Computer Networks Quiz # 4

Charlie Coleman

6 Link layer and LANS

6.1 Introduction, Services

Terminology:

- hosts & routers: nodes
- communication channels that connect adjacent nodes along communication path: links
  - wired links
  - wireless links
  - LANs
- layer-2 packet: frame, encapsulates datagram

data-link layer has responsibility of transferring datagram from one node to physically adjacent node over a link.

Link Layer Services

Framing:

Used in almost all link-layer protocols, framing encapsulates the network-layer datagrams within a link-layer frame before transmission. Frame consists of: data field (network layer datagram is inserted here) and a number of header fields. Structure is defined by the link-layer protocol.

Link Access:

MAC — medium access control

A MAC protocol specifies the rules by which a frame is transmitted onto the link. The MAC protocol complexity is tied to how many senders/receivers exist on the line.

Reliable delivery:

Reliable delivery means the service guarantees the transmission of the network-layer datagram without error, like TCP. Can be achieved with acks + retransmission. Reliable LL transport is typically used on links with high error rates (wireless). This prevents end-to-end retransmission. Adds potentially unnecessary overhead to low error rate conns, like fiber/ethernet.

Error detection & correction

Include some form of error checking bits, perform the check locally on the LL to prevent sending a bad datagram

Where is the LL implemented?

In every host.

Typically in an 'adaptor' (network interface card) or chip (e.g. ethernet card, 802.11 card, etc.)

6.2 Error detection, Correction

Most basic form: Redundancy

Error Detection and Correction (EDC)

EDC — Error Detection and Correction bits, a.k.a. the redundancy

D — Data protected by error checking, may include the header fields

Error Detection is not 100% reliable!

- protocols can miss errors (rarely though)
- larger EDC fields == better error detection/correction (but more overhead)

How do we detect errors?

1. Parity checking
   - Vertical parity checking
   - Horizontal parity checking
   - Both
2. Checksum (on IPv6 headers & UDP/TCP data)
3. CRCs

6.3 Multiple Access Protocols

Multiple Access Links

Two Types of "Links"

- point-to-point
  - PPP for dial-up access
  - point-to-point link between ethernet switch, host
- broadcast (shared wire or medium)
  - old-fashioned ethernet
  - upstream HFC
  - 802.11 wireless LAN

Access Control Point Goals

1. At any time, only one needs to access the channel
2. Even if more access the channel, there should be minimal or no collision!

No out-of-band channel are allowed for coordination

A "collision" occurs if a node receives two or more signals at the same time
Multiple Access protocol — distributed algo that determines how nodes share a channel, i.e. determine when nodes can transmit
No-out-of-bound channel constraint — communication about channel sharing must use the channel itself

An Ideal Multi-access protocol

Given: A broadcast channel of rate R bps
Want:

1. when one node wants to transmit, it can send at rate R.
2. when M nodes want to transmit, each can send at average rate R/M
3. fully decentralized (or distributed):
   - no special node coordinate transmissions
   - no synch of clocks, slots
4. As simple as possible to implement (always true)

3 Broad Classes of MAC protocols

- Channel Partitioning
  - divide channel into smaller pieces (time slots, frequency, code)
  - allocate piece to node for exclusive use
- Random Access
  - channel not divided, allow collisions
  - "recover" from collisions
- "Taking Turns"
  - nodes take turns, but nodes with more to send can take longer

Channel Partitioning MAC Protocols

- TDMA: Time Division Multiple Access
  - Access to channel in "rounds"
  - Each situation gets fixed length slot (length = packet transmission time) in each round
  - unused slots go idle (ew)

Pros	Cons
No Collision!	channel is underutilized when few sources have packets
Fair allocation	nodes must wait their turn, even if it is free

- FDMA: Frequency Division Multiple Access
  - channel spectrum divided into frequency bands
  - each station assigned fixed frequency band
  - unused transmission time in frequency bands goes idle
  - Guard bands are introduced to avoid interference
- CDMA: Code Division Multiple Access
  - Assign a different code to each channel
  - Channels then use a different code to reconstruct bits
  - **Multiple nodes can send at the same time!**
- WDMA: Wavelength Division ... (used in fiber)
  - Same principle as FDMA
- SDMA: Space Division ...
  - Reuse the same frequency but at different space (like radio stations)
- OFDMA: Orthogonal Frequency Division ...
  - Frequency slots are orthogonal so no guard bands

Random Access Protocols

When a node has a packet to send
- transmit at full channel data rate R
- no *a priori* coordination among nodes

Collision? Wait a bit (random amount) and retry!

1. Slotted ALOHA (retransmit with prob p)
   Assumptions:
   (a) All frames same size
   (b) Time divided into equal size slots (time to transmit 1 frame)
   (c) Nodes start to transmit only slot beginning
   (d) Nodes are sync'ed
   (e) if $\geq$2 nodes transmit in slot, all nodes detect collision
   (f) if collision, probability p you transmit in each frame until success
   - Pros:
     - single active node can continuously transmit at full channel rate
     - highly decentralized: only slots in nodes need to be in sync
     - simple
   - Cons:
     - collisions, wasting time slots
     - idle slots
     - nodes may be able to detect collision in less than time to transmit packet
     - clock sync required
2. ALOHA
   - No sync, no time slots, just wait a random amount of time
   - Less efficient than slotted!
3. CSMA: Carrier Sense Multiple Access
   - Listen before you transmit!
   - If idle, transmit everything
   - If busy, wait

- If collision, sucks for you. just do it again?
- propagation delay → collisions

4. CSMA/CD: CSMA + collision detection
   - Cancel transmissions when collision is detected
   - easy in wired transmission, difficult wirelessly

Taking Turns: Literally Jesus?

Channel Partitioning Protocols:
- share channel efficiently & fairly at high loads
- super shit at low load

Random Access Protocols:
- efficient at low loads
- 8 car pile up at high loads

"Taking Turns" Protocols:
Everything you've ever wanted and more

Examples:
- Polling:
  - master node invites slave nodes to transmit in turn
  - typically used with "dumb" slave devices
  - Concerns:
    * polling overhead
    * latency
    * single point of failure (master)
- Token Passing
  - Control token passed from one node to next sequentially
  - token message
  - concerns:
    * token overhead
    * latency
    * token is a single point of failure

6.4 LANs

Addressing

Every adapter on LAN has it's own unique LAN address
MAC addresses are allocated by IEEE, bought buy manufacturer to ensure uniqueness
MAC is portable, as LAN cards can move between LANs
IP hierarchical address is not portable, depends on IP subnet

ARP

ARP — Address Resolution Protocol, each IP node on LAN has table
- IP/MAC address mappings for some LAN nodes `< IP address; MAC address; TTL >`
- TTL (Time to Live): time after which address mappings will be forgotten (typically 20 min)

The Protocol
- A wants to send datagram to B
  but B's MAC address not in A's ARP table
- A broadcasts ARP query packet, containing B's IP address
  - destination MAC address = FF-FF-FF-FF-FF-FF
  - all nodes on LAN receive ARP query
- B receives ARP packet, replies to A with its (B's) MAC address, send to A's MAC
- A caches (saves) IP-to-MAC address pair in its ARP table until information becomes old (times out)
  (this is a soft state, information goes away)

- ARP is "plug-and-play", nodes create their own ARP table

Ethernet

- Dominant wired LAN tech
- Single chip, multiple speeds
- first widely used LAN tech
- simple, cheap
- kept up with speed race: 10Mbps - 10Gbps
- Connectionless - no handshaking
- Unreliable - no acks/nacks
- Uses CSMA/CD with binary back-off

Topologies

- Bus - popular through mid-90s
  - all nodes in same collision domain (can collide with each other)
- Star - popular today
  - active switch in the center of the network
  - each spoke runs a separate ethernet protocol (no collision)

Ethernet Frame

- sending adaptar encapsulates IP datagram in Ethernet Frame

1. Preamble - 7 bytes of 10101010 followed by 10101011, syncs the clock & rate
2. Addresses - 6 byte source & dest MAC addresses, if it's for the adapter it passes to the network layer protocol
3. type - indicates higher layer protocol (mostly IP, but others possible)
4. CRC - error detection, frame dropped if error detected

Switches

- Link-Layer device - active role
  - store & forward Ethernet frames
  - Examine MAC address, selectively forward, use CSMA/CD
- Transparent, hosts are unaware they exist
- Plug-and-play, self-learning — No config required!
- Buffer packets
- Separate instance of protocol on each link, no collisions

VLANs

VLAN — Virtual LAN, simplify LAN topology using software 'switches'

6.5 Link Virtualization

MPLS

MPLS — MultiProtocol Layer Switching
Operates between OSI Layer 2 and Layer 3

- Initial Goal — high-speed IP forwarding using fixed length label (instead of IP address)
  - fast lookup using fixed length identifier (rather than shortest prefix matching)
  - borrowing ideas from Virtual Circuit approach
  - but IP datagram still keeps IP address!
- MPLS forwarding can differ from IP
  - use destination and source addresses to route flows to same destination differently (traffic engineering)
  - re-route flows quickly if link fails: pre-computed backup paths (useful for VoIP)

8 Network Security

8.1 What is Networking Security?

Types of attacks

- Lying
  - DNS poisoning
  - BGP false route advertising
  - False IP or MAC address
- Talking too much
  - Congest someone's server
  - Congest someone's network
- Listening too much
  - side channel attacks in VM
  - Man in the middle attack

Properties of a Secure Communication

1. Confidentiality — only sender & intended receiver should "understand" message contents
   - sender encrypts message
   - receiver decrypts message
2. End Point Authentication
   - sender, receiver want to confirm identity of each other
3. Message Integrity — sender, receiver want to ensure message not altered without detection
4. Access & Availability — services must be accessible and available to users

8.2 Principles of Cryptography

- Symmetric Key Crypto — sender, receiver share a secret key
  - Stream ciphers — have a keystream, plaintext digits are encrypted one at a time to create a stream of encrypted data
  - Block ciphers — encrypt 1 block at a time, send it all
  - Cipher block chaining — prevents memorizing encrypted data and comparing to future, add some randomness to the cipher and send the randomness in plaintext
    to save bandwidth, send once then use a generator
  - **DES: Data Encryption Standard** — popular symmetric method
    - US encryption standard
    - 56 bit encryption key, 64 bit block size
    - block cipher + CBC
    - Not that secure, so just do it 3 times with 3 keys, duh
  - **AES: Advanced Encryption Standard** — DES? Never heard of him.
    - still symmetric, replaced DES
    - 128bit block, 128/192/256 bit keys
    - if DES can be cracked in 1 sec, AES will take 149 trillion years
- Public Key Crypto — sender, receiver have a public + private key
  - No symmetric key
  - Need a function that returns the same value when executed on either side
  - **RSA** — Rivest, Shamir, Adelson algo
    1. Choose 2 large prime numbers p, q (1024+ bits ea)
    2. n = pq, z = (p-1)(q-1)
    3. e ¡ n && e is relatively prime with z
    4. choose d where e*d mod z = 1
    5. Public Key: (n, e), Private Key: (n, d)

    Encryption/Decryption
    1. To encrypt message m, $c = m^e \bmod n$
    2. To decrypt encrypted message c, $m = c^d \bmod n$
    - DES is 100x faster

        * To improve speeds, establish a connection using RSA and generate a symmetric key, then use AES/DES/another symm key crypto

8.3 Message Integrity

Goals

- message is indeed send by intended sender
- message is not tampered with on its way to the receiver

Digital Signatures

- Cryptographic Hash
  - Hash function (H(m)) takes an input & computes a fixed-size string (checksum/CRC)
  - Hashes have the property that H(x) == H(y) is very unlikely (unfeasible)
  - Simple digital signature - encrypt with your private key!
  - Hash functions:
    * MD5 — 128 bit hash
    * SHA-1 — 160 bit message digest
  - Use a secret shared key to prevent tampering with the message
- Certification Authorities
  - binds public key to a particular entity
  - entity registers its public key with CA
    * entity provides "proof of identity" to CA
    * CA creates certificate binding entity to its public key
    * certificate contains entity's public key digitally signed by the CA

8.4 End Point Authentication

Authenticating a conversation at the time it is occurring

- needs to run before communication can commence
- basically use public key encryption + CA + a nonce (one time use random number to prevent replay attacks)

8.5 Securing e-mail

Confidentiality

1. Generate random symmetric private key
2. encrypt message with symm priv key
3. encrypts symm priv key with receiver's public key
4. send both to receiver
5. receiver decodes symm priv key using their private key
6. receiver decodes message with symm priv key

Message Integrity

1. Sign message with hash, m' = H(m + s)
2. Sign with priv key
3. Send message and encrypted hash
4. receiver can decode the hash, hash the received message and compare

Both?

Chain message integrity into confidentiality

8.6 Securing TCP Connections: SSL

- supported by almost all browsers & web servers
- Base for https
- billions sent over SSL every year
- TLS - variation
- Provides:
  - confidentiality
  - integrity
  - authentication
- PGP (the email stuff) would not work for byte streams or interactive data

4 Components

1. Handshake — use certificates & private keys to authenticate each other and exchange shared secret
2. Key derivation — use shared secret to derive a set of keys
3. Data transfer — break up data to be transferred into a series of records
4. Connection closure — special messages to securely close connection

Splitting into Records

- If we used streams, no message integrity until completed transfer
- With records, we are susceptible to replay attacks
- to prevent that, we use a sequence number in our hash
- attacker could still replay a whole connection
- to prevent, we use a nonce for each connection lifetime
- Attacker could close the connection before one side knows
- to prevent, add a type to the hash

8.7 Network Layer Security: IPsec

What is network layer confidentiality?

- Sender encrypts all network layer payload, IP payload would be hidden
- Payload hidden from 3rd party sniffing
- Said to provide "blanket coverage"

IPsec provides confidentiality, auth, integrity, and replay-attack prevention

Transport v Tunnel

- Transport mode:
  - provides a secure connection between two endpoints as it encapsulates IP's payload (only encrypts payload)
- Tunneling mode:
  - encapsulates entire IP packet to provide a virtual "secure hop" between two gateways

Security Associations & their Databases

Security Association — simplex, info is housed at the receiver. Includes:

- 32 bit SA id — Security Parameter Index (SPI)
- SA origin — IP addr
- SA dest — IP addr
- Encryption type
- Encryption key
- Type of Integrity check
- auth key

SAD — Security Ass. Database, holds all that shit I just listed, key is the SPI

8.8 Securing Wireless LANs

8.9 Operational Security: Firewall & IDS