Checklist

- **Protocol 5 (go-back-N sliding window) as discussed in class**
- **Chapter 4 (medium access control sublayer) summary -- slides 1 to 6**
- **(Written Notes) Concepts and operational characteristics of pure and slotted ALOHA as discussed in class**
    - background provided in relevant textbook section and papers cited in "Course Material" section of this Webpage
    - **throughput *S* as a function of offered load with a mean of *G***
    - instructor's simulation timelines and plotted summary of simulation results provide further practical background for concepts and operation
    - **the theoretical analysis is based on the **Poisson distribution**; the in-class discussion is based on the sources in the "Course Material" section**
- **(Written Notes) Concepts and operational characteristics of CSMA and the three variants (1-persistent, non-persistent, and *p*-persistent) as discussed in class**
    - background provided in relevant textbook section and in papers cited in "Course Material" section of this Webpage
    - instructor's throughput curves comparing two CSMA variants with slotted ALOHA for different ratios of propagation time to packet/frame transmission time
- **(Written Notes) In-class discussion of Week 5/6/7 problems**
- **Summary of textbook Section 4.3 on Ethernet -- all slides**
    - Concepts and operational characteristics of CSMA/CD in classic Ethernet as discussed in class (background in textbook and original paper on the first experimental Ethernet)
- Thick/thin shared coax cable and hub-connected twisted-pair wiring for classic Ethernet
- (Readings) Efficiency analysis for classic Ethernet
- Switched Ethernet for point-to-point full-duplex communication with sophisticated use of twisted-pair wires for higher data rates
- **Summary of textbook Section 4.4 on 802.11 wireless standard -- all slides**
    - Concepts and operational characteristics of 802.11 as discussed in class (background in textbook and in articles cited in "Course Material" section)
- **Frame format for 802.11 and frame format for Ethernet**
- **Any other relevant concepts/examples presented or discussed in class since Quiz 1**

Slides (20 Total)

Medium Access Control (MAC) Sublayer Summary

Broadcast Channels and Protocols

- Focus here is on broadcast channels/protocols, also known as multi-access or random-access
- Sublayer of data link has protocols for deciding the next user of a shared multi-access channel
- Particularly important in LANs and for wireless (most WANs typically use point-to-point links)
- Medium access control (MAC) sublayer is the lowermost portion of the overall data link layer
- Primary MAC issue is control over the channel

The Channel Allocation Problem

- Users competing for radio, wire, or fibre link; more than one user leads to interference/errors
- Static allocation of bandwidth or access time is inefficient for many users with varying usage
- Need dynamic allocation to enhance efficiency
- Key assumptions for the allocation problem: independent traffic from users, single channel, observable collisions, continuous/slotted time, with/without carrier sensing (is channel in use?)

Multiple Access Protocols

- ALOHA (U. of Hawaii, 1971) – pure and slotted
- Carrier sense multiple access (CSMA) variations of 1-persistent, non-persistent, and p-persistent
- CSMA that has collision detection (CSMA/CD) is the basis of classic Ethernet from 1973-1974
- Collision-free protocols: bit map, token passing; improved scalability with binary countdown
- Limited-contention protocols – adap. tree walk
- Wireless – mult. access with collision avoidance

Ethernet

- Classic Ethernet involved one shared coax cable
- CSMA/CD with binary exponential backoff
- Contention interval set by max. cable length
- Good efficiency achievable for large packets
- Switched Ethernet is used today; no collisions, but buffering of packets required at each port
- Evolution from 10Mbps to 100M, 1G, and 10G
- Success is due to simplicity and flexibility, and also good interworking with TCP/IP

Wireless LANs

- 802.11 MAC sublayer has evolved with changes in the physical layer (freq. hop, OFDM, MIMO)
- Logical link control (LLC) sublayer just above MAC sublayer hides those differences to make everything appear the same to network layer
- MAC sublayer uses sensing & collision avoidance because coll. detection not feasible for wireless
- Wait with random backoff before transmission, pausing the countdown if other users transmit
- Receiver acknowledges if no error/collision

Ethernet Summary

History

- Classic version uses CSMA/CD on a shared cable
- R. Metcalfe went to Hawaii and studied ALOHA, then to Xerox PARC where he and D. Boggs created first 3-Mbps version of Ethernet
- DEC, Intel, Xerox standardized 10-Mbps version
- Xerox did not pursue it, so Metcalfe did (3Com)
- IEEE standardized it in 1983 as 802.3
- One minor difference btwn 802.3 & "Ethernet" in preamble bytes at start of frame

Data Time Only (Efficiency) **not on slides**

$$data\ time\ only + (avg\ \#slots)(slot\ duration)$$

Classic Ethernet MAC Protocol

- Manchester encoding at 20 MHz for 10 Mbps
- Frame has preamble, 6-byte MAC addresses for source & dest, type/length, 0-1500 bytes data, pad for min. 64-byte frame, finally checksum
- Cable length limited for maximum round-trip delay of 50 μsec for 512-bit contention slot
- If collision detected, senders "jam" channel
- Retry uses binary exponential backoff
- If no collision, assume success; no acks used

Classic Ethernet Performance

- Analyzed in 1976 paper by Metcalfe and Boggs; textbook provides a similar analysis
- Differentiate short contention slots and frames
- Probabilistically determine average number of contention slots before collision-free frame
- Determine efficiency using avg. num. of slots, contention slot duration, and frame size
- Good efficiency (> 75%) for frames > 512 bytes

Switched Ethernet

- Long single cable evolved to hub architecture that centrally connected twisted-pair cables, but still a shared medium, so same capacity
- Switched version uses fast point-to-point links to a device with internal high-speed backplane, hence no more collisions (but buffers limited)
- Assumes full-duplex operation; need CSMA/CD if half-duplex mode used on link to/from switch
- Switched version also isolates/filters traffic

Fast Ethernet

- IEEE 802.3u approved in 1995 for 100 Mbps using only twisted-pair cabling (no more coax)
- 100Base-T4: four twisted pairs at 25 MHz with three voltage levels to achieve 100 Mbps
- 100Base-TX: two twisted pairs at 125 MHz, encoding 4 data bits in 5 signal bits
- 100Base-FX: fibre-optic cable

• Interoperability with 10-Mbps equipment enabled through autonegotiation of rate/duplex

Gigabit Ethernet

• IEEE 802.3ab in 1999 for 1 Gbps performance with backward compatibility & autonegotiation
• Initial high-speed cabling required upgrades
• Follow-up 1000Base-T used four twisted pairs (hence no upgrade needed to existing cabling)
• Simultaneous transmission in both directions on each pair using DSP to separate signals
• Five voltage levels carry 2 bits @ 125 Msym/sec for total of (4 pairs)(2 bits)(125 M) = 1 Gbps

Reasons for Ethernet Success

• Simplicity/flexibility → reliability/maintainability
• Difficult to replace something that works well
• No significant software requirements (drivers)
• No lengthy configuration; just plug in cables
• Good interworking with TCP/IP protocols; both IP and Ethernet are connectionless
• Good evolution for performance that retained all of the positive aspects described above; "borrowed" good ideas from other technologies

Wireless LANs (802.11 Summary)

Primary Standard: 802.11

• Consider protocol stack, radio transmission, MAC sublayer protocol, frames, and services
• Two modes: access point; ad hoc (less popular)
• Physical layer variations: FH, SS, OFDM, MIMO
• MAC sublayer determines channel allocation
• Logical link control (LLC) sublayer of data link hides differences between variations; primary purpose now is protocol identification (such as indicating IP for network layer)

802.11 Physical Layer

FH = Frequency Hopping
SS = Spread Spectrum
OFDM = Orthogonal frequency-division multiplexing
MIMO = Multi-Input, Multi-Output

• Short-range 2.4-GHz/5-GHz transmission (ISM), channel bandwidth of 20 MHz (except 11n)
• Rate adaptation responds to changing conditions
• 802.11b: spread-spectrum, up to 11 Mbits/sec
• 802.11a: OFDM using 52 subcarriers, 54 Mbps, but much lower range than 802.11b
• 802.11g: also OFDM, interoperability with 11b
• 802.11n: reduced overheads, multiple antennas

802.11 MAC Sublayer Protocol

• Radio environment – differs from Ethernet
• Half-duplex operation – received signal is weak, hence collision detection is not feasible

• Use CSMA with collision avoidance instead
• Sender begins with random backoff (0-15 slots), pausing countdown when other frames are sent
• Transmits when count reaches 0, awaits ack
• If no ack, double backoff interval to try again until success or maximum # of retries exceeded

802.11 MAC Sublayer Protocol

• Backoff before sending helps avoid collisions due to distributed/independent behavior
• Acks are necessary – variable radio reception makes collision detection difficult, and causes senders to falsely conclude idleness of channel
• Combine physical channel sensing with virtual using network allocation vector (NAV); frames indicate duration of busy channel, including ack
• RTS/CTS feature available, but not very useful

802.11 MAC Sublayer Protocol (ctd.)

• Reliability challenges from interference, etc., handled by automatically adjusting trans. rate, by using shorter frames (fragments in bursts)
• Power saving for mobile devices handled with periodic AP beacon frames for client wake-up, and also AP buffering until client transmission
• Quality of service handled with five intervals between frames; enables acks, VoIP frames to have higher priority than regular data frames
• QoS for different rates equalizes airtime

802.11 Frame Structure

• Frame types: data, control, and management
• Each has appropriate header information
• Frame control bits include indication that frame is part of a burst for a longer total transmission
• Data frame includes duration field for NAV and sequence number for duplicate detection
• With AP involved, frame has 3 address fields because AP is simply an intermediate point
• Payload field has LLC prefix for protocol info

802.11 Services

• Association/reassociation features for APs allow stations to get info, and support handoff
• Authentication features (if network is not open) emphasize the use of WPA2 after association
• Distribution features govern routing of frames to local receivers through AP or remote stations
• Privacy features provide encryption capability with keys determined during authentication
• Transmit power control; dynamic freq. selection

Protocol 5: Go-Back-N Sliding Window (Bidirectional w/ Piggybacked Acknowledgements)

```
/* PROTOCOL 5: Go-back-n sliding-window protocol, bidirectional with piggybacked acknowledgements,          */
/*             from Tanenbaum/Whetherall, Computer Networks (5th ed.), Figure 3-19 --- with minor changes  */

typedef enum {frame_arrival, chksum_error, timeout, network_layer_ready} event_type;  /* protocol-specific */
```

```
static void send_data (unsigned int outgoing_seq,
                       packet buf[], unsigned int ack_seq)
{
  frame s;
                                /* piggybacked ack */
  s.info = buf[outgoing_seq];
  s.seq = outgoing_seq;
  s.ack = (ack_seq + MAX_SEQ) % (MAX_SEQ + 1);
  to_physical_layer (&s);
  start_timer (outgoing_id);
}

static int circularly_in_between (
    unsigned int low, unsigned int mid,
    unsigned int high)
{
  if (   ((low <= mid) && (mid < high))
      || ((high < low) && (low <= mid))
      || ((mid < high) && (high < low)))
    return 1;
  else
    return 0;
}

void protocol5 (void)
{
  unsigned int next_frame_to_send, ack_expected,
               frame_expected, num_buffered, i;
  frame r;
  packet buffer[MAX_SEQ + 1];
  event_type event;

  enable_network_layer ();
  next_frame_to_send = ack_expected =
                frame_expected = num_buffered = 0;
  while (1) {
    wait_for_event (&event);
    switch (event) {
      case network_layer_ready:
        from_network_layer
              (&buffer[next_frame_to_send]);
        num_buffered = num_buffered + 1;
        send_data (next_frame_to_send, buffer,
                   frame_expected);
        next_frame_to_send =
              (next_frame_to_send + 1) % (MAX_SEQ + 1);
        break;
      case frame_arrival:
        /* accept data frame only if in seq. order, but
           always consider piggybacked ack in frame */
        from_physical_layer (&r);
        if (r.seq == frame_expected) {
          to_network_layer (&r.info);
          frame_expected =
                (frame_expected + 1) % (MAX_SEQ + 1);
        }
        while (circularly_in_between
                  (ack_expected,
                   r.ack, next_frame_to_send)) {
          num_buffered = num_buffered - 1;
          stop_timer (ack_expected);
          ack_expected =
                (ack_expected + 1) % (MAX_SEQ + 1);
        }
        break;
      case chksum_error:
        break;  /* ignore bad frame */
      case timeout:
        /* retransmit all outstanding frames */
        next_frame_to_send = ack_expected;
        for (i = 1; i <= num_buffered; i++) {
          send_data (next_frame_to_send, buffer,
                     frame_expected);
          next_frame_to_send =
                (next_frame_to_send + 1) % (MAX_SEQ + 1);
        }
        break
    }
    if (num_buffered < MAX_SEQ) /* after event handled */
      enable_network_layer ();  /*  control the flow   */
    else                        /*  from network layer */
      disable_network_layer (); /*  based on capacity  */
  }
}
```

ELEC 373 Computer Networks *Dr. N. Manjikian*

Ethernet Frame Structure

Preamble: 7 bytes with a binary pattern (i.e. 10101010…1010101) used for clock synchronization. Eighth byte is start of frame. (8 bytes total)
Source/Destination: 6 bytes (MAC addresses)
Chksum: Checks errors at receiver, if detected, discard frame
Payload: Sequence of bits (variable), carries data from upper layer protocols.
Minimum packet size is 64 bytes, 18 header bytes and 46 data bytes. If less than 46 bytes to send, then add dummy bits (padding) to increase length to 46 bytes.
Maximum packet size is 1518 bytes.

802.11 Frame Structure

FC: Frame control (2 bytes)
Duration: Duration ID (NAV – Network Allocation Vector), 2 bytes,
Source/Destination/Other: 6 bytes (MAC addresses)
Chksum: Checks errors at receiver, if detected, discard frame
Payload: Sequence of bits (variable), carries data from upper layer protocols.
Seq. Ctrl.: Fragment number (4 bits), Sequence number (12 bits)

Cables

Twisted pair standard – 10BaseT (10, 100, 1000 Mbps)
Thin Coaxial Standard – 10Base2 (Baseband)
Thick Coaxial Standard – 10Base5 (Broadband)
Coax: half duplex, uses collision detection, and if a collision is detected then the rest of the contention slot is "jammed" by the colliding senders to clearly mark that slot busy
Full duplex: - Sending and receiving at the same time. Implemented by twisted-pair wiring.

- the modern twisted-pair Ethernet that supports simultaneous sending and receiving

In-Class Practice Quiz

1. For a Go-Back-N implementation, circular buffer space for a total of 12 frames is allocated. What is the *maximum* size of the sliding window?
12 buffers = MAX_SEQ + 1, therefore, maximum window size is 11.

2. Briefly contrast WANs/MANs vs. LANs in terms of medium access.
WANs/MANs – point-to-point
LANs – CSMA/CD (WiFi) or Switched (Ethernet) ***(Shared broadcast channel classic ethernet, 802.11)

3. The Poisson probability of k events in an interval where the mean is G events is $\frac{(G^k * e^{-G})}{(k!)}$ provide an UNSIMPLIFIED expression for the probability of a collision occurring in slotted ALOHA.

$$P(Collision) = 1 - P(idle) - P(success)$$

$$P(Collision) = 1 - \frac{(G^0 * e^{-1})}{(0!)} - \frac{(G^1 * e^{-1})}{(1!)}$$

4. In two sentences, describe the operation of non-persistent CSMA.
If the channel is idle, proceed to transmit. If the channel is busy, retry from the start after a long, random delay.

Carrier Sense Multiple Access (CSMA)

- Pure Aloha – Transmit any time
- Slotted Aloha – Transmit at specific times, but still without concern for other sources
- Performance (throughput) was low
- Can we use knowledge of system activity to improve performance (throughput)?
- "Sense" if transmission is in progress
  - If busy, don't transmit yet
  - Wait for idle channel
- Central receiver provides some kind of acknowledgement
- Otherwise source times out and retries
- τ = propagation delay (worst case), frame time >> τ, $a = \frac{\tau}{frame\ time}$
- **1-persistent CSMA**
  - **If channel idle, begin transmitting with probability = 1**
  - **If channel busy, wait for idle**

- **Non-persistent CSMA**
  - **If channel idle, begin transmitting with probability = 1**
  - **If channel busy, wait for "random" time interval and retry**
- **P-persistent CSMA**
  - **If channel idle, begin transmitting with probability p**
    - **Otherwise, with prob = (1 – p), wait for delay τ and check for idle and transmit if possible. Repeat.**
  - **If channel busy, wait for "random" time interval and retry**

ELEC 373 Quiz 2 – 2018

No question 9 – 13, 16 – 18 as material concerning PAR or the Network Layer will not be examined

1. Why is the maximum throughput of slotted ALOHA higher than pure ALOHA?

The window of vulnerability for collisions is twice as large in pure ALOHA than in slotted ALOHA. Therefore, at higher offered loads, collisions are more likely in pure ALOHA. (Slotted ALOHA has fewer collisions, hence higher throughput)

2. Why is the maximum throughput of 1-persistent CSMA higher than slotted ALOHA?

CSMA has carrier sensing, whereas slotted ALOHA does not. Therefore, CSMA has fewer collisions because it checks for in-progress transmissions before starting a new transmission, hence higher throughput than slotted ALOHA for higher offered load. (Not all collisions are avoided, however)

3. In the context of computer networks as discussed in this course, what does a Poisson distribution with mean G represent? (I.e., what is it used to describe?)

It represents the number of events (e.g., frame transmission attempts from different sources) within a specified interval of time (e.g., duration of a frame or length of a time slot).

4. Describe the basis for the analysis of efficiency in classic Ethernet, i.e., just IDENTIFY the THREE factors that are considered (no math is required).

1. Duration of a contention slot
2. Average number of contention slots (due to collisions) before successful frame x unit.
3. Length of transmitted frame.

5. Compare classic Ethernet and 802.11 on the issue of collisions.

- Ethernet allows collisions and handles them afterward with binary exponential backoff to reduce the re-occurrence of collision between competing sources.
- 802.11 seeks to avoid collisions (can't entirely eliminate them) with random backoff before initializing frame transmission

6. Just identify two ways that 802.11 handles wireless reliability challenges arising from interference and other aspects.

- Auto-adjustment of transmission rate to reduce errors when signals are weak or in presence of interference
- Divide frames into smaller fragments so that error occurrence affects one fragment and not the entire frame (retransmit only the fragment)

7. How does 802.11 help to ensure that senders are not likely to wait indefinitely for acknowledgement?

Between frames, there are 5 defined intervals for different types of prioritized traffic. Transmission of acknowledgement frames can be initiated in one of these earlier intervals to have priority.

8. What is the purpose of the network allocation vector (NAV) in 802.11?

It indicates expected duration of actual use of the shared wireless channel as an additional virtual means of "channel-sensing" beyond physical sensing. It further aids in collision avoidance by delaying senders

from using the channel until presumed idle, even when physical sensing is less-reliable (e.g., interference)

14. What additional field is included in the frame for a go-back-n sliding-window protocol? *WHY*? (In terms of a key difference between go-back-n and PAR…)
Frame includes field for piggybacked acknowledgement (as sequence number). Go-back-n differs from PAR in that it is a bidirectional protocol for data frames, so data traffic in reverse carries with it acknowledgement information related to prior forward traffic.

15. In a go-back-n sliding window protocol implementation, write an if statement that shows how the limit on the window size is enforced. Assume the existence of functions that enable or disable the network layer from providing a packet.

```
If(num_buffered_frames < MAX_SEQ) { /*if(num_sent < window_limit)*/
        enable_network_layer();
else
        disable_network_layer();
}
```

Relevant Final Exam Questions

2. Data Link Layer
c) Why is the go-back-n protocol called "go-back-n"? Explain by describing a specific event and the specific response in the protocol to that event.
There can be up to n outstanding frames sent before an acknowledgement is received. In the case of a timeout after sending n frames and receiving no acknowledgement, the n outstanding frames will be retransmitted (go back and retransmit n frames, in other words).
d) The go-back-n protocol description in this course uses a parameter MAX_SEQ.
Number of packet buffers allocated at each end? MAX_SEQ + 1
Largest number of unacknowledged packets sent in either direction? MAX_SEQ

3. The Medium Access Sublayer
a) The primary MAC issue is: control over the channel
b) What does $P[k] = \frac{G^k e^{-G}}{k!}$ typically represent in the context of networks?
The Poisson probability of k transmission attempts per frame time where the mean offered load is G events.
c) For slotted ALOHA, make appropriate use of the expression from part (b) to derive the successful transmission throughput, S. *Explain* the derivation.
Success is one transmission attempt, k = 1. Vulnerable period is one frame time, G.
$S = GP_o = G*\frac{G^0 e^{-G}}{0!} = Ge^{-G}$
d) How is the maximum throughput S_{max} obtained from the result of part c)? This question is not asking for the value of S_{max}. Describe *HOW* to obtain it.
Using calculus, find the derivative of the S equation and set it equal to zero, then solve for the G value for which S_{max} occurs. Then, substitute the G value into the S equation to find S_{max}.
e) CSMA = Carrier Sense Multiple Access

Explain the 'MA' above, i.e., the situation circumstance that is relevant.

Multiple Access is relevant on shared/broadcast channels, wherein there is one central receiver and other stations within a given radius, as drawn in class.

f) State the difference(s) between p-persistent CSMA and non-persistent CSMA.

p-persistent CSMA: When channel idle, transmit with prob. P or wait for propagation delay, τ, with prob. (1 - p) and check for idle again.

Non-persistent CSMA: When channel idle, transmit with prob. 1.

g) There is a ratio that has an important role in determining the throughput for variants of CSMA. Describe the ratio (i.e., the numerator and denominator).

$$a = \frac{\tau}{frame\ time}$$

This is a ratio of propagation delay, τ, and frame time. Typically, propagation delay >> frame time. As this ratio approaches 1, the probability of a collision occurring increases as the period for subsequent frames to know that a slot is busy will be longer. This is a result of an increase in propagation delay. The smaller this ratio is, the better for CSMA variants.

h) *Explain* whether or not the ratio above is also important for ALOHA.

This ratio is not important for ALOHA as ALOHA does not check the channel for current transmissions and so does not reduce collisions by waiting for a delay.

4. Ethernet and 802.11

a) In classic shared-cable Ethernet, why is a *minimum* frame size required?

Minimum frame size is required to easily distinguish between valid frames and other things. This improves performance, and ensures constant time and size of a contention slot.

b) For 10-Mbps Ethernet on a shared cable, compute the channel efficiency if all frames have the same size of 1500 bytes, the bandwidth is 20 MHz (due to Manchester encoding), the contention slot interval is 51.2 microseconds, and there is an average of 3 contention slots per successful frame transmission.

$$\frac{data\ time\ only}{data\ time\ only + (avg\ \#\ slots) * (slot\ duration)} = \frac{\frac{1500 * 8\ bits}{10 * 10^6 \frac{bits}{sec}}}{\frac{1500 * 8\ bits}{10 * 10^6 \frac{bits}{sec}} + 3(51.2 * 10^{-6}\text{sec})} = 0.8865$$

c) Other than higher performance, state an additional benefit arising from the use of switched Ethernet over shared-cable/hub-based Ethernet.

Switched Ethernet has good interleaving with TCP/IP.

Switched Ethernet also isolates/filters traffic.

d) State two factors that have contributed to the long-term success of Ethernet.

Simplicity/Flexibility

No significant software requirements

e) How many address fields are there in an 802.11 frame and why?

Three, one for the destination (access point), one for the sender, and one for the "real" destination that the access point will ultimately send the frame to.

f) How are reliability challenges stemming from interference and other issues addressed in wireless 802.11 LANs?

Fragmentation of frames and auto adjustment of transmission rate to reduce errors.

g) What is done in 802.11n for higher performance relative to a/b/g variants?
802.11n uses multiple antennas resulting in reduced overhead.
h) Identify two of the schemes used for physical signal modulation in 802.11.
Frequency Hopping (FH), and Spread Spectrum (SS)
i) From *where* is the information for the network allocation vector (NAV) obtained?
The frame that is in transmission.

Supplementary Material (Articles and Simulations)

THE ALOHA SYSTEM -- Another alternative for computer communications (Pages 281-283)

INTRODUCTION

In September 1968 the University of Hawaii began work on a research program to investigate the use of radio communications for computer-computer and console-computer links. In this report we describe a remote-access computer system—THE ALOHA SYSTEM—under development as part of that research program1 and discuss some advantages of radio communications over conventional wire communications for interactive users of a large computer system. Although THE ALOHA SYSTEM research program is composed of a large number of research projects, in this report we shall be concerned primarily with a novel form of random-access radio communications developed for use within THE ALOHA SYSTEM. The University of Hawaii is composed of a main campus in Manoa Valley near Honolulu, a four-year college in Hilo, Hawaii and five two-year community colleges on the islands of Oahu, Kauai, Maui and Hawaii. In addition, the University operates a number of research institutes with operating units distributed throughout the state within a radius of 200 miles from Honolulu. The computing center on the main campus operates an IBM 360/65 with a 750 K byte core memory and several of the other University units operate smaller machines. A time-sharing system UHTSS/2, written in XPL and developed as a joint project of the University Computer Center and THE ALOHA SYSTEM under the direction of W. W. Peterson is now operating. THE ALOHA SYSTEM plans to link interactive computer users and remote-access input-output devices away from the main campus to the central computer via UHF radio communication channels.

WIRE COMMUNICATIONS AND RADIO COMMUNICATIONS FOR COMPUTERS

At the present time conventional methods of remote access to a large information processing system are limited to wire communications—either leased lines or dial-up telephone connections. In some situations, these alternatives provide adequate capabilities for the designer of a computer-communication system. In other situations, however the limitations imposed by wire communications restrict the usefulness of remote access computing.2 The goal of THE ALOHA SYSTEM is to provide another alternative for the system designer and to determine those situations where radio communications are preferable to conventional wire communications. The reasons for widespread use of wire communications in present day computer-communication systems are not hard to see. Where dial-up telephones and leased lines are available they can provide inexpensive and moderately reliable communications using an existing and well-developed technology.3,4 For short distances the expense of wire communications for most applications is not great. Nevertheless, there are a number of characteristics of wire communications which can serve as drawbacks in the transmission of binary data. The connect time for dial-up lines may be too long for some applications; data rates on such lines are fixed and limited. Leased lines may sometimes be obtained at a variety of data rates, but at a premium cost. For communication links over large distances (say 100 miles) the cost of communication for an interactive user on an alphanumeric console can easily exceed the cost of computation.5 Finally we note that in many parts of the world a reliable high-quality wire communication network is not available and the use of radio communications for data transmission is the only alternative. There are of course some fundamental differences between the data transmitted in an interactive timeshared computer system and the voice signals for which the telephone system is designed.6 First among these differences is the burst nature of the communication from a user console to the computer and back. The typical 110 baud console may be used at an average data rate of from 1 to 10 baud over a dial-up or leased line capable of transmitting at a rate of from 2400 to 9600 baud. Data transmitted in a time-shared computer system

comes in a sequence of bursts with extremely long periods of silence between the bursts. If several interactive consoles can be placed in close proximity to each other, multiplexing and data concentration may alleviate this difficulty to some extent. When efficient data concentration is not feasible however the user of an alphanumeric console connected by a leased line may find his major costs arising from communication rather than computation, while the communication system used is operated at less than 1 percent of its capacity. Another fundamental difference between the requirements of data communications for time-shared systems and voice communications is the asymmetric nature of the communications required for the user of interactive alphanumeric consoles. Statistical analyses of existing systems indicate that the average amount of data transmitted from the central system to the user may be as much as an order of magnitude greater than the amount transmitted from the user to the central system.6 For wire communications it is usually not possible to arrange for different capacity channels in the two directions so that this asymmetry is a further factor in the inefficient use of the wire communication channel. The reliability requirements of data communications constitute another difference between data communication for computers and voice communication. In addition to errors in binary data caused by random and burst noise, the dial-up channel can produce connection problems—e.g., busy signals, wrong numbers and disconnects. Meaningful statistics on both of these problems are difficult to obtain and vary from location to location, but there is little doubt that in many locations the reliability of wire communications is well below that of the remainder of the computer-communication system. Furthermore, since wire communications are usually obtained from the common carriers this portion of the overall computer-communication system is the only portion not under direct control of the system designer.

THE ALOHA SYSTEM

The central computer of THE ALOHA SYSTEM (an IBM 360/65) is linked to the radio communication channel via a small interface computer (Figure 1). Much of the design of this multiplexor is based on the design of the Interface Message Processors (IMP's) used in the ARPA computer net.4 - 7 The result is a Hawaiian version of the IMP (taking into account the use of radio communications and other differences) which has been dubbed the MENEHUNE (a legendary Hawaiian elf). The HP 2115A computer has been selected for use as the MENEHUNE. It has a 16-bit word size, a cycle time of 2 microseconds and an 8Kword core storage capacity. Although THE ALOHA SYSTEM will also be linked to remote-access input/output devices and small satellite computers through the MENEHUNE, in this paper we shall be concerned with a random-access method of multiplexing a large number of low data rate consoles into the MENEHUNE through a single radio communication channel. THE ALOHA SYSTEM has been assigned two 100 KHZ channels at 407.350 MHZ and 413.475 MHZ. One of these channels has been assigned for data from the MENEHUNE to the remote consoles and the other for data from the consoles to the MENEHUNE. Each of these channels will operate at a rate of 24,000 baud. The communication channel from the MENEHUNE to the consoles provides no problems. Since the transmitter can be controlled and buffering performed by the MENEHUNE at the Computer Center, messages from the different consoles can be ordered in a queue according to any given priority scheme and transmitted sequentially. Messages from the remote consoles to the MENEHUNE however are not capable of being multiplexed in such a direct manner. If standard orthogonal multiplexing techniques (such as frequency or time multiplexing) are employed we must divide the channel from the consoles to the MENEHUNE into a large number of low speed channels and assign one to each console, whether it is active or not. Because of the fact that at any given time only a fraction of the total number of consoles in the system will be active and because of the burst nature of the data from the consoles such a

scheme will lead to the same sort of inefficiencies found in a wire communication system. This problem may be partly alleviated by a system of central control and channel assignment (such as in a telephone switching net) or by a variety of polling techniques. Any of these methods will tend to make the communication equipment at the consoles more complex and will not solve the most important problem of the communication inefficiency caused by the burst nature of the data from an active console. Since we expect to have many remote consoles it is important to minimize the complexity of the communication equipment at each console. In the next section we describe a method of random access communications which allows each console in THE ALOHA SYSTEM to use a common high speed data channel without the necessity of central control or synchronization. Information to and from the MENEHUNE in THE ALOHA SYSTEM is transmitted in the form of "packets," where each packet corresponds to a single message in the system.8 Packets will have a fixed length of 80 8-bit characters plus 32 identification and control bits and 32 parity bits; thus each packet will consist of 704 bits and will last for 29 milliseconds at a data rate of 24,000 baud. The parity bits in each packet will be used for a cyclic error detecting code.9 Thus if we assume all error patterns are equally likely the probability that a given error pattern will not be detected by the code is

$$2^{32}=10^{-9}$$

Since error detection is a trivial operation to implement,10 the use of such a code is consistent with the requirement for simple communication equipment at the consoles. The possibility of using the same code for error correction at the MENEHUNE will be considered for a later version of THE ALOHA SYSTEM.

The random-access method employed by THE ALOHA SYSTEM is based on the use of this error detecting code. Each user at a console transmits packets to the MENEHUNE over the same high data rate channel in a completely unsynchronized (from one user to another) manner. If and only if a packet is received without error it is acknowledged by the MENEHUNE. After transmitting a packet the transmitting console waits a given amount of time for an acknowledgment; if none is received the packet is retransmitted. This process is repeated until a successful transmission and acknowledgment occurs or until the process is terminated by the user's console.

A transmitted packet can be received incorrectly because of two different types of errors; (1) random noise errors and (2) errors caused by interference with a packet transmitted by another console. The first type of error is not expected to be a serious problem. The second type of error, that caused by interference, will be of importance only when a large number of users are trying to use the channel at the same time. Interference errors will limit the number of users and the amount of data which can be transmitted over this random-access channel.

In Figure 2 we indicate a sequence of packets as transmitted by k active consoles in the ALOHA random access communication system.

We define T as the duration of a packet. In THE ALOHA SYSTEM r will be equal to about 34 milliseconds; of this total 29 milliseconds will be needed for transmission of the 704 bits and the remainder for receiver synchronization. Note the overlap of two packets from different consoles in Figure 2. For analysis purposes we make the pessimistic assumption that when an overlap occurs neither packet is received without error and both packets are therefore retransmitted. Clearly as the number of active consoles increases the number of interferences and hence the number of retransmissions increases until the channel clogs up with repeated packets. In the next section we compute the average number of active consoles which may be supported by the transmission scheme described above.

ALOHA packet broadcasting: a retrospect (Pages 203-205 end of first column)

INTRODUCTION

Packet broadcasting is a technique whereby data is sent from one node in a net to another by attaching address information to the data to form a packet—typically from 30 to 1000 bits in length. The packet is then broadcast over a communication channel which is shared by a large number of nodes in the net; as the packet is received by these nodes the address is scanned and the packet is accepted by the proper addressee (or addressees) and ignored by the others. The physical communication channel employed by a packet broadcasting net can be a ground-based radio channel, a satellite transponder or a cable. Packet broadcasting networks can achieve the same efficiencies as packet switched networks,1 but in addition they have special advantages for local distribution data networks2 and for data networks using satellite channels.3 In this paper we concentrate on those characteristics which are of interest for a local distribution data network. In particular, we discuss the lessons learned in the design and implementation of the ALOHANET, a packet broadcasting radio network in operation at the University of Hawaii since 1970. A number of design issues which arose in the construction of the system are defined, our solutions are explained, and in some cases, they are justified. The lessons learned from the ALOHANET are used to indicate how such a radio packet broadcasting system might best be built using the technology available in 1975. In the next section a brief description of the ALOHANET and its rationale is given. This is followed by a detailed discussion of the major system protocol choices that have evolved, pointing out some related theoretical work where appropriate. Choices concerning the design of the radio communication subsystem are then examined, followed by an evolutionary view of the important impact microcomputer technology has had on the user interface design and resulting system capabilities. The concluding section summarizes our present views with respect to the basic system configuration and properties of packet broadcasting nets.

THE ALOHANET

The ALOHANET is the first system which successfully utilized the packet broadcasting concept for on-line access of a central computer via radio. Its primary purpose is to provide inexpensive access to one or more time-sharing systems by a large number of terminal users, typically in the hundreds. However, it also allows user-to-user communication within the net and is evolving toward use in a more generally-oriented computer communications environment.

OPERATION

The present network configuration makes use of a broadcast channel for only one direction of traffic flow. (As we shall see in later sections, the lack of a broadcast capability in the other direction has seriously handicapped the development of effective protocols in certain areas.) Two 100 KHz channels are used in the UHF band—a random access channel for user-to-computer communication at 407.350 MHz and a broadcast channel at 413.475 MHz for computer-to-user messages. The original system was configured as a star network, allowing only a central node to receive transmissions in the random access channel; all users received each transmission made by the central node in the broadcast channel. Recently the addition of ALOHA repeaters has generalized the network structure. A block diagram of the present operational ALOHANET is shown in Figure 1. The central communications processor of the net is an HP 2100 minicomputer (32K of core, 16 bit words) called the MENEHUNE4 (Hawaiian for IMP) which functions as a message multiplexor/concentrator in much the same way as an ARPANET IMP.5 The MENEHUNE accepts messages from the UH central computer, an IBM System 360/65 running TSO (as of December 1974, a 370/158) or from ALOHA's own time-sharing computer, the BCC 500, or from any ARPANET computer linked to the MENEHUNE via the ALOHA TIP.6 Outgoing messages in the

MENEHUNE are converted into packets, the packets are queued on a firstin, first-out basis, and are then broadcast to the remote users at a data rate of 9600 baud. The packet consists of a header (32 bits) and a header parity check word (16 bits), followed by up to 80 bytes of data and a 16-bit data parity check word. The header contains information identifying the particular user so that when the MENEHUNE broadcasts a packet, only the intended user's node will accept it. More will be said about packet formats later. The random access channel (at 407.35 MHz) for communication between users and the MENEHUNE is designed specifically for the traffic characteristics of interactive computing. In a conventional communication system a user might be assigned a portion of the channel on either an FDMA or TDMA basis. Since it is well known that in time-sharing systems, computer and user data streams are bursty,7 such fixed assignments are generally wasteful of bandwidth because of the high peak-to-average data rates that characterize the traffic. The multiplexing technique the t is utilized by the ALOHANET is a purely random-access packet switching method that has come to be known as the pure ALOHA technique.8 Under a pure ALOHA mode of operation, packets are sent by the user nodes to the MENEHUNE in a completely unsynchronized manner—when a node is idle it uses none of the channel. Each full packet of 704 bits requires only 73 msecs at a rate of 9600 baud to transmit (neglecting propagation time). The random or multi-access channel can be regarded as a resource which is shared among a large number of users in much the same way as a multiprocessor's memory is "shared". Each active user node is in contention with all other active users for the user of the MENEHUNE receiver. If two nodes transmit packets at the same time, a collision occurs and both packets are rejected. In the ALOHANET, a positive acknowledgment protocol is used for packets sent on the random-access channel. Whenever a node sends a packet it must receive an acknowledgment message (ACK) from the MENEHUNE within a certain time-out period. If the ACK is not received within this interval the node automatically retransmits the packet after a randomized delay to avoid further collisions. These collisions will limit the number of users and the amount of data which can be transmitted over the channel as loading is increased. Ah analysis8 of the random-access method of transmitting packets in a pure ALOHA channel shows that the normalized theoretical capacity of such a channel is lAe=0.184. Thus, the average data rate which can be supported is about one sixth the data rate which could be supported if we were able to synchronize the packets from each user in order to fill up the channel completely. Put another way, this result shows the present 9600 bit/second channel could support between 100 and 500 active teletype users—depending upon the rate at which they generate packets and upon the packet lengths.

ALOHANET REMOTE UNITS

The original user interface developed for the system is an all-hardware unit called an ALOHANET Terminal Control Unit (TCU), and is the sole piece of equipment necessary to connect any terminal or minicomputer into the ALOHA channel. As such it takes the place of two dedicated modems for each user, a dial-up connection and a multiplexor port usually used for computer networks. The TCU is composed of a UHF antenna, transceiver, modem, buffer and control unit. The buffer and control unit functions of the TCU can also be handled by a minicomputer or a microcomputer. In the present system several minicomputers have been connected in this manner in order to act as multiplexors for terminal clusters or as computing stations with network access for resource sharing. A new version of the TCU using an Intel 8080 microcomputer for buffer and control has been built. Since these programmable units allow a high degree of flexibility for packet formats and system protocols, they are referred to as PCU's (Programmable Control Unit). A more detailed discussion of terminal considerations is given in a companion paper in these proceedings.9 Since the transmission scheme of the ALOHANET is by line-of-

sight, the radio range of the transceivers is severely limited by the diversity of terrain (mountains, high rise buildings, heavy foliage) that exists in Hawaii. A recent development has allowed the system to expand its geographical coverage beyond the range of its central transmitting station. Because of the burst nature of the transmissions in the ALOHA channel it is possible to build a simple store-and-forward repeater which accepts a packet within a certain range of ID's and then repeats the packet on the same frequency. Each repeater performs identically and independently for packets directed either to or from the MENEHUNE. Two of the repeaters have been built which extend coverage of the ALOHANET from the island of Oahu to other islands in the Hawaiian chain. These repeaters are discussed in more detail in the following section.

Simulation results with timeline for pure ALOHA, frames are 5 time units, 100 frame slots simulated (5 time units per slot), 20 sources, probability of 0.05 for transmission from each source

A probabilistic simulation program has been prepared to obtain results
and also provide printed output to allow for understanding. The program
the number of sources and frame size to be varied, along with the
duration of the simulation and the source probability for transmission.

For ease of understanding of the printed output, 20 sources have been
used for the results provided in this file.

Each frame occupies 5 time units.

The total simulation time covers the equivalent of 100 slots,
which is (5 time units per frame) * (100 slots or frames) = 500 time units.

Each source has a random initial starting time to obtain pure ALOHA,
rather than strictly slotted ALOHA. The starting time is random,
but thereafter, that particular source makes decisions about frame
transmission every 5 time units. Although each source is behaving
in a "slotted" manner, the random start times across the sources
effectively spreads out the frame starting times, which results in
behavior that reflects pure ALOHA.

The offered load is controlled by adjusting the probability that
each source attempts a transmission every 5 time units. That probability
multiplied by the number of sources gives the theoretical offered load.
The simulation program computes an empirical offered load from the
number of total attempted transmissions for comparison with the
theoretical load.

The simulation detects collisions from overlapping frames during
the same time unit.

Wherever there is no overlap for an entire frame from a given source,
that particular source succeeds in its transmission.

The total number of successes for all sources is used at the end
to obtain an overall throughput that is normalized to the number
of slots or frames for the duration of the simulation (100 in this case).

This throughput result should be close to the theoretical value
predicted for pure ALOHA for any offered load.

In the trace below, time progress from top to bottom. The timelines
for the 20 sources are provided from left to right. The '.' character
indicates idle time, and '#' is for transmission. On the left side,
units of time are identified numerically. On the right side, 5-time-unit
frame slots are identified numerically. Note that with pure ALOHA, there
is no slot-based synchronization. The frame slots are identified for the
sake of convenience in this case. Note how the start of frame transmission
from different sources are not aligned to the frame slots.

For example, the transmission from the third source succeeds in between
time unit 9 and time unit 13 (the left-side labelling). In contrast,
the two transmissions between time unit 23 and time unit 30 collide,
hence both of those transmissions fail.

Final statistics from the simulation are provided after the trace.

The summary of per-source behavior is provided below.

source 0: 0 successes / 2 attempts = 0
source 1: 1 successes / 6 attempts = 0.166667
source 2: 2 successes / 6 attempts = 0.333333
source 3: 1 successes / 4 attempts = 0.25
source 4: 0 successes / 5 attempts = 0
source 5: 0 successes / 3 attempts = 0
source 6: 0 successes / 5 attempts = 0
source 7: 2 successes / 4 attempts = 0.5
source 8: 0 successes / 4 attempts = 0
source 9: 1 successes / 5 attempts = 0.2
source 10: 1 successes / 4 attempts = 0.25
source 11: 1 successes / 2 attempts = 0.5
source 12: 0 successes / 2 attempts = 0
source 13: 1 successes / 4 attempts = 0.25
source 14: 2 successes / 6 attempts = 0.333333
source 15: 3 successes / 7 attempts = 0.428571
source 16: 0 successes / 3 attempts = 0
source 17: 1 successes / 2 attempts = 0.5
source 18: 1 successes / 11 attempts = 0.0909091
source 19: 0 successes / 10 attempts = 0

probability of each source transmitting is 0.05
number of sources is 20
resulting offered load G is 1

total number of attempts from all sources is 95
empirical offered load G normalized to 100 frame slots is 0.95
(which is close to the theoretical offered load based on
the probability of transmission and the number of sources)

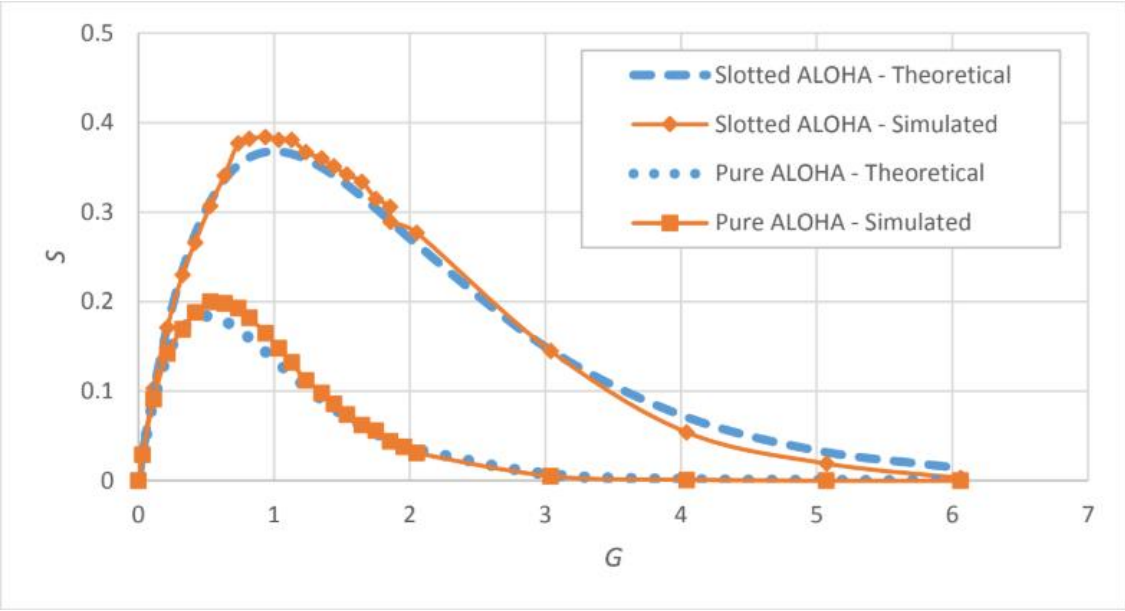
total number of successful transmissions is 17
throughput normalized to 100 frame slots is 0.17

Simulation results with timeline for slotted ALOHA, same parameters as for the pure ALOHA simulation above

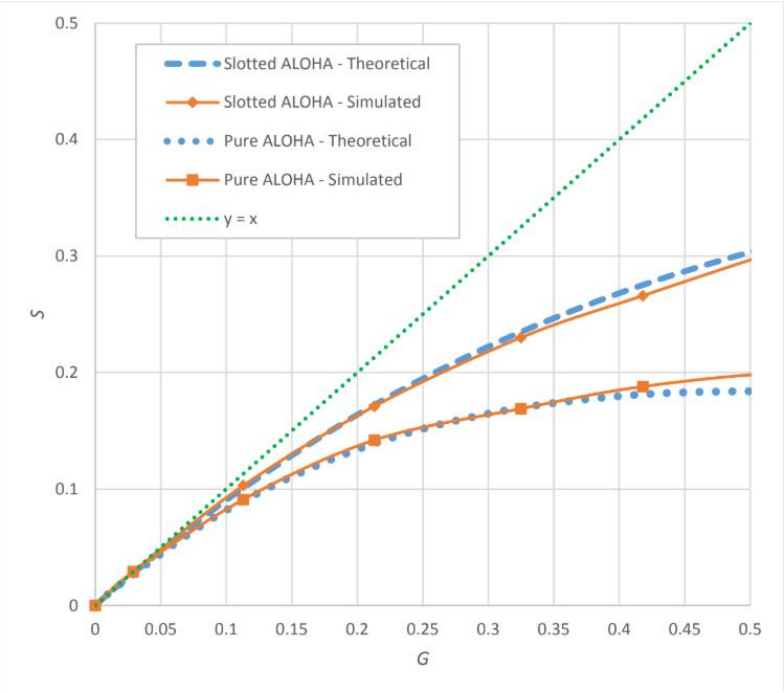
```
A probabilistic simulation program has been prepared to obtain results
and also provide printed output to allow for understanding. The program
the number of sources and frame size to be varied, along with the
duration of the simulation and the source probability for transmission.

For ease of understanding of the printed output, 20 sources have been
used for the results provided in this file.

Each frame occupies 5 time units.

The total simulation time covers the equivalent of 100 slots,
which is (5 time units per frame) * (100 slots or frames) = 500 time units.

Transmissions from each source always begin on the boundary of a
5-time-unit frame slot, reflecting strictly slotted ALOHA behavior.

The offered load is controlled by adjusting the probability that
each source attempts a transmission every 5 time units. That probability
multiplied by the number of sources gives the theoretical offered load.
The simulation program computes an empirical offered load from the
number of total attempted transmissions for comparison with the
theoretical load.

The simulation detects collisions from overlapping frames during
the same time unit (but with slotted ALOHA, entire frames overlap).
Wherever there is no overlap for an entire frame from a given source
(i.e., a frame slot is used only that one source with no others active),
that particular source succeeds in its transmission.

The total number of successes for all sources is used at the end
to obtain an overall throughput that is normalized to the number
of slots or frames for the duration of the simulation (100 in this case).

This throughput result should be close to the theoretical value
predicted for slotted ALOHA for any offered load.

In the trace below, time progress from top to bottom. The timelines
for the 20 sources are provided from left to right.  The '.' character
indicates idle time, and '#' is for transmission. On the left side,
units of time are identified numerically. On the right side, 5-time-unit
frame slots are identified numerically. With slotted ALOHA, all frames
are transmitted in a manner that is aligned with the frame slots.

For example, the transmission from the third source succeeds in between
time unit 6 and time unit 10 (the left-side labelling). In contrast,
the three transmissions between time unit 41 and time unit 45 collide,
hence all three of those transmissions fail.

Final statistics from the simulation are provided after the trace.

The summary of per-source behavior is provided below.

source 0: 1 successes / 2 attempts = 0.5
source 1: 1 successes / 6 attempts = 0.166667
```

```
source 2: 4 successes / 6 attempts = 0.666667
source 3: 1 successes / 4 attempts = 0.25
source 4: 3 successes / 5 attempts = 0.6
source 5: 0 successes / 3 attempts = 0
source 6: 2 successes / 5 attempts = 0.4
source 7: 2 successes / 4 attempts = 0.5
source 8: 1 successes / 4 attempts = 0.25
source 9: 1 successes / 5 attempts = 0.2
source 10: 2 successes / 4 attempts = 0.5
source 11: 1 successes / 2 attempts = 0.5
source 12: 1 successes / 2 attempts = 0.5
source 13: 1 successes / 4 attempts = 0.25
source 14: 4 successes / 6 attempts = 0.666667
source 15: 5 successes / 7 attempts = 0.714286
source 16: 2 successes / 3 attempts = 0.666667
source 17: 2 successes / 2 attempts = 1
source 18: 4 successes / 11 attempts = 0.363636
source 19: 3 successes / 10 attempts = 0.3

probability of each source transmitting is 0.05
number of sources is 20
resulting offered load G is 1

total number of attempts from all sources is 95
empirical offered load G normalized to 100 frame slots is 0.95
(which is close to the theoretical offered load based on
the probability of transmission and the number of sources)

total number of successful transmissions is 41
throughput normalized to 100 frame slots is 0.41
```

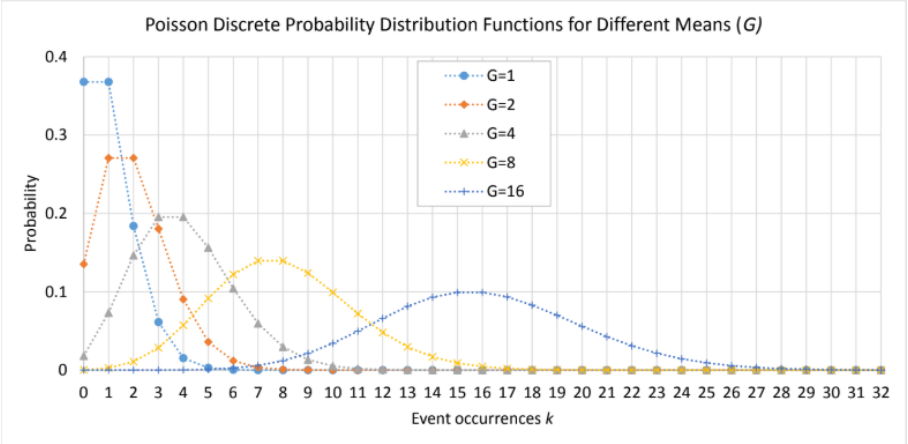
Complete set of pure/slotted ALOHA simulated throughput results, frames are 100 time units, 1000 frame slots simulated (100 time units per slot), 20 sources, different probabilities of transmission to give different offered loads, points plotted using empirical load and simulated throughput, and finally theoretical curves also included for comparison



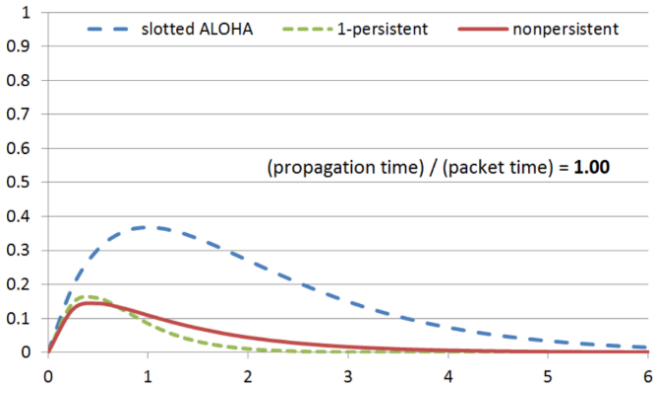
Zoomed-in view of same graph above for the range *G*=0 to *G*=0.5 to show how throughput for small loads is close to the *S*=*G* ideal behavior

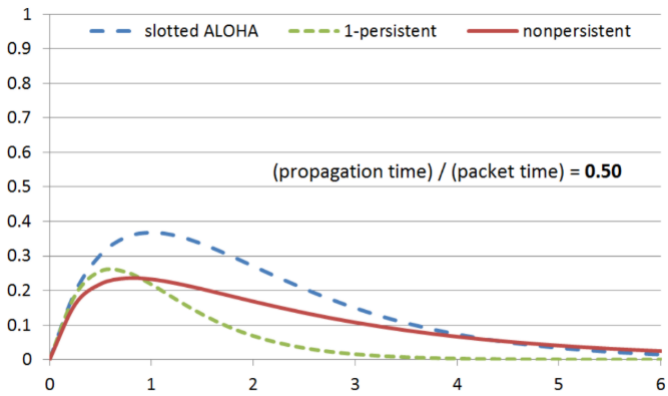


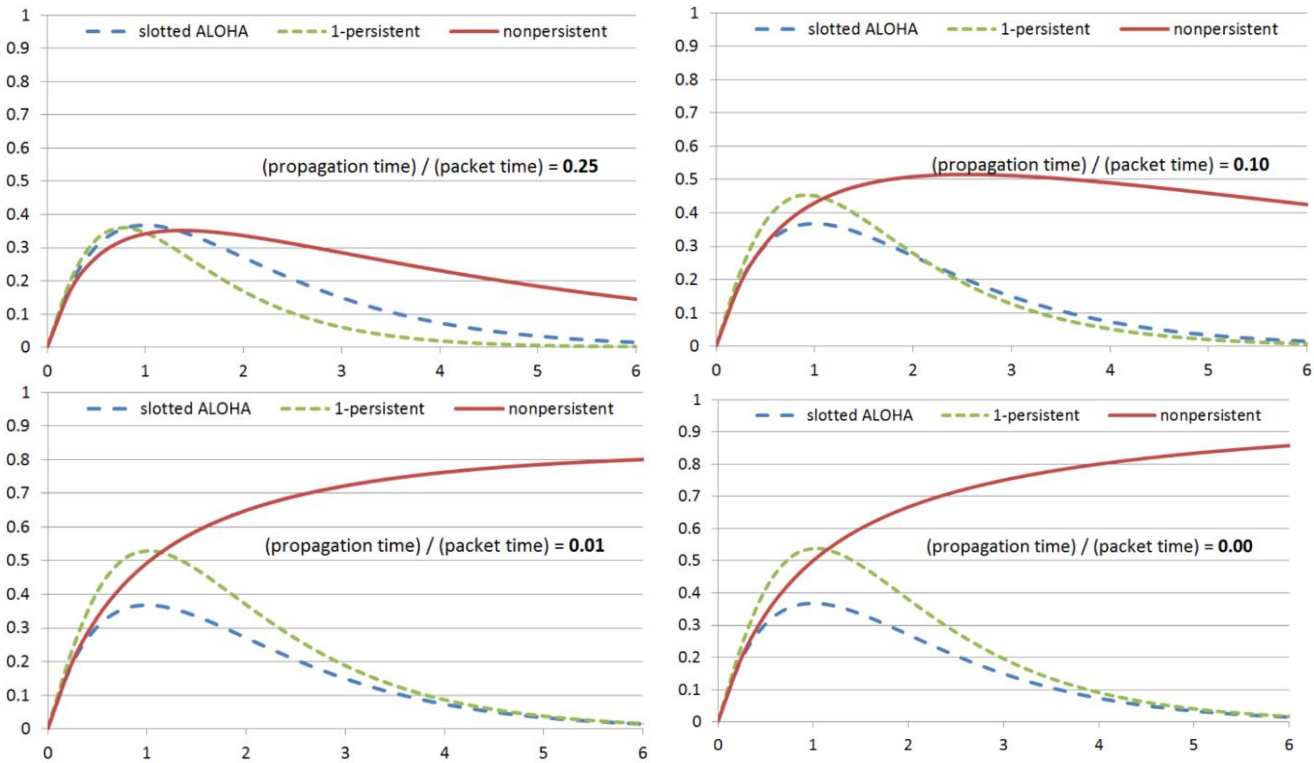
Discrete Poisson probability distributions for different means



Throughput curves generated by the instructor to compare slotted ALOHA with CSMA 1-persistent/nonpersistent







Random access techniques for data transmission over packet-switched radio channels

Skim the INTRODUCTION section.

- *** ***Read*** *the following portions of the CARRIER SENSE MULTIPLE ACCESS MODES section.* ***

  - CSMA transmission protocols and system assumptions
  - 1-persistent CSMA
  - p-persistent CSMA
  - non-persistent CSMA

- You are responsible for knowing the three CSMA protocols above. They are also discussed in Section 4.2.2 of the Tenanbaum/Wetherall textbook, which cites the above Kleinrock/Tobagi paper.
- Skim the section on throughput equations for the three protocols above and examine Figure 4 (noting the logarithmic horizontal axis, which differs from the linear horizontal axis used in the graphs provided by the instructor and the graph in Figure 4-4 on page 268 of the Tananbaum/Wetherall textbook.)

Ethernet: distributed packet switching for local computer networks (Sections 1-to-6, covers 7 pages)

- Of particular interest for your reading are the following parts: last paragraph of Section 2, last two paragraphs of Section 3.1, Sections 3.3-3.5, Section 4, and the efficiency discussion in Section 6.3 along with Table 1.
- All of the above is for classic Ethernet with a shared transmission medium.

LAST PARAGRAPH OF SECTION 2

Even when transmitted without source-detected interference, a packet may still not reach its destination without error; thus, packets are delivered *only with high probability*. Stations requiring a residual error rate lower than that provided by the bare Ethernet packet transport mechanism must follow mutually agreed upon packet protocols.

LAST TWO PARAGRAPHS OF SECTION 3.1

Looking at the relationship of interconnection and control, we see that Ethernet is the dual of a star network. Rather than distributed interconnection through many separate links and central control in a switching node, as in a star network, the Ethernet has central interconnection through the Ether and distributed control among its stations.

Unlike an Aloha Network, which is a star network with an outgoing broadcast channel and an incoming multi-access channel, an Ethernet supports many-to-many communication with a single broadcast multi-access channel.

SECTIONS 3.3-3.5

3.3 Addressing Each packet has a source and destination, both of which are identified in the packet's header. A packet placed on the Ether eventually propagates to all stations. Any station can copy a packet from the Ether into its local memory, but normally only an active destination station matching its address in the packet's header will do so as the packet passes. By convention, a zero-destination address is a wildcard and matches all addresses; a packet with a destination of zero is called a broadcast packet.

3.4 Reliability An Ethernet is probabilistic. Packets may be lost due to interference with other packets, impulse noise on the Ether, an inactive receiver at a packet's intended destination, or purposeful discard. Protocols used to communicate through an Ethernet must assume that packets will be received correctly at intended destinations *only with high probability*.

An Ethernet gives its best efforts to transmit packets successfully, but it is the responsibility of processes in the source and destination stations to take the precautions necessary to assure reliable communication of the quality they themselves desire [18, 21]. Recognizing the costliness and dangers of promising "error-free" communication, we refrain from guaranteeing reliable delivery of any single packet to get both economy of transmission and high reliability averaged over many packets [21]. Removing the responsibility for reliable communication from the packet transport mechanism allows us to tailor reliability to the application and to place error recovery where it will do the most good. This policy becomes more important as Ethernets are interconnected in a hierarchy of networks through which packets must travel farther and suffer greater risks.

3.5 Mechanisms A station connects to the Ether with a tap and a transceiver. A tap is a device for physically connecting to the Ether while disturbing its transmission characteristics as little as possible. The design of the transceiver must be an exercise in paranoia. Precautions must be taken to ensure that likely failures in the transceiver or station do not result in pollution of the Ether. In particular, removing power from the transceiver should cause it to disconnect from the Ether.

Five mechanisms are provided in our experimental Ethernet for reducing the probability and cost of losing a packet. These are (1) carrier detection, (2) interference detection, (3) packet error detection, (4) truncated packet filtering, and (5) collision consensus enforcement.

3.5.1 Carrier Detection 3.5.1 Carrier detection. As a packer's bits are placed on the Ether by a station, they are phase encoded (like bits on a magnetic tape), which guarantees that there is at least one transition on the Ether during each bit time. The passing of a packet on the Ether can therefore be detected by listening for its transitions. To use a radio analogy, we speak of the presence of carrier as a packet passes a transceiver. Because a station can sense the carrier of a passing packet, it can delay sending one of its own until the detected packet passes safely. The Aloha Network does not have carrier detection and consequently suffers a substantially higher collision rate. Without carrier detection, efficient use of the Ether would decrease with increasing packet length. In Section 6 below, we show that with carrier detection, Ether efficiency increases with increasing packet length. With carrier detection we are able to implement deference: no station will start transmitting while hearing carrier. With deference comes acquisition: once a packet transmission has been in progress for an Ether end-to-end propagation time, all stations are hearing carrier and are deferring; the Ether has been acquired and the transmission will complete without an interfering collision.

With carrier detection, collisions should occur only when two or more stations find the Ether silent and begin transmitting simultaneously: within an Ether end-toend propagation time. This will almost always happen immediately after a packet transmission during which two or more stations were deferring. Because stations do not now randomize after deferring, when the transmission terminates, the waiting stations pile on together, collide, randomize, and retransmit.

3.5.2 Interference Detection Each transceiver has an interference detector. Interference is indicated when the transceiver notices a difference between the value of the bit it is receiving from the Ether and the value of the bit it is attempting to transmit.

Interference detection has three advantages. First, a station detecting a collision knows that its packet has been damaged. The packet can be scheduled for retransmission immediately, avoiding a long acknowledgment timeout. Second, interference periods on the Ether are limited to a maximum of one round trip time. Colliding packets in the Aloha Network run to completion, but the truncated packets resulting from Ethernet collisions waste only a small fraction of a packet time on the Ether. Third, the frequency of detected interference is used to estimate Ether traffic for adjusting retransmission intervals and optimizing channel efficiency.

3.5.3 Packet Error Detection As a packet is placed on the Ether, a checksum is computed and appended. As the packet is read from the Ether, the checksum is recomputed. Packets which do not carry a consistent checksum are discarded. In this way transmission errors, impulse noise errors, and errors due to undetected interference are caught at a packet's destination.

3.5.4 Truncated Packet Filtering Interference detection and deference cause most collisions to result in truncated packets of only a few bits; colliding stations detect interference and abort transmission within an Ether round trip time. To reduce the processing load that the rejection of such obviously damaged packets would place on listening station software, truncated packets are filtered out in hardware.

3.5.5 Collision Consensus Enforcement When a station determines that its transmission is experiencing interference, it momentarily jams the Ether to ensure that all other participants in the collision will detect interference and, because of deference, will be forced to abort. Without this collision consensus enforcement mechanism, it is possible that the transmitting station which would

otherwise be the last to detect a collision might not do so as the other interfering transmissions successively abort and stop interfering. Although the packet may look good to that last transmitter, different path lengths between the colliding transmitters and the intended receiver will cause the packet to arrive damaged.

SECTION 6.3 EFFICIENCY

We now compute E, that fraction of time the Ether is carrying good packets, the efficiency. The Ether's time is divided between transmission intervals and contention intervals. A packet transmission takes P/C seconds. The mean time to acquisition is W,T. Therefore, by our simple model,

$$E = \frac{\frac{P}{C}}{\left(\frac{P}{C}\right) + W * T}$$

Table I presents representative performance figures (i.e. E) for our experimental Ethernet with the indicated packet sizes and number of continuously queued stations. The efficiency figures given do not account for inevitable reductions due to headers and control packets nor for losses due to imprecise control of the retransmission parameter 1/Q; the former is straightforwardly protocol-dependent and the latter requires analysis beyond the scope of this paper. Again, we feel that all of the Ethernets in the table are overloaded; normally loaded Ethernets will usually have a Q much less than 1 and exhibit behavior not covered by this model.

For our calculations we use a C of 3 megabits per second and a T of 16 microseconds. The slot duration T must be long enough to allow a collision to be detected or at least twice the Ether's round-trip time. We limit in software the maximum length of our packets to be near 4000 bits to keep the latency of network access down and to permit efficient use of station packet buffer storage.

For packets whose size is above 4000 bits, the efficiency of our experimental Ethernet stays well above 95 percent. For packets with a size approximating that of a slot, Ethernet efficiency approaches l/e, the asymptotic efficiency of a slotted Aloha network.

TABLE 1

Table I. Ethernet Efficiency.

Q	$P = 4096$	$P = 1024$	$P = 512$	$P = 48$
1	1.0000	1.0000	1.0000	1.0000
2	0.9884	0.9552	0.9143	0.5000
3	0.9857	0.9447	0.8951	0.4444
4	0.9842	0.9396	0.8862	0.4219
5	0.9834	0.9367	0.8810	0.4096
10	0.9818	0.9310	0.8709	0.3874
32	0.9807	0.9272	0.8642	0.3737
64	0.9805	0.9263	0.8627	0.3708
128	0.9804	0.9259	0.8620	0.3693
256	0.9803	0.9257	0.8616	0.3686

Wireless LANs and mobile networking: standards and future directions (Pages 86-89 first two paragraphs)

The field of wireless local area networks (LANs) is expanding rapidly as a result of advances in digital communications, portable computers, and semiconductor technology. The early adopters of this technology have primarily been vertical applications that place a premium on the mobility offered by such systems. Examples of these types of applications include inventory control in store and warehouse environments, point-of-sale terminals, and rental car check-in. Wireless LANs are also increasingly being used in the hospital and university environments in which users are highly mobile and may only require moderate bandwidths. In addition to the mobility that becomes possible with wireless LANs, these systems have also been used in environments where cable installation is expensive or impractical. Such environments include manufacturing floors, trading floors on stock exchanges, conventions and trade shows, and historic buildings. With the increasing proliferation of wireless LANs comes the need for standardization to allow interoperability for an increasingly mobile workforce. In this article, we discuss several emerging standards that relate to wireless LAN systems. These standards include two physical- and link-layer standards, IEEE 802.11 and European Telecommunications Standards Institute (ETSI) high-performance radio LAN (HIPERLAN), as well as a mobile networking standard, Mobile IP, and some developing standards for wireless link management. In this article, we focus on the use of radio frequency wireless LANs, as opposed to infrared wireless systems. For radio frequency wireless LANs, the availability of unlicensed spectrum is a significant enabler. In the United States, it was the Federal Communications Commission's rule change, first published in 1985 (modified in 1990) allowing unlicensed spread spectrum use of the three industrial, scientific, and medical (ISM) frequency bands, that encouraged the development of a number of wireless technologies. Today, unlicensed wireless LAN products are available in all three of the ISM bands at 902-928 MHz,' 2.400-2.4835 GHz, and 5.725-5.850 GHz. As described later, the IEEE 802.11 committee makes use of the 2.4 GHz ISM band. The discussion that follows treats several types of emerging standards which impact wireless LAN systems. We begin with a description of two influential physical- and data-link-layer standards, IEEE 802.11 and HIPERLAN. Following this, we briefly examine some developments concerning the U.S. personal communication services (PCS) bands, future spectrum allocations, and wireless asynchronous transfer mode (ATM) systems. After describing these physical- and link-layer developments, we focus on the network layer. We discuss the extensions being made to the widely used Internet Protocol (IP) to deal with mobility (wired or wireless). Finally, we describe some emerging standards for wireless link management in which interfaces are specified to provide wireless link information to protocol stacks and applications on the mobile client. In the conclusion, we speculate on future directions of wireless LAN systems.

IEEE 802.11 WIRELESS LAN STANDARD

The IEEE 802.11 committee has been working on the establishment of a standard for wireless LANs. Having begun its work in 1990, the 802.11 committee is nearing completion of the standard, which is expected to be finalized in mid-1996 Much of the standard appears to have reached final form at the current time (early 1996), so we can describe the main features of the architecture, the multiple physical layers, and the common medium access control (MAC) sublayer [1].

ARCHITECTURE

We introduce the general architecture and terminology defined by the 802 11 committee [l]. As shown in Fig. 1, two primary topologies are supported by the 802.11 standard. one in which the stations access the backbone network1 (distnbution system in 802.11 nomenclature) via access points (i.e., base stations), and one in which a group of stations communicate directly with each other in an ad hoc

network, independent of any infrastructure or base stations The first topology is useful for providing wireless coverage of building or campus areas by deploying multiple access points whose radio coverage areas overlap to provide complete coverage. The stations associated with a given access point are referred to as its basic service set (BSS) in the 802.11 standard, but more commonly as the members of the access point's cell. The second topology, the one for ad hoc networks, is useful for applications such as file sharing in a conference room scenario. The MAC protocol of the 802.11 standard was developed to allow these two types of topologies to coexist, as illustrated by the overlap in the coverage range of the ad hoc network and access point B in Fig. 1. As a prelude to the following discussion on the HIPERLAN standard, we mention that the IEEE 802.11 draft standard does not provide a mechanism for multihop routing, with the exception of the case discussed in the footnote above. That is, in an ad hoc network a station can only communicate directly with another station, and in the access point topology a station can only send packets (i.e., frames) through the access point or directly to another station. No station can be used as a relay to the access point without the use of mechanisms that go beyond those currently defined in the standard.

PHYSICAL LAYERS

The 802.11 draft standard provides for three different types of physical layers to be used:

- 2.4 GHz ISM band frequency hopping (FH) spread-spec
- 2.4 GHz ISM band direct sequence (DS) spread-spec
- Infrared (IR) light

Note that in Europe, the same 2.4 GHz band (as the U.S. ISM band) has been allocated to allow wireless LAN operation, whereas in Japan only the frequencies from 2.471 to 2.497 GHz have been allocated (requiring special provisions in the IEEE 802.11 draft standard). In addition to having three types of physical (PHY) layers, two different data rates (1 Mb/s and 2 Mb/s) have been specified for each of the above PHY layers.2 At this point in time, most of the attention has been directed toward the radio physical layers, so we will only consider these here. Note that the Infrared Data Association (IrDA), a consortium of leading U.S. and Japanese manufacturers of computers, communications equipment, and semiconductors, has been developing standards for infrared-based attachment. While current IrDA standards focus on the replacement of the point-to-point serial/parallel cables that connect computers to peripherals [2], future activities of the IrDA will focus on multipoint protocols as are used in LAN systems. The IEEE 802.11 committee allowed the definition of multiple PHY layers, in part, because the members of the committee had some interest in each of the aforementioned PHY layers and hence they sought to accommodate all of' them. The benefit of this approach is that the various advantages of each of the PHY layers can be exploited by users who want an 802.11-compliant wireless LAN [3]. The disadvantage is that two users need to specify additionally the type and data rate of their wireless LAN system to permit interoperability (e.g., an 802.11 FH 1 Mb/s system). Thus, the advantages of interoperability we experience with, say, wireline modem technology are lost, as is the cost advantage of large volumes that would accompany the choice of a single PHY layer. In FH systems, the frequency at which data is transmitted is varied among a set of frequencies (i.e., 79 frequencies in the U.S./European version of the 802.11 standard, and 23 in the Japanese version). That is, the transmitter sends data on a given frequency for a fixed length of time (i.e., the dwell time in 802.11) and then switches to the next frequency for another fixed length of time. The FH pattern is known to the receiver so that the receiver's frequency synthesizer can hop in synchronism and recover the original data signal. The FH systems defined in the 802.11 PHY are slow FH systems since they transmit multiple consecutive symbols at the

same frequency. In FH systems, adjacent or overlapping cells (Le., BSSs) use different hopping patterns. For hopping patterns with many frequencies (e.g., 79 in the U.S./European 802.11 standard), it is unlikely that the same frequency will be used at the same time by two adjacent cells. The January 1996 draft standard specifies three different sets of hopping patterns, each of which is composed of 26 patterns (i.e., 26 logical channels). The patterns within a given set have been chosen to exhibit good properties; for example, the consecutive frequencies in a given pattern are spectrally separated by at least 6 MHz to avoid a narrowband interferer. In DS systems, the original data signal is modulated by a wideband spreading signal. This spreading signal is known to the receiver, which can then recover the original data signal. Note that in the 802.11 DS PHY, unlike multicode code division multiple access (CDMA) systems, only one predefined spreading signal is used. The factor by which the bandwidth of the signal is expanded is known as theprocessinggain of the DS system; in 802.11, it is 11 (10.4 dB), which permits some resilience to narrowband noise and permits the 83 MHz U.S. band to be segmented into a few channels (i.e., 11 DS center frequencies are defined in 802.11 for the US., but only three of these channels can be used without overlap). In summary, we note that since an FH system can offer a larger number of channels (i.e., frequency-hopping patterns) than a DS system, an FH system may be more useful for dense environments in which cells have overlap with many adjacent cells. Furthermore, FH and DS systems have somewhat different types of resilience to narrowband interference. FH systems experience the interference only for a fraction of time, whereas DS systems experience a fraction of the interference power all of the time. Thus, FH systems have the performance advantage if the interference is high, DS systems if the interference is low. Currently, both types of radio systems, FH and DS, have some manufacturers backing them. It remains to be seen whether the market will be winnowed to a dominant PHY layer or both types of PHYs will maintain significant market shares. Both of these types of radio systems aim to transmit at power levels of 100 mW or less, which will enable them to achieve ranges of up to 100 m indoors, depending on data rate and building geometry and composition.

MEDIUM ACCESS CONTROL

The IEEE 802.11 draft standard defines a single MAC protocol for use with all of the aforementioned physical layers. The use of a single MAC protocol better enables chip vendors to achieve high-volume production, which will help keep the costs low for these systems. There was considerable debate and compromise preceding the adoption of the current 802.11 MAC protocol. The MAC protocol defined in the 802.11 draft is sophisticated and entails considerable complexity. The protocol has a few options, as well as several features that can be turned on and off, and combines most of the functionality that was contained in the dozen or so MAC proposals considered by the committee [4].

The important characteristics of the 802.11 MAC protocol, which are likely to remain unchanged in the final standard, are its ability to support:

- The access-point-oriented and ad hoc networking topologies
- Both asynchronous and time-critical traffic (called time-bounded services in 802.11)
- Power management

The primary access method, the distributed coordination function (DCF), used in the protocol is drawn from the family of carrier-sense multiple access with collision avoidance (CSMNCA) protocols. Since the radio medium does not permit the use of a collision detection (CD) mechanism, as used in the CSMA/CD protocol of Ethernet, the CSMNCA protocol uses a random backoff to reduce the likelihood of two frames colliding. Collisions are most likely to occur during the time period immediately following the transmission of some frame, since two or more stations may be listening to a busy medium and hence

transmit when it becomes free. In the CSMNCA protocol of 802.11, the random backoff time is distributed according to a uniform distribution (in discrete slot times) where the maximum extent of the uniform range is called the contention window (CW) in 802.11. The CW parameter, that is, the range of this uniform distribution, is doubled (up to a maximum limit) each time a frame transmission is unsuccessful, as determined by the absence of an acknowledgment (ACK) frame. This exponential backoff mechanism helps reduce collisions in response to increasing numbers of contending stations. Furthermore, as shown in Fig. 2, there is an initial interframe space (IFS) that can take on three different values representing priorities for transmission. The highest-priority frames are transmitted using the short IFS (SIFS). For example, the immediate acknowledgment that a receiving station sends back to the transmitting station makes use of the SIFS to guarantee that no other station intervenes. The next longest IFS, the point coordination function IFS (PIFS), is used to provide a priority mechanism by which time-critical frames can be transmitted before asynchronous data frames, which use the longest IFS, the distributed coordination function IFS (DIFS).

In radio systems that depend on the physical sensing of the carrier, a problem arises (called the hidden node problem [5]) in which a single receiving station can hear (i.e., is in radio range of) two different transmitters, but the two transmitters cannot hear the carrier signals of one another. In this type of topology, the transmitters send frames without performing a random backoff (because the carrier signal of the other transmitter is never heard). This results in a high likelihood of collision. The 802.11 MAC protocol includes, as an option, a well-known mechanism to solve this hidden node problem. The protocol makes use of two control frames:

- A request to send (RTS) frame that a potential transmitter issues to a receiver
- A clear to send (CTS) frame that a receiver issues in response to a transmitter's RTS frame

The CTS frame grants the requesting station permission to transmit while at the same time notifying all stations within radio range not to initiate any transmissions for a given time, which is called the net allocation vector (NAV) in 802.11. Because of the signaling overhead involved, the RTS/CTS feature is not used for short packets,for which the collision likelihood and cost (in terms of retransmission time) are both small anyway.

In order to support time-bounded services, the 802.11 standard specifies the optional use of the aforementioned point coordination function (PCF) in which a point coordinator (or PCF station) has priority control of the medium. That is, when the PCF is active, the PCF station allows only a single station in each cell to have priority access to the medium at any one time. This is implemented through the use of the previously mentioned PIFS and a beacon frame (Fig. 3) that notifies all4 of the other stations in the cell not to initiate transmissions for the length of the contention-free period (CFP). Having silenced all the stations, the PCF station can then allow a given station to have contention-free access through the use of an (optional) polling frame that is sent by the PCF station. Note that the length of the CFP can vary within each CFP repetition interval according to the system load. A typical wireless LAN installation would use different channels for adjacent cells to prevent two PCF stations (i.e., access points) from using (and hence colliding on) the same channel during the CFP. This would allow coexistence, even on the same channel, with an ad hoc network that is using DCF only.

Most of the devices in which the 802.11 standard will be used have power limitations (e.g. small handheld personal digital assistants), so options for power conservation were included in the MAC protocol. When a station is in the powersaving mode (i.e., the doze state) it cannot transmit or receive frames; however, it does keep some timers operating. The 802.1 1 standard defines power management procedures for cases with and without infrastructure (i.e., access points). In the presence of

infrastructure, a dozing station periodically wakes up and listens to selected beacons sent by the access point. If the station hears a control frame indicating that the access point has queued data for that station, the station sends a special poll frame that tells the access point to send the data. In the absence of infrastructure, the power-conserving stations in the ad hoc cell wake up for only short predefined periods of time to hear if they should remain on to receive a frame.

A final issue to consider for a wireless LAN standard is that of security to guarantee both privacy of the wirelessly transmitted data and to verify the authenticity of the wireless station or user. The 802.11 draft standard specifies an (optional) data encryption algorithm called the Wired Equivalency Privacy (WEP) algorithm. The WEP algorithm is based on the RC4 PRNG algorithm developed by RSA Data Security, Inc. [6]. The 802.11 standard describes a couple of mechanisms for supporting authentication; however, the shared key mechanism is the only one fully defined at this time. As its name suggests, in this mechanism the authentication of stations/users is based on the communicating stations having knowledge of a shared secret key

IEEE 802.11 Wireless Local Area Networks (Pages 117-121)

DESCRIPTION OF THE IEEE 802.1 1 DRAFT STANDARD ARCHITECTURE

The basic service set (BSS) is the fundamental building block of the IEEE 802.11 architecture. A BSS is defined as a group of stations that are under the direct control of a single coordination function (i.e., a DCF or PCF) which is defined below. The geographical area covered by the BSS is known as the basic service area (BSA), which is analogous to a cell in a cellular communications network. Conceptually, all stations in a BSS can communicate directly with all other stations in a BSS. However, transmission medium degradations due to multipath fading, or interference from nearby BSSs reusing the same physical-layer characteristics (e.g., frequency and spreading code, or hopping pattern), can cause some stations to appear "hidden" from other stations. An ad hoc network is a deliberate grouping of stations into a single BSS for the purposes of internetworked communications without the aid of an infrastructure network. Figure 1 is an illustration of an independent BSS (IBSS), which is the formal name of an ad hoc network in the IEEE 802.11 standard. Any station can establish a direct communications session with any other station in the BSS, without the requirement of channeling all traffic through a centralized access point (AP). In contrast to the ad hoc network, infrastructure networks are established to provide wireless users with specific services and range extension. Infrastructure networks in the context of IEEE 802.11 are established using APs. The AP is analogous to the base station in a cellular communications network. The AP supports range extension by providing the integration points necessary for network connectivity between multiple BSSs, thus forming an extended service set (ESS). The ESS has the appearance of one large BSS to the logical link control (LLC) sublayer of each station (STA). The ESS consists of multiple BSSs that are integrated together using a common distribution system (DS). The DS can be thought of as a backbone network that is responsible for MAC-level transport of MAC service data units (MSDUs). The DS, as specified by IEEE 802.11, is implementation-independent. Therefore, the DS could be a wired IEEE 802.3 Ethernet LAN, IEEE 802.4 token bus LAN, IEEE 802.5 token ring LAN, fiber distributed data interface (FDDI) metropolitan area network (MAN), or another IEEE 802.11 wireless medium. Note that while the DS could physically be the same transmission medium as the BSS, they are logically different, because the DS is solely used as a transport backbone to transfer packets between different BSSs in the ESS.

An ESS can also provide gateway access for wireless users into a wired network such as the Internet. This is accomplished via a device known as a portal. The portal is a logical entity that specifies the integration point on the DS where the IEEE 802.11 network integrates with a non-IEEE 802.11 network. If the network is an IEEE 802.X, the portal incorporates functions which are analogous to a bridge; that is, it provides range extension and the translation between different frame formats. Figure 2 illustrates a simple ESS developed with two BSSs, a DS, and a portal access to a wired LAN.

PHYSICAL LAYER

The IEEE 802.11 draft specification calls for three different physical-layer implementations: frequency hopping spread spectrum (FHSS), direct sequence spread spectrum (DSSS), and IR. The FHSS utilizes the 2.4 GHz Industrial, Scientific, and Medical (ISM) band (i.e., 2.4000-2.4835 GHz). In the United States, a maximum of 79 channels are specified in the hopping set. The first channel has a center frequency of 2.402 GHz, and all subsequent channels are spaced 1 MHz apart. The 1 MHz separation is mandated by the FCC for the 2.4 GHz ISM band. The channel separation corresponds to 1 Mb/s of instantaneous bandwidth. Three different hopping sequence sets are established with 26 hopping

sequences per set. Different hopping sequences enable multiple BSSs to coexist in the same geographical area, which may become important to alleviate congestion and maximize the total throughput in a single BSS. The reason for having three different sets is to avoid prolonged collision periods between different hopping sequences in a set [3]. The minimum hop rate permitted is 2.5 hops/s. The basic access rate of 1 Mb/s uses two-level Gaussian frequency shift keying (GFSK), where a logical 1 is encoded using frequency Fc + f and a logical 0 using frequency Fc - f. The enhanced access rate of 2 Mbis uses four-level GFSK, where 2 bits are encoded at a time using four frequencies. The DSSS also uses the 2.4 GHz ISM frequency band, where the 1 Mbis basic rate is encoded using differential binary phase shift keying (DBPSK), and a 2 Mbis enhanced rate uses differential quadrature phase shift keying (DQPSK). The spreading is done by dividing the available bandwidth into 11 subchannels, each 11 MHz wide, and using an 11-chip Barker sequence to spread each data symbol. The maximum channel capacity is therefore (11 chipsisymbol)/(ll MHz) = 1 Mbis if DBPSK is used [8]. Overlapping and adjacent BSSs can be accommodated by ensuring that the center frequencies of each BSS are separated by at least 30 MHz [3]. This rigid requirement will enable only two overlapping or adjacent BSSs to operate without interference. The IR specification identifies a wavelength range from 850 to 950 nm. The IR band is designed for indoor use only and operates with nondirected transmissions. The IR specification was designed to enable stations to receive line-of-site and reflected transmissions. Encoding of the basic access rate of 1 Mb/s is performed using 16-pulse position modulation (PPM), where 4 data bits are mapped to 16 coded bits for transmission, the enhanced access rate (2 Mbis) is performed using 4-PPM modulation, where 2 data bits are mapped to 4 coded bits for transmission.

MEDIUM ACCESS CONTROL SUBLAYER

The MAC sublayer is responsible for the channel allocation procedures, protocol data unit (PDU) addressing, frame formatting, error checking, and fragmentation and reassembly. The transmission medium can operate in the contention mode exclusively, requiring all stations to contend for access to the channel for each packet transmitted. The medium can also alternate between the contention mode, known as the contention period (CP), and a contention-free period (CFP). During the CFP, medium usage is controlled (or mediated) by the AP, thereby eliminating the need for stations to contend for channel access. IEEE 802.11 supports three different types of frames: management, control, and data. The management frames are used for station association and disassociation with the AP, timing and synchronization, and authentication and deauthentication. Control frames are used for handshaking during the CP, for positive acknowledgments during the CP, and to end the CFP. Data frames are used for the transmission of data during the CP and CFP, and can be combined with polling and acknowledgments during the CFP. The standard IEEE 802.11 frame format is illustrated in Fig. 3. Note that the frame body (MSDU) is a variable-length field consisting of the data payload and 7 octets for encryption/decryption if the optional Wired Equivalent Privacy (WEP) protocol is implemented. The IEEE standard 48-bit MAC addressing is used to identify a station. The 2 duration octets indicate the time (in microseconds) the channel will be allocated for successful transmission of a MAC protocol data unit (MPDU). The type bits identify the frame as either control, management, or data. The subtype bits further identify the type of frame (e.g., Clear to Send control frame). A 32-bit cyclic redundancy check (CRC) is used for error detection.

DISTRIBUTED COORDINATION FUNCTION

The DCF is the fundamental access method used to support asynchronous data transfer on a best effort basis. As identified in the specification, all stations must support the DCF. The DCF operates solely in the ad hoc network, and either operates solely or coexists with the PCF in an infrastructure

network. The MAC architecture is depicted in Fig. 4, where it is shown that the DCF sits directly on top of the physical layer and supports contention services. Contention services imply that each station with an MSDU queued for transmission must contend for access to the channel and, once the MSDU is transmitted, must recontend for access to the channel for all subsequent frames. Contention services promote fair access to the channel for all stations. The DCF is based on carrier sense multiple access with collision avoidance (CSMA/CA). CSMA/CD (collision detection) is not used because a station is unable to listen to the channel for collisions while transmitting. In IEEE 802.11, carrier sensing is performed at both the air interface, referred to as physical currier sensing, and at the MAC sublayer, referred to as virtual carrier sensing. Physical carrier sensing detects the presence of other IEEE 802.11 WLAN users by analyzing all detected packets, and also detects activity in the channel via relative signal strength from other sources. A source station performs virtual carrier sensing by sending MPDU duration information in the header of request to send (RTS), clear to send (CTS), and data frames. An MPDU is a complete data unit that is passed from the MAC sublayer to the physical layer. The MPDU contains header information, payload, and a 32-bit CRC. The duration field indicates the amount of time (in microseconds) after the end of the present frame the channel will be utilized to complete the successful transmission of the data or management frame. Stations in the BSS use the information in the duration field to adjust their network allocation vector (NAV), which indicates the amount of time that must elapse until the current transmission session is complete and the channel can be sampled again for idle status. The channel is marked busy if either the physical or virtual carrier sensing mechanisms indicate the channel is busy. Priority access to the wireless medium is controlled through the use of interframe space (IFS) time intervals between the transmission of frames. The IFS intervals are mandatory periods of idle time on the transmission medium. Three IFS intervals are specified in the standard: short IFS (SIFS), point coordination function IFS (PIFS), and DCF-IFS (DIFS). The SIFS interval is the smallest IFS, followed by PIFS and DIFS, respectively. Stations only required to wait a SIFS have priority access over those stations required to wait a PIFS or DIFS before transmitting; therefore, SIFS has the highest-priority access to the communications medium. For the basic access method, when a station senses the channel is idle, the station waits for a DIFS period and samples the channel again. If the channel is still idle, the station transmits an MPDU. The receiving station calculates the checksum and determines whether the packet was received correctly. Upon receipt of a correct packet, the receiving station waits a SIFS interval and transmits a positive acknowledgment frame (ACK) back to the source station, indicating that the transmission was successful. Figure 5 is a timing diagram illustrating the successful transmission of a data frame. When the data frame is transmitted, the duration field of the frame is used to let all stations in the BSS know how long the medium will be busy. All stations hearing the data frame adjust their NAV based on the duration field value, which includes the SIFS interval and the ACK following the data frame. Since a source station in a BSS cannot hear its own transmissions, when a collision occurs, the source continues transmitting the complete MPDU. If the MPDU is large (e.g., 2300 octets), a lot of channel bandwidth is wasted due to a corrupt MPDU. RTS and CTS control frames can be used by a station to reserve channel bandwidth prior to the transmission of an MPDU and to minimize the amount of bandwidth wasted when collisions occur. RTS and CTS control frames are relatively small (RTS is 20 octets and CTS is 14 octets) when compared to the maximum data frame size (2346 octets). The RTS control frame is first transmitted by the source station (after successfully contending for the channel) with a data or management frame queued for transmission to a specified destination station. All stations in the BSS, hearing the RTS packet, read the duration field (Fig. 3) and set their NAVs accordingly. The destination station responds to the RTS packet with a CTS packet

after an SIFS idle period has elapsed. Stations hearing the CTS packet look at the duration field and again update their NAV. Upon successful reception of the CTS, the source station is virtually assured that the medium is stable and reserved for successful transmission of the MPDU. Note that stations are capable of updating their NAVs based on the RTS from the source station and CTS from the destination station, which helps to combat the “hidden terminal” problem. Figure 6 illustrates the transmission of an MPDU using the RTS/CTS mechanism. Stations can choose to never use RTS/CTS, use RTS/CTS whenever the MSDU exceeds the value of RTS-Threshold (manageable parameter), or always use RTSICTS. If a collision occurs with an RTS or CTS MPDU, far less bandwidth is wasted when compared to a large data MPDU. However, for a lightly loaded medium, additional delay is imposed by the overhead of the RTSiCTS frames. Large MSDUs handed down from the LLC to the MAC may require fragmentation to increase transmission reliability. To determine whether to perform fragmentation, MPDUs are compared to the manageable parameter Fragmentation-Threshold. If the MPDU size exceeds the value of Fragmentation-Threshold, the MSDU is broken into multiple fragments. The resulting MPDUs are of size Fragmentation-Threshold, with exception of the last MPDU, which is of variable size not to exceed Fragmentation-Threshold. When an MSDU is fragmented, all fragments are transmitted sequentially (Fig. 7). The channel is not released until the complete MSDU has been transmitted SUCcessfully, or the source station fails to receive an acknowledgment for a transmitted fragment. The destination station positively acknowledges each successfully received fragment by sending a DCF ACK back to the source station. The source station maintains control of the channel throughout the transmission of the MSDU by waiting only an SIFS period after receiving an ACK and transmitting the next fragment. When an ACK is not received for a previously transmitted frame, the source station halts transmission and recontends for the channel. Upon gaining access to the channel, the source starts transmitting with the last unacknowledged fragment. 5 If RTS and CTS are used, only the first fragment is sent using the handshaking mechanism. The duration value of RTS and CTS only accounts for the transmission of the first fragment through the receipt of its ACK. Stations in the BSS thereafter maintain their NAV by extracting the duration information from all subsequent fragments. The collision avoidance portion of CSWCA is performed through a random backoff procedure. If a station with a frame to transmit initially senses the channel to be busy; then the station waits until the channel becomes idle for a DIFS period, and then computes a random backoff time. For IEEE 802.11, time is slotted in time periods that correspond to a Slot-Time. Unlike slotted Aloha, where the slot time is equal to the transmission time of one packet, the Slot-Time used in IEEE 802.11 is much smaller than an MPDU and is used to define the IFS intervals and determine the backoff time for stations in the CP. The Slot-Time is different for each physical layer implementation. The random backoff time is an integer value that corresponds to a number of time slots. Initially, the station computes a backoff time in the range 0-7. After the medium becomes idle after a DIFS period, stations decrement their backoff timer until the medium becomes busy again or the timer reaches zero. If the timer has not reached zero and the medium becomes busy, the station freezes its timer. When the timer is finally decremented to zero, the station transmits its frame. If two or more stations decrement to zero at the same time, a collision will occur, and each station will have to generate a new backoff time in the range 0-15. For each retransmission attempt, the backoff time grows as LZ2 + . ranf()l . Slot-Time, where i is the number of consecutive times a station attempts to send an MPDU, ranf() is a uniform random variate in (0,1), and Lx] represents the largest integer less than or equal to x. The idle period after a DIFS period is referred to as the contention window (CW). The advantage of this channel access method is that it promotes fairness among stations, but its weakness is that it probably could not support DTBS. Fairness is maintained because each station

must recontend for the channel after every transmission of an MSDU. All stations have equal probability of gaining access to the channel after each DIFS interval. Time-bounded services typically support applications such as packetized voice or video that must be maintained with a specified minimum delay. With DCF, there is no mechanism to guarantee minimum delay to stations supporting time-bounded services.

POINT COORDINATION FUNCTION (PCF)

The PCF is an optional capability, which is connection-oriented, and provides contention-free (CF) frame transfer. The PCF relies on the point coordinator (PC) to perform polling, enabling polled stations to transmit without contending for the channel. The function of the PC is performed by the AP within each BSS. Stations within the BSS that are capable of operating in the CF period (CFP) are known as CF-aware stations. The method by which polling tables are maintained and the polling sequence is determined, is left to the implementor. The PCF is required to coexist with the DCF and logically sits on top of the DCF (Fig. 4). The CFP repetition interval (CFP-Rate) is used to determine the frequency with which the PCF occurs. Within a repetition interval, a portion of the time is allotted to contention-free traffic, and the remainder is provided for contention-based traffic. The CFP repetition interval is initiated by a beacon frame, where the beacon frame is transmitted by the AP. One of its primary functions is synchronization and timing. The duration of the CFP repetition interval is a manageable parameter that is always an integral number of beacon frames. Once the CFP-Rate is established, the duration of the CFP is determined. The maximum size of the CFP is determined by the manageable parameter CFP-Max-Duration. The minimum value of CFP-Max-Duration is the time required to transmit two maximum-size MPDUs, including overhead, the initial beacon frame, and a CF-End frame. The maximum value of CFP-Max-Duration is the CFP repetition interval minus the time required to successfully transmit a maximumsize MPDU during the CP (which includes the time for RTS/CTS handshaking and the ACK). Therefore, time must be allotted for at least one MPDU to be transmitted during the CP. It is up to the AP to determine how long to operate the CFP during any given repetition interval. If traffic is very light, the AP may shorten the CFP and provide the remainder of the repetition interval for the DCF. The CFP may also be shortened if DCF traffic from the previous repetition interval carries over into the current interval. The maximum amount of delay that can be incurred is the time it takes to transmit an RTSICTS handshake, maximum MPDU, and ACK. Figure 8 is a sketch of the CFP repetition interval, illustrating the coexistence of the PCF and DCF.

At the nominal beginning of each CFP repetition interval, all stations in the BSS update their NAV to the maximum length of the CFP (i.e., CFP-Max-Duration). During the CFP, the only time stations are permitted to transmit is in response to a poll from the PC or for transmission of an ACK a SIFS interval after receipt of an MPDU. At the nominal start of the CFP, the PC senses the medium. If the medium remains idle for a PIFS interval, the PC transmits a beacon frame to initiate the CFP. The PC starts CF transmission a SIFS interval after the beacon frame is transmitted by sending a CF-Poll (no data), Data, or Data+CF-Poll frame. The PC can immediately terminate the CFP by transmitting a CF-End frame, which is common if the network is lightly loaded and the PC has no traffic buffered. If a CF-aware station receives a CF-Poll (no data) frame from the PC, the STA can respond to the PC after a SIFS idle period, with a CF-ACK (no data) or a Data + CF-ACK frame. If the PC receives a Data + CFAck frame from a station, the PC can send a Data + CFACK + CF-Poll frame to a different station, where the CF-ACK portion of the frame is used to acknowledge receipt of the previous data frame. The ability to combine polling and acknowledgment frames with data frames, transmitted between stations and the PC, was designed to improve efficiency. If the PC transmits a CF-Poll (no data) frame and the destination station does not

have a data frame to transmit, the station sends a Null Function (no data) frame back to the PC. Figure 9 illustrates the transmission of frames between the PC and a station, and vice versa. If the PC fails to receive an ACK for a transmitted data frame, the PC waits a PIFS interval and continues transmitting to the next station in the polling list. After receiving the poll from the PC, as described above, the station may choose to transmit a frame to another station in the BSS. When the destination station receives the frame, a DCF ACK is returned to the source station, and the PC waits a PIFS interval following the ACK frame before transmitting any additional frames. Figure 10 illustrates station-to-station frame transmission during the CFP. The PC may also choose to transmit a frame to a non-CFaware station. Upon successful receipt of the frame, the station would wait a SIFS interval and reply to the PC with a standard ACK frame. Fragmentation and reassembly are also accommodated with the Fragmentation-Threshold value used to determine whether MSDUs are fragmented prior to transmission. It is the responsibility of the destination station to reassemble the fragments to form the original MSDU.