Announcements

- Reading
  - Chapter 4.5 & 7.1
- Midterm #2 was returned
- No office hours next week for Dr. Hollingsworth
- Project #4
  - Due Thursday at 5 PM

Midterm Results

	#1	#2	#3	#4	#5	#6	Tot
min	4	0	0	0	0	0	15
max	20	15	15	15	15	20	92
avg	17	8	10	5	11	14	64.0
std							16.1

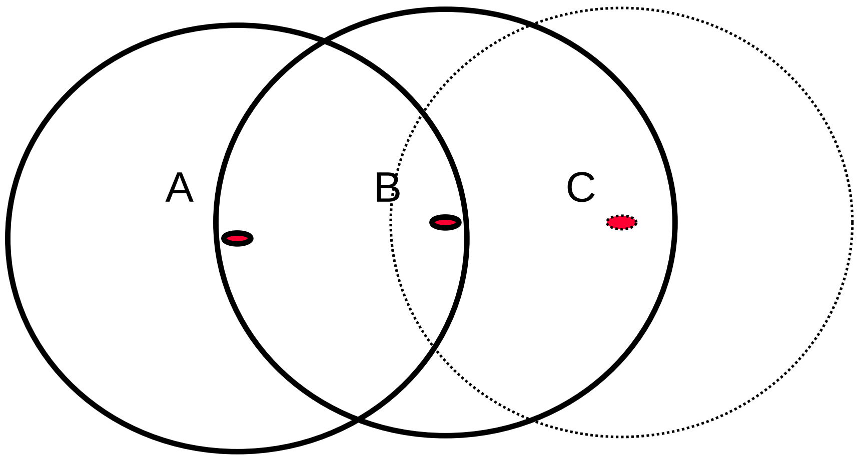
Collision Free Protocols

- Use an allocation scheme
  - must be dynamic (based on load) or we are reduced to TDM
- Bit Map Reservation Protocol
  - round of allocation (contention period)
  - everyone who indicated a desire to send goes in turn
  - requires an overhead of one bit per **per station** per round
- Binary Countdown
  - reservation round send your host address
    - uses a “wired or” to compute winner
    - as soon as a station senses a 1 where it sent 0 it backs off
  - winner sends packet
  - gives higher priority to higher numbered hosts
    - can “rotate” station number after successful transmission

Wireless Networks (MACA)

- Stations send data into the air
  - not all stations can “see” all other stations
- Need to avoid collisions between sender an receiver
  - possible for the sender to not be able to sense collision
- Use a two stage protocol
  - send a RTS (request to send)
  - receiver responds CLS (clear to send)
- Hosts that hear a RTS or CLS wait and don’t send
  - collisions still possible since two RTS frames may collide

Wireless Shared Channels



- Every node may node be in range of every other node
  - a is in range to send to b, but not c
  - b can send to a or c
  - c can send to b
- Collisions
  - carrier sense will not work due to range
  - must avoid any host sending that is in rang of sender **or** receiver

FDDI

- Fiber base ring
  - two rings, one clockwise the other counter clockwise
  - use LEDs to send data
- Encoding
  - uses 4 of 5 encoding
  - looses self clocking property of Manchester encoding
    - uses long frame header to compensate
- Supports Synchronous traffic
  - each sync frame has 96 bytes of data every 125µs
    - supports 4 T-1 lines
    - up to 16 synchronous slots may be used
- Timers
  - token holding timer: forces a node to give up the token
  - token rotation timers: recovers from lost token if its not seen

HIPPI

- KISS based path to almost 1Gbps
  - no options
  - use copper interface
- Parallel Connection
  - 32 bits wide
  - 18 control bits
  - 50 twisted pair wires
- Connections
  - uses a cross-bar switch
  - sends in groups of 256 words
- Error checking
  - parity bit per word
  - parity word at the end of each frame
    - over the vertical 256 bits

Computer And Network Security

- Issues
  - secrecy: can someone read a message
  - authentication: determine who you are communicating with
    - this can be one way or two way
  - nonrepudiation: verify that something send can't be recanted
  - integrity: a third party can't change a message in flight
  - denial of service: make the system unavailable to others
- Threat Model
  - must consider acceptable risks
    - value of item to be protected
    - $2,000 of computer time to steal 50 cents of data
      - this is a sufficient deter someone
      - **but** computers keep getting faster
  - who do you trust?
    - employees
    - vendor of security software
    - network provider

Where to Provide Security?

- Short Answers: at all levels
- physical:
  - wrap gas or tripwires around cable
- link:
  - encryption protects the wire but not the router
- network:
  - firewalls filter packets
  - end-to-end encryption
- session/presentation:
  - “secure” socket layer
- application:
  - PGP signed messages
  - application specific authentication

Other Attacks

- Random Messages
  - Will a random message likely be a valid message
  - Need to have redundancy in the message
  - **tension** more redundancy ease cryptoanalysis
- Replay Attacks
  - can the same message be sent twice?
    - transfer $10,000 from Smith to Jones
    - make an exact copy of a metro fare card
  - need to ensure messages apply exactly once
    - use a timestamped lifetime
    - sequence numbers

Digital Water Marks

- Issue: If I have a copy of a digital object, I can make many
  - if you pay per-copy for the object, how to you prevent copies?
- Goal: Track where an object came from
  - make every object unique
  - the objects should not appear different

Cryptography

- Terms
  - plaintext (P): the raw message to be sent
  - key (K): data used to protect one or more messages
  - ciphertext (C): output of applying key to plaintext
  - encrypt (E): a function to combine the key and plaintext
  - decrypt (D): a function to combine ciphertext and key
    - may be the same as E
  - $C = E_k(P)$ and $D_k(E_k(P)) = P$
- Substitution Cipher
  - Ceaser Cipher
    - shift letters by a constant amount
    - key is how many letters to shift
  - Monoalphabetic substitution
    - for each letter pick some a different letter to use
    - key is 26 characters representing substitution
    - can use properties of language to break it

Transposition Cipher

- Block of text is used to break up digrams
- To Break:
  - each letter is itself, so normal distribution of letters is seen
  - guess number of columns (verify with known plaintext)
  - order columns using trigram frequency

M	E	G	A	B	U	C	K
7	4	5	1	2	8	3	6
p	l	e	a	s	e	t	r
a	n	s	f	e	r	o	n
e	m	i	l	l	i	o	n
d	o	l	l	a	r	s	t
o	m	y	s	w	i	s	s
b	a	n	k	a	c	c	o
u	n	t	s	i	x	t	w
o	t	w	o	a	b	c	d

Plaintext
pleasetransferonemilliondollarsto
myswissbankaccountsixtwotwo

Ciphertext
AFLLSKSOSELAWAIATOOSSCTCLNMOMAI
ESILYNTWRNNTSOWDPAEDOBUOERIRICXI

From: *Computer Networks*, 3rd Ed. by Andrew S. Tanenbaum, (c)1996 Prentice Hall.

One Time Pad

- Key Idea: randomness in key
- Create a random string as long as the message
  - each party has the pad
  - xor each bit of the message with the a bit of the key
- Almost impossible to break
- Some practical problems
  - need to ensure key is not captured
  - a one bit drop will corrupt the rest of the message
- Pseudo-random is not good enough
  - Japanese JN-25 during WWII was pseudo random onetime pad