802.11 Wireless

ITS 625
(Adapted from ITS/CS 575 Lectures
© 2007 by Hans Kruse and Carl Bruggman)
Introduction

- 802.11 is not “Ethernet over radiowaves”
  - The protocol and the frame format are different
- 802.11 Resource:
802.11 Basics

- 802.11 is a family of standards
  - Different frequency bands
  - Different encoding methods
  - Different range
- 802.11a operates in the 5GHz band, everything else is in the 2.5GHz band
- We are not alone..... (in the 2.5GHz band)
  - Cordless Phones
  - Bluetooth
  - Baby Monitors
The 802 Family

From “802.11 Wireless Networks: The Definitive Guide”, by Matthew Gast
Physical Layers

- 802.11 (DSSS)
  - 1 Mbps and 2 Mbps
- 802.11b (HR/DSSS)
  - 5.5 Mbps and 11 Mbps
- 802.11a (OFDM at 5GHz)
  - n-QAM/Convolutional Coding - 6 Mbps to 54 Mbps
- 802.11g (ERP)
  - Collection of standards
    - Compatible with 802.11 and 802.11b
    - OFDM, same rates as 802.11a, at 2.5 GHz
802.11 Infrastructure Mode

- ESS - Extended Service Set
- SSID - Service Set Identifier
  - The “Name” of the network

From "802.11 Wireless Networks: The Definitive Guide", by Matthew Gast
Ad-Hoc Network Mode

- Direct communication station to station
- With Zeroconf, mDNS, and Service Discovery
  - Create small peer-to-peer networks automatically
  - Exchange information among laptops, PDAs, printers, etc.
- Most operating systems allow the user to select the network mode
- A bad choice by the user means misery for everyone.....
Basic MAC Operation

- CSMA/CA - Carrier Sense Multiple Access with Collision Avoidance
  - Also called DCF - Distributed Coordination Function
    - Listen for a current transmission
    - After transmissions stop, wait for the DIFS (DCF Inter-Frame Spacing) plus a random additional time
    - First transmitter “wins”
    - Next frame in a sequence is sent after a shorter SIFS (Short Inter-Frame Spacing), locking out other transmitters
MAC Timing

From “802.11 Wireless Networks: The Definitive Guide”, by Matthew Gast
What About Collisions?

• Non-broadcast packets are acknowledged
• Un-acknowledged frames are retransmitted
  • Retransmissions wait for a longer than normal back-off period
  • A configurable counter limits the number of re-transmissions for a frame
Hidden Nodes

- Two stations can both see the AP, but not each other
RTS/CTS and the NAV

• If hidden nodes exist, transmissions will collide
  • Both frames are lost
  • Random back-off before retransmit should fix the problem
  • Expensive if this happens a lot with large frames

• Stations can send a RTS frame
  • Include the Network Allocation Vector (NAV), essentially “I need the network for NAV amount of time”
  • AP responds with CTS including a NAV
    • The hidden station uses this as a “virtual carrier sense”
NAV-based carrier sense

From “802.11 Wireless Networks: The Definitive Guide”, by Matthew Gast
Startup Sequence

- Station listens for beacons
- Station/user select a network to attach to
- Authenticate
  - “Open” -- just send me your MAC address
  - “Shared Key” -- 802.11 standard is so weak that this is rarely used
- Associate
  - Station sends request
  - AP accepts/rejects request, assigns ID
Security 802.11

• Authentication
  • Station to Network
  • Network to Station not included

• Encryption
Options

• 802.1X
  • Enterprise solution
  • AP relays authentication to a back-end server
    • Usually RADIUS (Remote Authentication Dial In User Service)
  • Lots of options for authentication protocols

• WPA (Wi-Fi Protected Access)
  • Shared key ("Personal")
  • Enterprise