Instituto Tecnológico y de Estudios Superiores de Monterrey

Act 3.3 - Actividad Integral de BST: Reflexiones

Programación de estructuras de datos y algoritmos fundamentales (Gpo 570)

Integrantes:

Noreth Sofia Villalpando Saldaña A01368579

Héctor Calderón Reyes A01350637

Campus:

Toluca y Guadalajara

Profesores:

Dr. Eduardo Arturo Rodríguez Tello

Fecha de entrega:

23 de Julio de 2023

Reflexión Héctor Calderón:

Las estructuras de datos jerárquicas son de suma importancia en el desarrollo y optimización de soluciones informáticas. Los árboles binarios, heaps, y árboles de búsqueda son solo algunos ejemplos de estas estructuras jerárquicas. El uso de estas estructuras puede ayudar a mejorar la eficiencia de la ejecución del código, reducir la complejidad del tiempo y también puede hacer que el código sea más fácil de entender.(GeeksforGeeks, 2022)

En la situación problema, se implementó un Heap para el ordenamiento de las direcciones IP basado en la frecuencia de apariciones en un registro de red. Los Heaps son árboles binarios especiales que mantienen una relación específica entre el nodo padre y los nodos hijos. En este caso, se usó un Max Heap, donde cada nodo padre es mayor que o igual a sus nodos hijos. Este tipo de estructura es especialmente útil para ordenar rápidamente datos o para obtener los valores más altos o más bajos de un conjunto de datos. (GeeksforGeeks, 2022)

Aplicado a nuestro problema, el uso del Heap permite ordenar de manera eficiente las direcciones IP por su frecuencia, permitiendo identificar rápidamente las direcciones IP que aparecen con más frecuencia en los registros, lo que puede ser un indicador de actividad sospechosa. Además, la complejidad de tiempo de un algoritmo de ordenamiento basado en Heap es de O(n log n), lo que es muy eficiente comparado con otros algoritmos de ordenamiento como Bubble Sort o Insertion Sort que tienen una complejidad de tiempo de O(n^2).

En términos de determinar si una red está infectada o no, podemos buscar ciertos patrones en los registros de red que son indicativos de actividad maliciosa. Por ejemplo, un gran volumen de solicitudes provenientes de una única dirección IP, especialmente si estas solicitudes son a múltiples direcciones IP o a puertos inusuales, puede indicar la presencia de un ataque de fuerza bruta o un escaneo de red realizado por un software malicioso. De la misma forma, un patrón de solicitudes fallidas seguidas de solicitudes exitosas puede indicar la presencia de un ataque de diccionario o un intento de inicio de sesión por fuerza bruta.

Al combinar la eficiencia de las estructuras de datos jerárquicas con un análisis detallado de los patrones de tráfico de red, podemos identificar rápidamente actividad sospechosa y tomar medidas para investigar y remediar cualquier potencial compromiso de la red.

Reflexión Noreth Villalpando:

Durante esta actividad integral, exploramos la aplicación de estructuras de datos jerárquicas, en específico el MaxHeap, para abordar el desafío de identificar los IPs que más accesos tuvieron en una red a partir de una extensa bitácora de registros. Al enfrentarnos a esta situación problema, nos dimos cuenta de la importancia crítica de seleccionar la estructura de datos adecuada, ya que esto determinaría en gran medida la eficiencia y precisión de nuestra actividad.

El uso de una estructura de datos jerárquica, como el MaxHeap, fue una opción acertada para nuestro propósito debido a su capacidad para organizar los datos de manera jerárquica, asegurando que el el IP con más accesos se encuentre siempre en la cima del árbol. Esto nos permitió optimizar la búsqueda y recuperación de información, ya que podíamos acceder rápidamente al nodo principal sin necesidad de recorrer toda la estructura, lo que aumentó significativamente la eficiencia del algoritmo. Al evaluar el rendimiento de nuestro algoritmo, notamos que el MaxHeap nos brindó un tiempo de ejecución razonable y una capacidad de respuesta óptima incluso con una gran cantidad de datos, pues tiene una complejidad de O(logn) que lo hace bastante eficiente.

La eficiencia en el uso de estructuras de datos jerárquicas es esencial en esta situación problema debido a la gran cantidad de datos que se deben analizar para determinar si una red está infectada. Con una estructura jerárquica, como el MaxHeap, se logra una búsqueda rápida y eficiente del IP más accesado, lo que facilita la detección de actividades inusuales y que podrían ser maliciosas. Además, estas estructuras optimizan las operaciones de inserción y extracción, permitiendo un procesamiento ágil y oportuno de la información (GeeksforGeeks, 2023).

Encontrar el IP más accesado es un proceso crucial para determinar si la red podría estar infectada, ya que las actividades de acceso inusualmente altas podrían indicar una actividad maliciosa. Además de identificar el IP más accesado utilizando estructuras de datos jerárquicas, se deben monitorear el tráfico de red, examinar las solicitudes de autenticación, analizar comunicaciones sospechosas y rastrear procesos en los sistemas en busca de actividad maliciosa (Sullivan, 2015).

Referencias

- GeeksforGeeks. (2022). Heap Data Structure. Recuperado el 22 de julio de 2023, de https://www.geeksforgeeks.org/heap-data-structure/

- GeeksforGeeks. (2022). Heap Sort. Recuperado el 22 de julio de 2023, de https://www.geeksforgeeks.org/heap-sort/

- GeeksforGeeks. (2023c). Applications Advantages and Disadvantages of HeAP. GeeksforGeeks. https://www.geeksforgeeks.org/applications-advantages-and-disadvantages-of-heap/

- Sullivan, P. (2015). Detección de anomalías en la red: la herramienta antimalware esencial. ComputerWeekly.es. https://www.computerweekly.com/es/consejo/Deteccion-de-anomalias-en-la-red-la-herramienta-antimalware-esencial
-