18-452/18-750
Wireless Networks and Applications
Lecture 9: Wireless LANs
Aloha and 802 Wireless

Peter Steenkiste

Spring Semester 2017

http://www.cs.cmu.edu/~prs/wirelessS17/

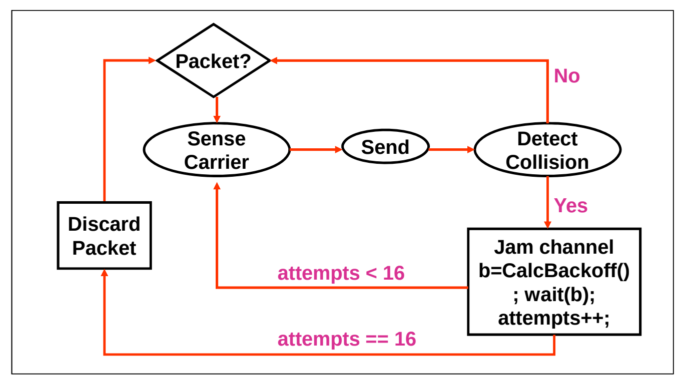
Outline

- **Data link fundamentals**
  - » **And what changes in wireless**
- **Aloha**
- **Ethernet**
- **Wireless-specific challenges**
- **802.11 and 802.15 wireless standards**

"Regular" Ethernet CSMA/CD

- **Multiple Access: multiple hosts are competing for access to the channel**
- **Carrier-Sense: make sure the channel is idle before sending – "listen before you send"**
- **Collision Detection: collisions are detected by listening on the medium and comparing the received and transmitted signals**
- **Collisions results in 1) aborting the colliding transmissions and 2) retransmission of the packets**
- **Exponential backoff is used to reduce the chance of repeat collisions**
  - » **Also effectively reduces congestion**

Carrier Sense Multiple Access/ Collision Detection (CSMA/CD)



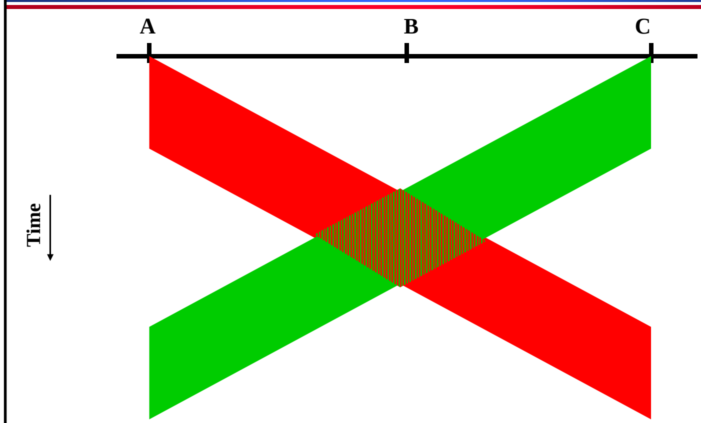
Ethernet Backoff Calculation

- Challenge: how do we avoid that two nodes retransmit at the same time collision
- Exponentially increasing random delay
  - » Infer “number” senders from # of collisions
  - » More senders → increase wait time
- First collision: choose K from {0,1}; delay is K x 512 bit transmission times
- After second collision: choose K from {0,1,2,3}
- After ten or more collisions, choose K from {0,1,2,3,4,…,1023}

How to Handle Transmission When Line is Sensed Busy

- *p-persistent scheme*:
  - » Transmit with probability p once the channel goes idle
  - » Delay the transmission by t_{prop} with the probability (1-p)
- *1-persistent scheme*: p = 1
  - » E.g. Ethernet
- *nonpersistent scheme*:
  - » Reschedule transmission for a later time based on a retransmission delay distribution (e.g. exp backoff)
  - » Senses the channel at that time
  - » Repeat the process
- When is each solution most appropriate?

Collisions



Dealing with Collisions

- Collisions will happen: nodes can start to transmit “simultaneously”
  - » Vulnerability window depends on length of wire
- Recovery requires that both transmitters can detect the collision reliably
  - » Clearly a problem as shown on previous slide
- How can we guarantee detection?
  - » Packets must be “long enough” and,
  - » Wires must be short enough
  - » This guarantees that ALL nodes will see both packets simultaneously, i.e., see the collision
  - » Not really relevant to wireless

So What about Wireless?

- Depends on many factors, but high level:
- Random access solutions are a good fit for data in the unlicensed spectrum
  - » Lower control complexity, especially for contention-based protocols (e.g., Ethernet)
  - » There may not always be a centralized controller
  - » May need to support multi-hop
  - » Also used in many unlicensed bands
- Cellular uses scheduled access
  - » Need to be able to guarantee performance
  - » Have control over spectrum – simplifies scheduled access
  - » More on this later in the course

Summary

- Wireless uses the same types of protocols as wired networks
  - » But it is inherently a multiple access technology
- Some fundamental differences between wired and wireless may result in different design choices
  - » Higher error rates
  - » Must support variable bit rate communication
  - » Signal propagation and radios are different

Outline

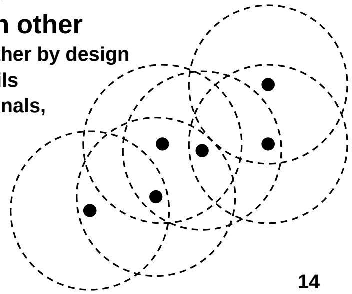
- Data link fundamentals
  - » And what changes in wireless
- Aloha
- Ethernet
- Wireless-specific challenges
- 802.11 and 802.15 wireless standards

Wireless Ethernet is a Good Idea, but …

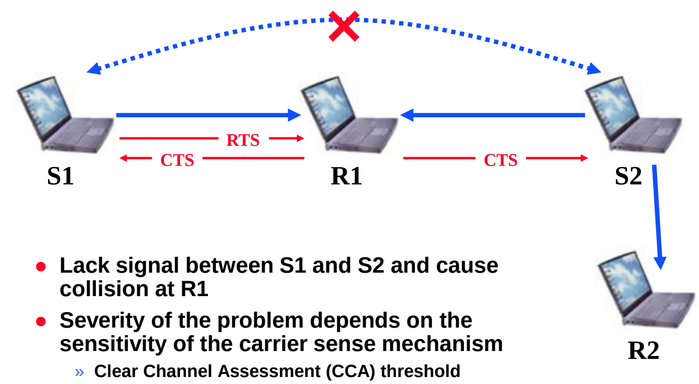
- Attenuation varies with media
  - » Also depends strongly on distance, frequency
- Wired media have exponential dependence
  - » Received power at d meters proportional to 10^{-kd}
  - » Attenuation in dB = *k d*, where *k* is dB/meter
- Wireless media has logarithmic dependence
  - » Received power at d meters proportional to d^{-n}
  - » Attenuation in dB = *n log d*, where *n* is path loss exponent; *n=2* in free space
  - » Signal level maintained for much longer distances?
- But we are ignoring the constants!
  - » Wireless attenuation at 2.4 GHz: 60-100 dB
  - » In practice numbers can be much lower for wired

Implications for Wireless Ethernet

- Collision detection is not practical
  - » Ratio of transmitted signal power to received power is too high at the transmitter
  - » Transmitter cannot detect competing transmitters (is deaf while transmitting)
  - » So how do you detect collisions?
- Not all nodes can hear each other
  - » Ethernet nodes can hear each other by design
  - » “Listen before you talk” often fails
  - » Hidden terminals, exposed terminals,
  - » Capture effects
- Made worse by fading
  - » Changes over time!

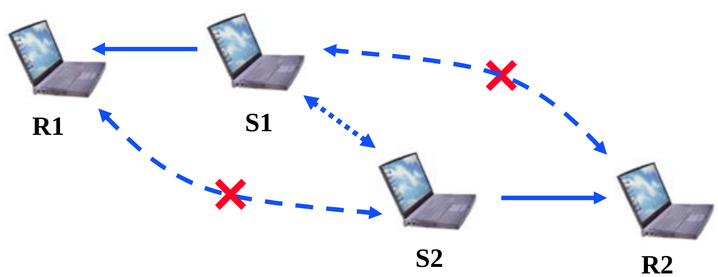


Hidden Terminal Problem



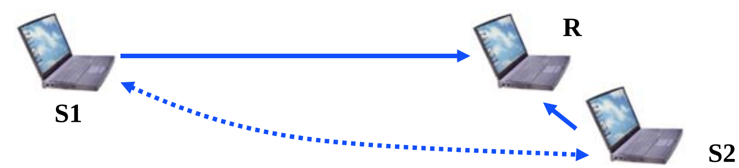
- Lack signal between S1 and S2 and cause collision at R1
- Severity of the problem depends on the sensitivity of the carrier sense mechanism
  - » Clear Channel Assessment (CCA) threshold

Exposed Terminal Problem



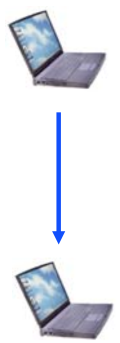
- Carrier sense prevents two senders from sending simultaneously although they do not reach each other’s receiver
- Severity again depends on CCA threshold
  - » Higher CCA reduces occurrence of exposed terminals, but can create hidden terminal scenarios

Capture Effect



- Sender S2 will almost always “win” if there is a collision at receiver R.
- Can lead to extreme unfairness and even starvation.
- Solution is power control
  - » Very difficult to manage in a non-provisioned environment!

Wireless Packet Networking Problems



- Some nodes suffer from more interference than others
  - » Node density
  - » Traffic volume sent by neighboring nodes
- Leads to unequal throughput
- Similar to wired network: some flows traverse tight bottleneck while others do not

Summary

- Wireless signal propagation creates problems for “wireless Ethernet”
  - » Collision Detection is not possible
  - » Hidden and exposed terminals
  - » Capture effect
- Aloha was the first wireless data communication protocol
  - » Simple: send whenever you want to
  - » Has low latency but low capacity

Outline

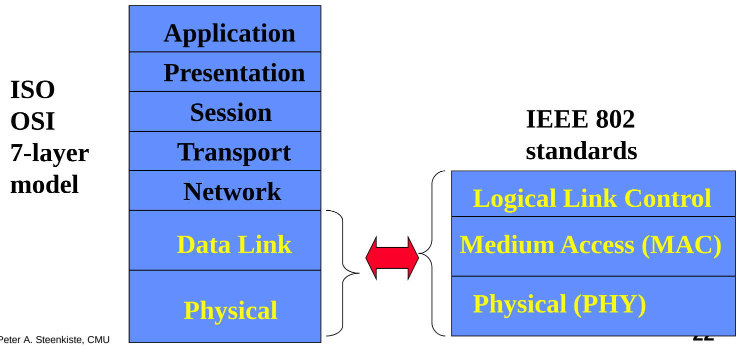
- Data link fundamentals
  - » And what changes in wireless
- Ethernet
- Aloha
- Wireless-specific challenges
- 802.11 and 802.15 wireless standards
  - » 802 protocol overview
  - » Wireless LANs – 802.11
  - » Personal Area Networks – 802.15

History

- Aloha wireless data network
- Car phones
  - » Big and heavy “portable” phones
  - » Limited battery life time
  - » But introduced people to “mobile networking”
  - » Later turned into truly portable cell phones
- Wireless LANs
  - » Originally in the 900 MHz band
  - » Later evolved into the 802.11 standard
  - » Later joined by the 802.15 and 802.16 standards
- Cellular data networking
  - » Data networking over the cell phone
  - » Many standards – throughput is the challenge

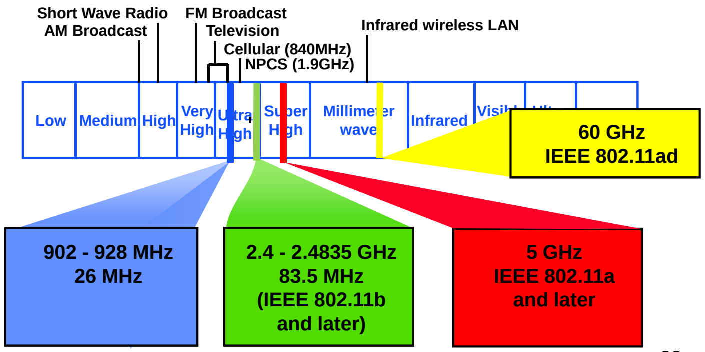
Standardization of Wireless Networks

- Wireless networks are standardized by IEEE
- Under 802 LAN MAN standards committee



Frequency Bands

- Industrial, Scientific, and Medical (ISM) bands
- Generally called "unlicensed" bands



The 802 Class of Standards

- List on next slide
- Some standards apply to all 802 technologies
  - » E.g. 802.2 is LLC
  - » Important for inter operability
- Some standards are for technologies that are outdated
  - » Not actively deployed anymore
  - » E.g. 802.6

- 802.1 Overview Document Containing the Reference Model, Tutorial, and Glossary
- 802.1 b Specification for LAN Traffic Prioritization
- 802.1 q Virtual Bridged LANs
- 802.2 Logical Link Control
- 802.3 Contention Bus Standard 1 Obase 5 (Thick Net)
  - » 802.3a Contention Bus Standard 10base 2 (Thin Net)
  - » 802.3b Broadband Contention Bus Standard 10broad 36
  - » 802.3d Fiber-Optic InterRepeater Link (FOIRL)
  - » 802.3e Contention Bus Standard 1 base 5 (Starlan)
  - » 802.3i Twisted-Pair Standard 10base T
  - » 802.3j Contention Bus Standard for Fiber Optics 10base F
  - » 802.3u 100-Mb/s Contention Bus Standard 100base T
  - » 802.3x Full-Duplex Ethernet
  - » 802.3z Gigabit Ethernet
  - » 802.3ab Gigabit Ethernet over Category 5 UTP
- 802.4 Token Bus Standard
- 802.5 Token Ring Standard
  - » 802.5b Token Ring Standard 4 Mb/s over Unshielded Twisted-Pair
  - » 802.5f Token Ring Standard 16-Mb/s Operation
- 802.6 Metropolitan Area Network DQDB
- 802.7 Broadband LAN Recommended Practices
- 802.8 Fiber-Optic Contention Network Practices
- 802.9a Integrated Voice and Data LAN
- 802.10 Interoperable LAN Security
- 802.11 Wireless LAN Standard
- 802.12 Contention Bus Standard 1 OOVG AnyLAN
- 802.15 Wireless Personal Area Network
- 802.16 Wireless MAN Standard

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

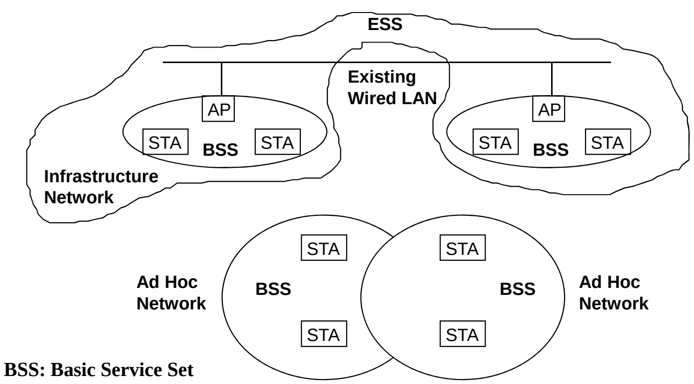
IEEE 802.11 Overview

- 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 ← **Our Focus**
  - » 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



BSS: Basic Service Set
ESS: Extended Service Set

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

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

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?

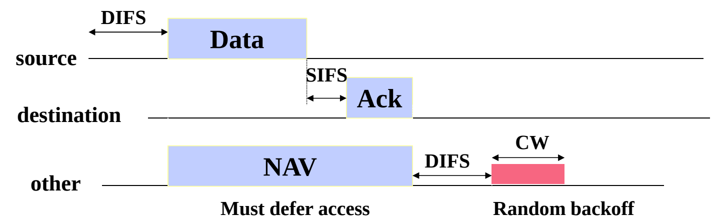
Features of 802.11 MAC protocol

- 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)

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

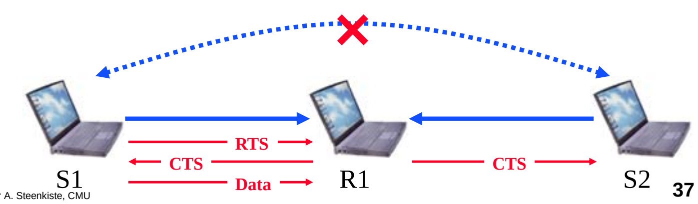


Exponential Backoff

- 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, ...

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



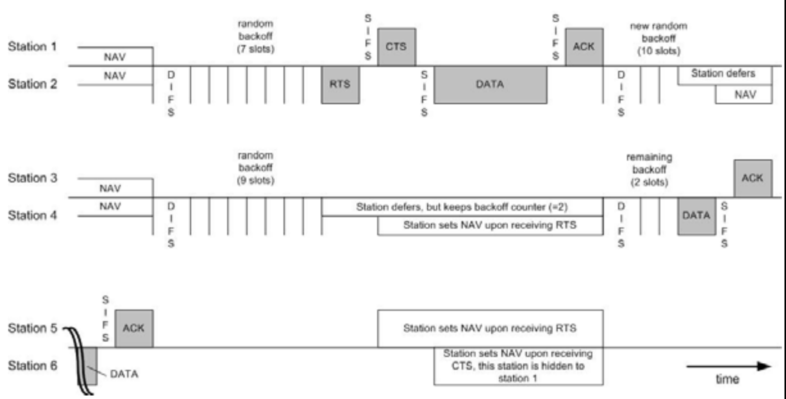
Request-to-Send and Clear-to-Send

- 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)**