Computer Networks

Sungchan Yi

February 2020

1 Introduction

1.1 What is the Internet?

1.2 Network Edge

1.3 Network Core

1.4 Internet Structure

1.5 Performance Metrics

1.5.1 Evaluation Metrics

- **Delay**: Packet delivering time from source to destination

- **Packet loss**: Ratio of lost packets to total sent packets[1]

    - If the queue is full, the arriving packets will be dropped

    - Lost packets may be re-transmitted by previous nodes, by source end system, or not at all

- **Throughput**: Amount of traffic delivered / unit time

    - Rate at which bits are transferred between source and destination

    - Can be measured instantaneously, or on average

    - *Bottleneck link*: The link on end-end path that constrains the throughput (usually the one with minimum capacity)

1.5.2 Four sources of delay

$$d_{nodal} = d_{proc} + d_{queue} + d_{trans} + d_{prop}$$

- Queueing Delay

    - Time waiting at output buffer for transmission

    - **Congestion** dependent

---

[1]PDR: Packet delivery ratio

- Transmission Delay

  - $d_{trans} = L/R$ where L: packet length (bits), R: link bandwidth (bps)

- Processing Delay

  - Bit error checking

  - Decision of output link

  - Typically takes less than a few milliseconds (hardware acceleration)

- Propagation Delay

  - $d_{prop} = d/s$ where d: length of physical link, s: signal speed

Queueing and transmission delay take up most of the delay.

1.5.3   More on Queueing Delay

$$\text{(Traffic Intensity)} = \frac{La}{R}$$

where R is the link bandwidth (bps) or transmission rate, L is the average packet length (bits), a is the average packet arrival rate. As the traffic intensity $\to 1$, the average queueing delay will grow without bound.

1.6   Protocol Stack

A communication protocol stack is composed of several **layers**. Each layer implements a service via its own internal actions, and by relying on services provided by the underlying layers.

Layering or **modularization** eases development, maintenance, and updating of the whole system. But this can be harmful in cases when a higher level layer needs information from the lower layers.[2]

1.6.1   Internet Protocol Stack

1. **Physical**: Bits on the wire

2. **Link**: Data transfer between neighboring network elements

3. **Network**: Routing of datagrams from source to destination

4. **Transport**: Process to process data transfer

5. **Session**: Synchronization, connection management, recovery of data exchange

6. **Presentation**: Allows applications to interpret the meaning of data

7. **Application**: Supporting network applications

---

[2]Consider a navigation system, which uses "physical" information like actual traffic, when choosing the fastest route between two places. But this "physical" information wouldn't normally be visible to other layers.

1.7 Network Security

The field of network security arises from these questions:

- How can bad guys attack our computer networks?

- How do we defend our networks against those attacks?

- How do we design architectures that are immune to attacks?

1.7.1 Forms of Attacks

- Malware

    - virus: A self-replicating infection by receiving or executing an object

    - worm: A self-replicating infection by passively receiving object that gets itself executed

    - spyware

    - ransomware

- Packet Sniffing: Promiscuous network interface reads/records all packets passing by

- Denial of Service: Attackers make resources unavailable by sending a huge amount of fake traffic

- Fake Addresses: Send packets with fake source address

- Fake Wi-Fi AP: Steal user's credentials using fake AP

1.8 History of the Internet

- Firstly developed as ARPAnet

- Internetworking architecture = autonomy + minimalism

- TCP/IP, WWW

2 Application Layer