Project Proposal

for M21.CS1.301 – Algorithm Analysis and Design

by Pratham Gupta (2020101080)

on 04/10/2021

Algorithmic Analysis of TCP/IP Network Model

Overview

The TCP/IP model is the default method of data communication on the Internet. It breaks messages into packets to avoid having to resend the entire message in case it encounters a problem during transmission. TCP/IP divides communication tasks into layers that keep the process standardized through a set of discretely defined protocols, without hardware and software providers doing the management themselves. The data packets must pass through four layers before they are received by the destination device, then TCP/IP goes through the layers in reverse order to reassemble the packets, i.e., put the message back into its original format.

The protocols followed in the network model layers are, in fact, defined abstractions of particular computational algorithms that are employed to achieve/secure their respective functionalities.

Objective

We aim to produce a *technical writing* based on extensive and intensive analysis of these algorithms, to develop a critical understanding of the TCP/IP model from the viewpoint of computational and algorithmic design.

Description

[Keywords highlighted]

The objective shall be realized following a layer-wise approach (Layer 1 onwards) to discuss the algorithmic design and implementation under the governing protocols that constitute the network model, which would include their time, space and optimality analysis.

1 - Network-access Layer

This layer corresponds to the combination of Data Link Layer and Physical Layer. It looks out for hardware addressing and the protocols present in this layer allows for the physical transmission of data. **Point-to-Point Protocol (PPP)** is a data link layer communication protocol between two routers, that provides connectivity to physical serial links (that are relatively slow). One way to improve performance over serial links is to use compression on the data sent over the line. **Data compression** provides a coding scheme at each end of a transmission link that allows characters to be removed from the frames of data at the sending side of the link and then replaced correctly at the receiving side. Because the condensed frames take up less bandwidth, we can transmit greater volumes at a time. It is implemented using the **PPP Compression Control Protocol (CCP)**, which is responsible for negotiating and managing the use of compression algorithms that perform the actual compression and decompression of data viz **Huffman codes.** (Later - discuss other

data compression algorithms in fields of audio, image processing that includes algorithms of **Discrete Cosine Transform** closely related to **Fast Fourier Transform**.)

II - Internet Layer

The network/internet layer is responsible for packet forwarding including routing through intermediate routers. It defines the protocols which are responsible for logical transmission of data over the entire network. Some of these protocols extensively employ **Shortest Path algorithms** that aim to find the optimal paths between the network nodes so that routing cost is minimized. **RIP (Routing Information Protocol)** and **OSPF (Open Shortest Path First) Protocol** are types of dynamic routing. Routing Information Protocol (RIP) is one of dynamic routing that uses the bellman-ford algorithm where this algorithm will search for the best path that traversed the network by leveraging the value of each link, so with the **Bellman-Ford algorithm** owned by RIP can optimize existing networks. OSPF(Open Shortest Path First) is a Link State Protocol and is a most famous protocol among the Interior Gateway Protocol (IGP) family, working group of IETF. When configured OSPF will listen to neighbours and gather all link state data available to build a **topology map** of all available paths in its network and then save the information in its topology database (its Link-State Database), using both **Greedy and Dynamic Programming**. OSPF has capability to calculate the best shortest path to each reachable subnet/network using an algorithm called SPF (Shortest Path First) also known as **Dijkstra algorithm**. (Later - discuss the computational complexity of traffic hijacking under Border Gateway Protocol (BGP) and Secure(S)-BGP, while the interception problem is solvable, under reasonable assumptions, in **polynomial time** for the type of attacks that are usually performed in BGP, it is **NP-hard** for S-BGP)

III - Transport layer

It is responsible for end-to-end communication and error-free delivery of data. It shields the upper-layer applications from the complexities of data. The main protocol at this layer, the **TCP** performs sequencing and segmentation of data. It also has acknowledgment feature and controls the flow of the data through **flow control** mechanism which ensure the sender is not overwhelming the receiver with more data than it can handle. It also uses a network congestion-avoidance algorithm that includes various aspects of an **additive increase/multiplicative decrease (AIMD) scheme**, along with other schemes including slow start and congestion window, to achieve congestion avoidance. The TCP congestion-avoidance algorithm is the primary basis for congestion control in the Internet. (Later - additionally we might discuss some data flow/congestion management techniques like **max-flow algorithms**, and **leaky bucket**, **token bucket algorithms**.)

IV - Application layer

Comprised of the Application, Presentation and Session Layer, it is responsible for node-to-node communication and controls user-interface specifications While using a service from any server application, the client and server exchange a lot of information on the underlying intranet or Internet. Since, these information transactions are vulnerable to various attacks, a major role of the protocols at this layer is to ensure network security, which entails securing data against attacks while it is in transit on a network. Protocols like **SSH (Secure Shell) and SSL/TLS (Secure Sockets Layer/ Transport Layer Security)** are used as protection layers over protocols like the HTTP that employ encryption schemes like **RSA, ECC, 3DES, AES**. We do a detailed analysis of these symmetric, asymmetric and hybrid encryption algorithms.

Outline

~~Phase 1 *(Project Proposal – **2 weeks**)*~~ [DONE]

1. Developing a preliminary understanding of the TCP/IP model and its layers.
2. Researching the protocols associated with the layers and the underlying algorithms.
3. Project Proposal.

Phase 2 *(Algorithm Analysis – **4 weeks**)*

1. Understanding protocols, layer-wise, starting from the Network-Access Layer.
2. Analysis of respective algorithms in terms of implementation, costs and complexity.

Phase 3 *(More related algorithms - **2 weeks**)*

1. Discussion of past or alternate algorithms related to the model and their analysis.
2. Addressing problems and suggesting improvements wherever possible.
3. Miscellaneous discussions for unoptimized solutions/unresolved problems.

Phase 4 *(Project Submission – **2 week**)*

1. Compilation of the analysis information from all the layers.
2. Highlighting results, unresolved issues, problems for future research and/or new solutions(if any).
3. Formatting into a technical writing.
4. Project Submission.