

18-759 : Wireless Networks
Lecture 10: LAN MAC Protocols

Peter Steenkiste
Dina Papagiannaki
Spring Semester 2009
<http://www.cs.cmu.edu/~prs/wireless09/>

Peter A. Steenkiste, SCS, CMU

1

Cellular versus WiFi

	Cellular	WiFi
Spectrum	Licensed	Unlicensed
Service model	Provisioned "for pay"	Unprovisioned "free" – no SLA
MAC services	Fixed bandwidth SLAs	Best effort no SLAs

Peter A. Steenkiste, SCS, CMU

2

Implications Cellular

	Cellular	Implication
Spectrum	Licensed	Provider has control over interference
Service model	Provisioned "for pay"	Can and must charge + make commitments
MAC services	Fixed bandwidth SLAs	TDMA, FDMA, CDMA; access control

Peter A. Steenkiste, SCS, CMU

3

Implications WiFi

	WiFi	Implication
Spectrum	Unlicensed	No control – open, diverse access
Service model	Unprovisioned "free"	No guarantees maximize throughput, fairness
MAC services	Best effort no SLAs	???

Peter A. Steenkiste, SCS, CMU

4

Outline

- **Data link fundamentals**
 - » And what changes in wireless
- **Supporting data traffic**
- **Wireless-specific challenges**
- **Aloha**

Peter A. Steenkiste, SCS, CMU

5

Datalink Functions

- **Framing: encapsulating a network layer datagram into a bit stream.**
 - » Add header, mark and detect frame boundaries, ...
- **Logical link control: managing the frame transfer, e.g.**
 - » Error detection and correction to deal with bit errors
 - » Flow control: avoid that the sender outruns the receiver
- **Media access: controlling which frame should be sent over the link next.**
 - » Easy for point-to-point links; half versus full duplex
 - » Harder for multi-access links: who gets to send?

Peter A. Steenkiste, SCS, CMU

6

Framing

- **Similar design as in wired networks.**
 - › But must be more robust because of noise, ...
- **Typical structure:**
 - › Preamble: synchronize clocks sender and receiver
 - › Header: addresses, demultiplexing, type field, etc.
 - › Data packet
 - › Trailer: padding, CRC, ...
- **How does wireless differ?**
 - › Different transmit rates for different parts of packet
 - › Explicit multi-hop support
 - › Control information for physical layer

Peter A. Steenkiste, SCS, CMU

7

Error Control: Error Detection and Error Recovery

- **Detection: only detect errors**
 - › Make sure corrupted packets get thrown away, e.g. Ethernet
 - › Use of error detection codes, e.g. CRC
- **Recovery: also try to recover from lost or corrupted packets**
 - › Option 1: forward error correction (redundancy)
 - › Option 2: retransmissions
- **How does wireless differ?**
 - › Uses CRC to detect errors, similar to wired
 - › Error recovery is much more important because errors are more common and error behavior is very dynamic
 - › What approach is used?

Peter A. Steenkiste, SCS, CMU

8

Error Recovery in Wireless

- **Use of redundancy:**
 - › Very common at physical layer – see PHY lectures
 - › Spread spectrum, OFDM, etc.
- **Use of Automatic Repeat Request (ARQ)**
 - › Use time outs to detect loss and retransmit
- **Many variants:**
 - › Stop and wait: one packet at a time
 - › Go Back N: sender keeps sending and retransmits, starting with the unacknowledged packet
 - › Selective Repeat: only packets that are not acknowledged are retransmitted
- **When should what variant be used?**

Peter A. Steenkiste, SCS, CMU

9

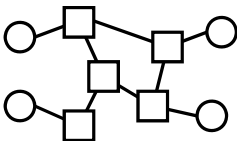
Media Access Control

- **How do we transfer packets between two hosts connected to the same network?**
- **Using point-to-point “links” with “switches” -- store-and-forward**
 - › Very common in wired networks, at multiple layers
- **Multiple access networks**
 - › Multiple hosts are sharing the same transmission medium
 - › Need to control access to the medium
 - › Taking turn versus contention based protocols
- **What is different in wireless?**
 - › Is store and forward used?
 - › Is multiple access used?

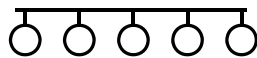
Peter A. Steenkiste, SCS, CMU

10

Datalink Architectures



- **Packet forwarding.**
- **Error and flow control.**



- **Media access control.**
- **Scalability.**

Peter A. Steenkiste, SCS, CMU

11

Outline

- **Data link fundamentals**
 - › And what changes in wireless
- **Supporting data traffic**
- **Wireless-specific challenges**
- **Aloha**

Peter A. Steenkiste, SCS, CMU

12

Creating Multiple Channels (101)

- Multiple channels can coexist if they transmit at a different frequency, or at a different time, or in a different part of the space (or use a different code)
 - › Three dimensional space: frequency, space, time
- Space can be limited (using wires or) using transmit power of wireless transmitters
- Frequency multiplexing means that different users use a different part of the spectrum
 - › Again, similar to radio: 95.5 versus 102.5 station
- Time division multiplexing means that users send at different times
 - › Static partitioning of time
- Duplexing: splitting the time/frequencies between the up and down link

Peter A. Steenkiste, SCS, CMU

13

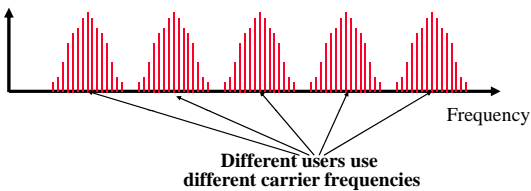
How About Wireless?

- All these techniques are useful!
 - › See cellular lectures
- But they have a number of limitations:
- They do not support bursty traffic efficiently
 - › Lots of unused capacity, ...
 - › while active users squeeze their bit stream through a very thin pipe
- Techniques work best in a provisioned service
 - › Management of frequencies, time slots, placement of devices, etc.

Peter A. Steenkiste, SCS, CMU

14

Frequency and Time Division Multiplexing



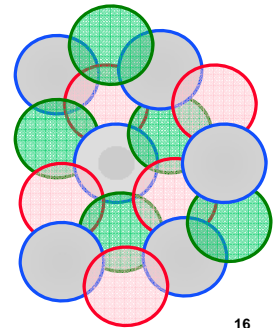
- Effective way of creating fixed bandwidth channels
- Difficult to match bandwidth to bursty traffic
- Complex to manage: assign frequencies/time slots, control interference in overlapping cells, etc.

Peter A. Steenkiste, SCS, CMU

15

Frequency Reuse in Space

- Users want access everywhere.
- Can control capacity of cells by controlling power
 - › Users in "small" cells will have more bandwidth on average
 - › Difficult to do dynamically
- Layout of cells and frequency assignment best done in a provisioned service
 - › What happens in residential networks?



Peter A. Steenkiste, SCS, CMU

16

So What about WiFi?

- Or more general: unprovisioned data services in the unlicensed spectrum
- Approach used in cellular is not very attractive
 - › Not a good fit for bursty traffic
 - › Designed for provisioned services in licensed spectrum
- Multiple access solutions are a better fit
 - › Optimized for bursty traffic
 - › Lower management and control complexity, especially for contention-based protocols (e.g. Ethernet)

Peter A. Steenkiste, SCS, CMU

17

Outline

- Data link fundamentals
 - › And what changes in wireless
- Supporting data traffic
- Wireless-specific challenges
 - › Ethernet review
 - › How wireless differs
- Aloha

Peter A. Steenkiste, SCS, CMU

18

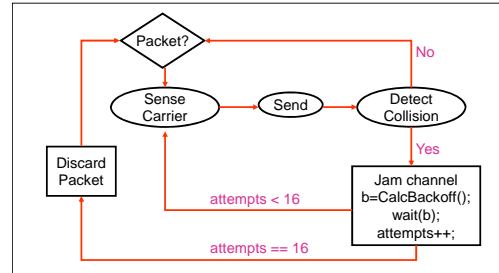
"Regular" Ethernet

- Multiple access: multiple hosts are competing for access to the channel
- Carrier-sense: make sure the channel is idle before sending
- 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

Peter A. Steenkiste, SCS, CMU

19

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



Peter A. Steenkiste, SCS, CMU

20

Carrier Sensing in CSMA/CD

- How to handle transmission if 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?

Peter A. Steenkiste, SCS, CMU

21

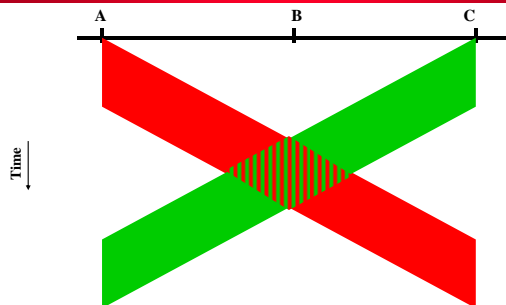
Ethernet Backoff Calculation

- Exponentially increasing random delay
 - » Infer senders from # of collisions
 - » More senders \rightarrow increase wait time
- First collision: choose K from $\{0,1\}$; delay is $K \times 512$ bit transmission times
- After second collision: choose K from $\{0,1,2,3\}$...
- After ten or more collisions, choose K from $\{0,1,2,3,4,\dots,1023\}$

Peter A. Steenkiste, SCS, CMU

22

Collisions

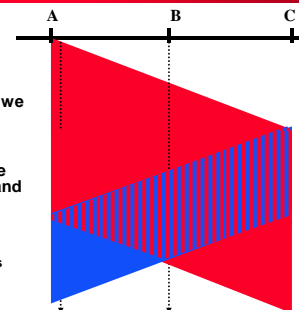


Peter A. Steenkiste, SCS, CMU

23

Collision Detection: Implications

- All nodes must be able to detect the collision.
 - » Any node can be sender
- The implication is that either we must have a short wires, or long packets.
 - » Or a combination of both
- Can calculate length/distance based on transmission rate and propagation speed.
 - » Messy: propagation speed is media-dependent, low-level protocol details, ...
 - » Minimum packet size is 64 bytes
 - Cable length ~ 256 bit times
 - » Example: maximum coax cable length is 2.5 km



Peter A. Steenkiste, SCS, CMU

24

Wireless Ethernet is a Good Idea, but ...

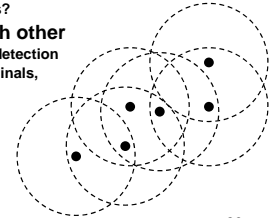
- **Attenuation varies with media**
 - » Also depends strongly on distance, frequency
- **Wired media has exponential dependence**
 - » Received power at d meters proportional to 10^{-kd}
 - » Attenuation in dB = $k d$, where k is dB/meter
- **Wireless media has logarithmic dependence**
 - » Received 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

Peter A. Stenikite, SCS, CMU

25

Implications for Wireless Ethernet

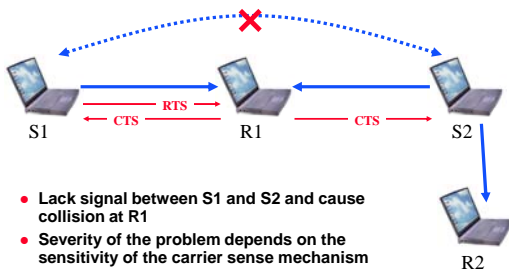
- **Collision detection is not practical**
 - » Ratio of transmitted signal power to received power is too high at the transmitter
 - » Transmitter cannot detect competing transmitters (is deaf while transmitting)
 - » So how do you detect collisions?
- **Not all nodes can hear each other**
 - » A further problem for collision detection
 - » Hidden terminals, exposed terminals, Capture effects
- **Made worse by fading**
 - » Changes over time!



Peter A. Stenikite, SCS, CMU

26

Hidden Terminal Problem

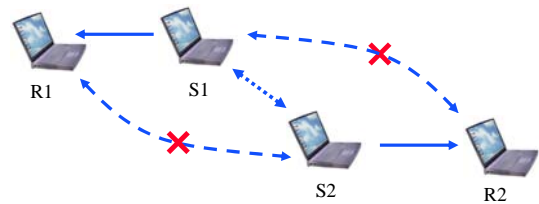


- Lack signal between S1 and S2 and cause collision at R1
- Severity of the problem depends on the sensitivity of the carrier sense mechanism
 - » Clear Channel Assessment (CCA) threshold

Peter A. Stenikite, SCS, CMU

27

Exposed Terminal Problem

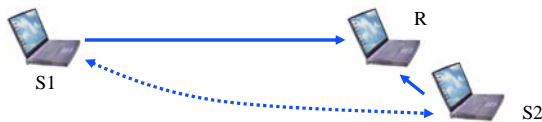


- Carrier sense prevents two senders from sending simultaneously although they do not reach each other's receiver
- Severity again depends on CCA threshold

Peter A. Stenikite, SCS, CMU

28

Capture Effect

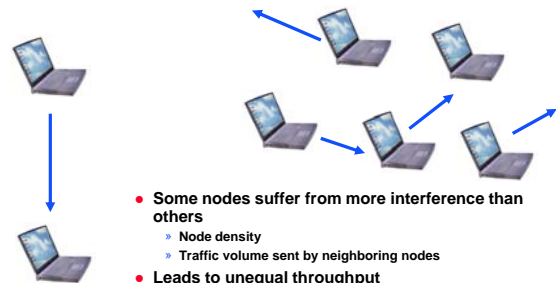


- Sender S2 will almost always "win" if there is a collision at receiver R.
- Can lead to extreme unfairness and even starvation.
- Solution is power control
 - » Very difficult to manage in a non-provisioned environment!

Peter A. Stenikite, SCS, CMU

29

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

Peter A. Stenikite, SCS, CMU

30

Outline

- Data link fundamentals
 - And what changes in wireless
- Supporting data traffic
- Wireless-specific challenges
- Aloha

Peter A. Stenikate, SCS, CMU

31

Why ALOHA



Peter A. Stenikate, SCS, CMU

32

Pure ALOHA

- Developed in University of Hawaii in early 1970's.
- It does not get much simpler:
 1. A user transmits at will
 2. If two or more messages overlap in time, there is a collision – receiver cannot decode packets
 3. Receive waits for roundtrip time plus a fixed increment – lack of ACK = collision
 4. After a collision, colliding stations retransmit the packet, but **they stagger their attempts randomly** to reduce the chance of repeat collisions
 5. After several attempts, senders give up
- Although very simple, it is wasteful of bandwidth, attaining efficiency of at most $1/(2e) = 0.18$

Peter A. Stenikate, SCS, CMU

33

Poisson Distribution

- Above definitions lead to: Probability $P(k)$ that there are exactly k events in interval of length T is then,

$$P(k) = \frac{(\lambda T)^k e^{-\lambda T}}{k!}$$

- We call the above probability the “Poisson distribution”
- Its mean and variance are:

$$E(k) = \lambda T$$

$$\sigma_k^2 = E(k^2) - E^2(k) = \lambda T$$

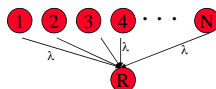
- Many nice properties, e.g. sum of a N independent Poisson processes is a Poisson process

Peter A. Stenikate, SCS, CMU

34

Pure ALOHA: Model

- Let there be N stations contending for use of the channel.
- Each station transmits λ packets/sec on average based on a Poisson arrival process
- All messages transmitted are of the same fixed length, m , in units of time
- Let new traffic intensity be $S \equiv N\lambda m$
- Since all new packets eventually get through, ‘ S ’ is also the network throughput



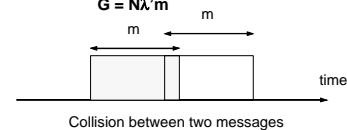
Peter A. Stenikate, SCS, CMU

35

Pure Aloha: Vulnerability

- Simplification: assume the retransmitted messages are independent Poisson process as well
- The total rate of packets attempting transmission = newly generated packets + retransmitted ones = $\lambda' > \lambda$
- The total traffic intensity (including retransmissions) is ,

$$G = N\lambda' m$$



- The “vulnerable period” in which a collision can occur for a given packet is $2 \times m$ sec

Peter A. Stenikate, SCS, CMU

36

Pure Aloha: Analysis

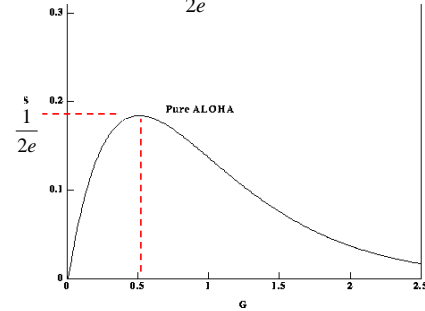
- Calculate "Probability of no collision" two ways:
1. Probability that there is no arrival in interval $2 \times m$:
 $P(\text{no arrival in } 2 \times m \text{ sec}) = e^{-2\lambda \times m} = e^{-2G}$
 2. Since all new arrivals eventually get through, we have
 $\lambda \lambda' = S/G = \text{Fraction of transmissions that are successful}$
- So, $S/G = \text{Probability of no collision} = P(\text{no arrival in } 2m \text{ sec})$
 - Thus, $S/G = e^{-2G}$ → Maximum Throughput of Pure Aloha
 $S = Ge^{-2G}$

Peter A. Steenkiste, SCS, CMU

37

Analysis Conclusion

- S is maximum at $S = \frac{1}{2e}$ at $G = 0.5$



Peter A. Si

38

Application of Pure ALOHA

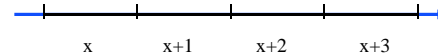
- Maximum throughput of ALOHA is only very low $1/(2e) = 18\%$, but
- Has very low latency under light load
- Maybe be sufficient for some applications, e.g. highly bursty interactive traffic, very lightly loaded networks
- But not appropriate for as a general purpose network technology
- Especially when capacity is a scarce resource
 - › As is often the case in wireless

Peter A. Steenkiste, SCS, CMU

39

Slotted ALOHA

- Competition to send only occurs at the start of each slot of length T
- Vulnerable period is T
 - › Period is $2 \times T$ in Aloha
- Doubles maximum throughput.
 - › Result based on many assumptions

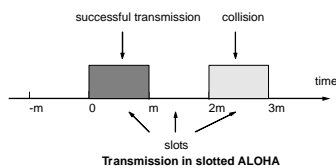


Peter A. Steenkiste, SCS, CMU

40

Slotted ALOHA

- Slot the time scale into units of time m (equal to message length)
- Modify Aloha by allowing users to attempt transmission at the beginning of a time slot only
- All users need to be synchronized in time.



Peter A. Steenkiste, SCS, CMU

41

Slotted ALOHA Analysis

- Collisions occur if two or more users attempt transmission in the same slot.
- Key point: The "vulnerable period" of the packet of size m has been reduced from $2m$ to only m !

- Since Poisson arrivals, $P(\text{successful transmission}) = e^{-G}$ Note: Not $2G$

- The throughput is then, $S = Ge^{-G}$

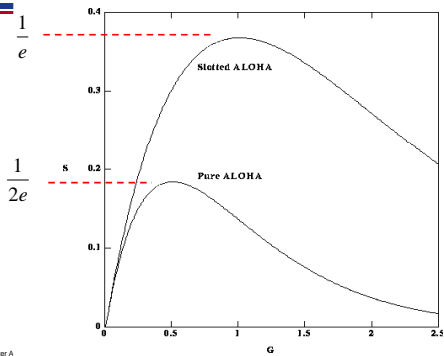
- The throughput S has maximum value of $1/e = 0.368$ at $G = 1$.

Peter A. Steenkiste, SCS, CMU

42

42

Analysis Results Slotted ALOHA



Peter A

3

Discussion of ALOHA

- **Slotted Alohas has twice the performance of basic Aloha, but performance is still poor**
 - » Slotted design is also not very efficient when carrying variable sized packets!
 - » Also (slightly) longer delay than pure Aloha
- **Still, not bad for an absolutely minimal protocol!**
- **How do we go faster?**

Peter A. Steenkiste, SCS, CMU

44