

Wireless Networks

Lecture 12: Wireless LAN

802.11 MAC

Peter Steenkiste
CS and ECE, Carnegie Mellon University
Peking University, Summer 2016

Peter A. Steenkiste, CMU

1

Outline

- **802 protocol overview**
- **Wireless LANs – 802.11**
 - » Overview of 802.11
 - » 802.11 MAC, frame format, operations
 - » 802.11 management
 - » 802.11*
 - » Deployment example
- **Personal Area Networks – 802.15**

Peter A. Steenkiste, CMU

2

IEEE 802.11 Overview

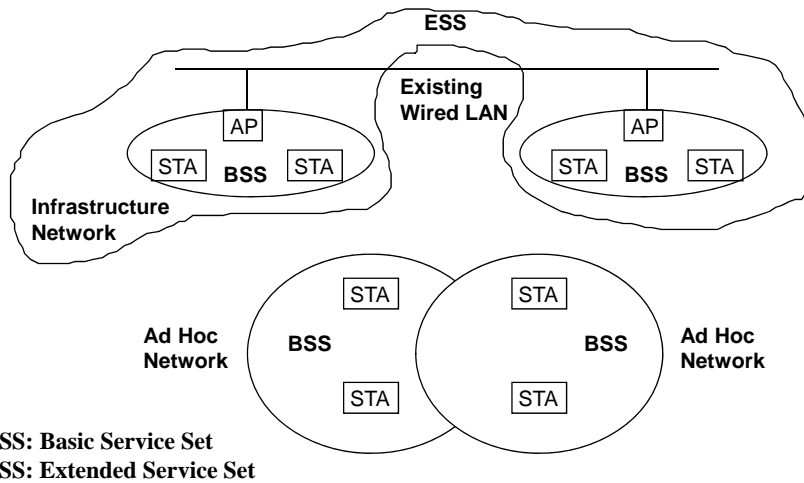
- **Adopted in 1997 with goal of providing**
 - » Access to services in wired networks
 - » High throughput
 - » Highly reliable data delivery
 - » Continuous network connection, e.g. while mobile
- **The protocol defines**
 - » MAC sublayer
 - » MAC management protocols and services
 - » Several physical (PHY) layers: IR, FHSS, DSSS, OFDM
- **Wi-Fi Alliance is industry group that certifies interoperability of 802.11 products**

Infrastructure and Ad Hoc Mode

- **Infrastructure mode: stations communicate with one or more access points which are connected to the wired infrastructure**
 - » What is deployed in practice
- **Two modes of operation:**
 - » Distributed Control Functions - DCF
 - » Point Control Functions – PCF
 - » PCF is rarely used - inefficient
- **Alternative is “ad hoc” mode: multi-hop, assumes no infrastructure**
 - » Rarely used, e.g. military
 - » Hot research topic!



802.11 Architecture



Peter A. Steenkiste, CMU

5

Terminology for DCF

- **Stations and access points**
- **BSS - Basic Service Set**
 - » One access point that provides access to wired infrastructure
 - » Infrastructure BSS
- **ESS - Extended Service Set**
 - » A set of infrastructure BSSs that work together
 - » APs are connected to the same infrastructure
 - » Tracking of mobility
- **DS – Distribution System**
 - » AP communicates with each other
 - » Thin layer between LLC and MAC sublayers

Peter A. Steenkiste, CMU

6

Outline

- **802 protocol overview**
- **Wireless LANs – 802.11**
 - » Overview of 802.11
 - » 802.11 MAC, frame format, operations
 - » 802.11 management
 - » 802.11*
 - » Deployment example
- **Personal Area Networks – 802.15**

Features of 802.11 MAC protocol

- **Supports MAC functionality**
 - » Addressing
 - » CSMA/CA
- **Error detection (FCS)**
- **Error correction (ACK frame)**
- **Flow control: stop-and-wait**
- **Fragmentation (More Frag)**
- **Collision Avoidance (RTS-CTS)**

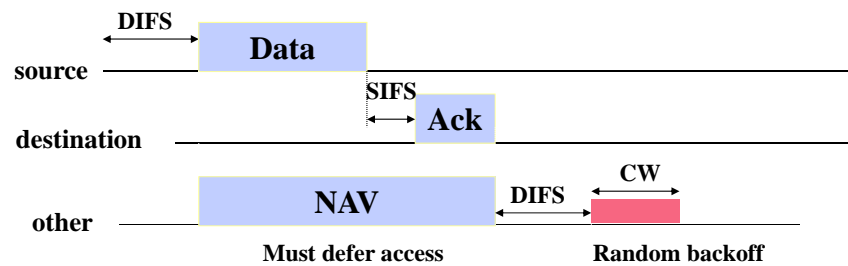
How Does WiFi Differ from Wired Ethernet?

- **Signal strength drops off quickly with distance**
 - » Path loss exponent is highly dependent on context
- **Should expect higher error rates**
 - » Solutions
- **Makes it impossible to detect collisions**
 - » Difference between signal strength at sender and receiver is too big
 - » Solutions
- **Senders cannot reliably detect competing senders resulting in hidden terminal problems**
 - » Solutions

Carrier Sense Multiple Access

- **Before transmitting a packet, sense carrier**
- **If it is idle, send**
 - » After waiting for one DCF inter frame spacing (DIFS)
- **If it is busy, then**
 - » Wait for medium to be idle for a DIFS (DCF IFS) period
 - » Go through exponential backoff, then send (non-persistent solution)
 - » Want to avoid that several stations waiting to transmit automatically collide
 - » Cost of back off is high and expect a lot of contention
- **Wait for ack**
 - » If there is one, you are done
 - » If there isn't one, assume there was a collision, retransmit using exponential backoff

DCF mode transmission without RTS/CTS



Peter A. Steenkiste, CMU

11

Exponential Backoff

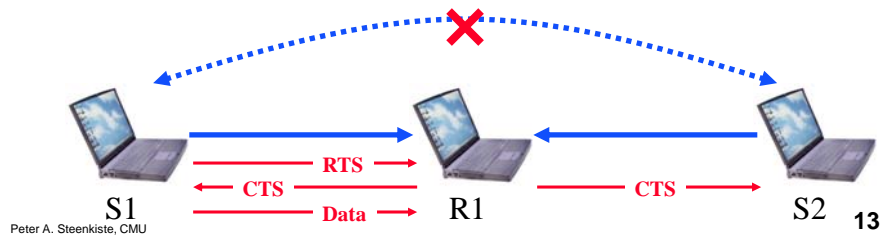
- **Force stations to wait for random amount of time to reduce the chance of collision**
 - › Backoff period increases exponential after each collision
 - › Similar to Ethernet
- **If the medium is sensed it is busy:**
 - › Wait for medium to be idle for a DIFS (DCF IFS) period
 - › Pick random number in contention window (CW) = backoff counter
 - › Decrement backoff timer until it reaches 0
 - But freeze counter whenever medium becomes busy
 - › When counter reaches 0, transmit frame
 - › If two stations have their timers reach 0; collision will occur;
- **After every failed retransmission attempt:**
 - › increase the contention window exponentially
 - › $2^i - 1$ starting with CW_{min} up to CW_{max} e.g., 7, 15, 31, ...

Peter A. Steenkiste, CMU

12

Collision Avoidance

- **Difficult to detect collisions in a radio environment**
 - » While transmitting, a station cannot distinguish incoming weak signals from noise – its own signal is too strong
- **Why do collisions happen?**
 - » Near simultaneous transmissions
 - Period of vulnerability: propagation delay
 - » Hidden node situation: two transmitters cannot hear each other and their transmission overlap at a receiver



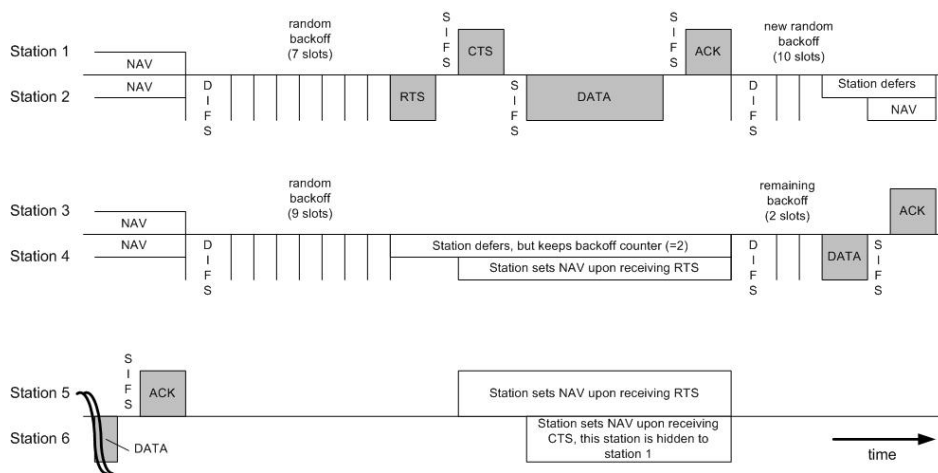
Request-to-Send and Clear-to-Send

- **Before sending a packet, first send a station first sends a RTS**
 - » Collisions can still occur but chance is relatively small since RTS packets are short
- **The receiving station responds with a CTS**
 - » Tells the sender that it is ok to proceed
- **RTS and CTS use shorter IFS to guarantee access**
 - » Effectively priority over data packets
- **First introduced in the Multiple Access with Collision Avoidance (MACA) protocol**
 - » Fixed problems observed in Aloha

Virtual Carrier Sense

- **RTS and CTS notify nodes within range of sender and receiver of upcoming transmission**
- **Stations that hear either the RTS or the CTS “remember” that the medium will be busy for the duration of the transmission**
 - » Based on a Duration ID in the RTS and CTS
 - » Note that they may not be able to hear the data packet!
- **Virtual Carrier Sensing: stations maintain Network Allocation Vector (NAV)**
 - » Time that must elapse before a station can sample channel for idle status
 - » Consider the medium to be busy even if it cannot sense a signal

Use of RTS/CTS



Some More MAC Features

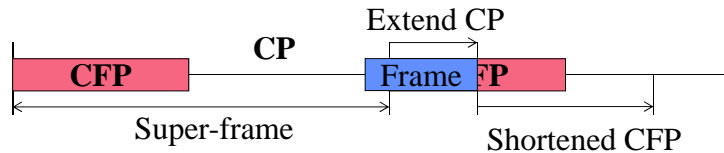
- **Use of RTS/CTS is controlled by an RTS threshold**
 - » RTS/CTS is only used for data packets longer than the RTS threshold
 - » Pointless to use RTS/CTS for short data packets – high overhead!
- **Number of retries is limited by a Retry Counter**
 - » Short retry counter: for packets shorter than RTS threshold
 - » Long retry counter: for packets longer than RTS threshold
- **Packets can be fragmented.**
 - » Each fragment is acknowledged
 - » But all fragments are sent in one sequence
 - » Sending shorter frames can reduce impact of bit errors
 - » Lifetime timer: maximum time for all fragments of frame

Features of 802.11 MAC protocol

- **Supports MAC functionality**
 - » Addressing
 - » CSMA/CA
- **Error detection (FCS)**
- **Error correction (ACK frame)**
- **Flow control: stop-and-wait**
- **Fragmentation (More Frag)**
- **Collision Avoidance (RTS-CTS)**

Now What about PCF?

- IEEE 802.11 combines random access with a “taking turns” protocol
 - » DCF (Distributed Coordination Mode) – Random access
 - CP (Contention Period): CSMA/CA is used
 - » PCF (Point Coordination Mode) – Polling
 - CFP (Contention-Free Period): AP polls hosts



Peter A. Steenkiste, CMU

19

Playing Games with Inter Frame Spacing

- Assigning different IFS effectively provides a mechanism for prioritizing packets and events
- SIFS - short IFS: for high priority transmissions
- PIFS – PCF IFS: used by PCF during contention-free period
- DIFS – DCF IFS: used for contention-based services
- EIFS – extended IFS: used when there is an error

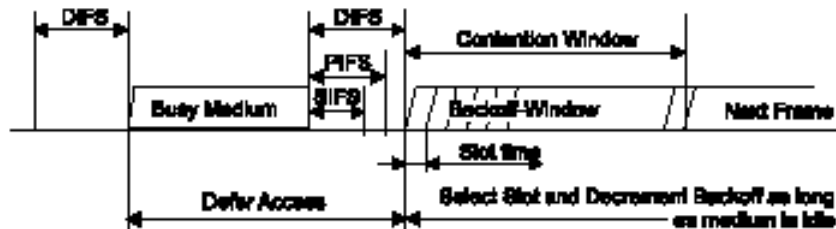


Peter A. Steenkiste, CMU

20

Effect of Different IFS

Immediate access when medium is free \geq DIFS



- PCF transmissions effectively get priority over DCF transmission because they use a shorter IFS

PCF Operation Overview

- **PC – Point Coordinator**
 - › Uses polling – eliminates contention
 - › Polling list ensures access to all registered stations
 - › Over DCF but uses a PIFS instead of a DIFS – gets priority
- **CFP – Contention Free Period**
 - › Alternate with DCF
- **Periodic Beacon – contains length of CFP**
 - › NAV prevents transmission during CFP
 - › CF-End – resets NAV
- **CF-Poll – Contention Free Poll by PC**
 - › Stations can return data and indicate whether they have more data
 - › CF-ACK and CF-POLL can be piggybacked on data

And What about Ad Hoc?

- **Infrastructure mode: access points relay packets**
 - » Based on an Infrastructure BSS
 - » APs are connected through a distribution system
- **Ad-hoc mode: no fixed network infrastructure**
 - » Based on an Independent BSS
 - » A wireless endpoint sends and all nodes within range can pick up signal
 - » Each packet carries destination and source address
 - » Effectively need to implement a “network layer”
 - How do know who is in the network?
 - Routing?
 - Security?
 - » Research area – discussed later in the course

Summary WiFi

- **Supports infrastructure and ad hoc mode**
- **Uses ACKs to detect collisions**
- **Uses RTS-CTS to avoid hidden terminals**
 - » Adds virtual carrier sense to physical carrier sense
 - » Almost never used because of overhead
- **Supports a point control function in addition to distributed control**
 - » Supports scheduled access in addition to random access
 - » Almost never used because of overhead