scanning example

Steps to Association:

- Station sends Probe.
- APs send Probe Response.
- Station selects best AP.
- Station sends Association Request to selected AP.
- AP sends Association Response.