Act 4.3 - Reflexión

Fernando Doddoli Lankenau - A00827038

Programación de Estructuras de Datos y Algoritmos Fundamentales

Grupo 14

Prof. Luis Humberto González Guerra

Octubre 21 2020

Una estructura de datos es una forma particular de organizar datos en una computadora para que puedan ser utilizados de manera eficiente. En esta reflexión analizaremos la importancia y eficiencia del uso del uso de grafos, un tipo de estructura de datos, para resolver un problema de la naturaleza de la actividad 4.3.

La implementación de un Grafo dirigido para resolver un problema de esta naturaleza es eficiente, dado que podemos almacenar los datos en una lista de adyacencia organizada por dirección de IP origen utilizando un unordered_map. De esta manera, podemos almacenar el IP de origen como el key value y su respectivo índice, referente a la lista de adyacencia, y outdegree en un pair como el map value del unordered_map. Todo esto es importante porque hace a nuestro programa muy eficiente ya que la complejidad de almacenar los datos en una lista de adyacencia es O(|V|+|E|)y la utilización de un unordered_map es O(1). Además, aparte de que utilizar un Grafo como estructura de datos es una estrategia eficiente para resolver problemas de esta naturaleza, hacer uso de un unordered_map, donde un pair es su map value que tiene como el número de out degrees su segundo valor, nos permite fácilmente determinar cuales IPs son los que están infectando la red.

Una forma de detectar cuales IPs son los que están infectando la red es analizar qué IPs tiene el mayor número de out degrees, es decir, cuales IPs son los que están apuntando a más IPs. Por ejemplo, un ataque cibernético DDoS, donde muchos bots viniendo de varios dispositivos conectados al internet hacen que los servidores de un producto o servicio dejen de funcionar correctamente a través de una avalancha de accesos, se puede detectar fácilmente a través de un Grafo dirigido almacenado en una lista de adyacencia gracias a que los nodos causando el ataque pueden ser identificados rápidamente. Esto es gracias a que si existe un ataque cibernético de bots, los accesos maliciosos serán los nodos que tengan el mayor número de out degrees, es decir, los que estén apuntando a los mayores números de nodos. Esto es importante porque significa que si queremos detectar qué IPs están atacando la red, lo podemos hacer de una manera rápida y eficiente con una complejidad O(n).