

Actividad individual: Act-Integradora-3 Estructura de datos jerárquica

ReflexActIntegradora3

Importancia y eficiencia del uso de BST

El uso de un árbol binario en este tipo de problemas tiene muchos beneficios, en especial un Binary Heap.

Un Binary Heap:

1) Es un árbol completo, esta propiedad de Binary Heap los hace adecuados para ser almacenados en una matriz.

2) Los padres siempre tiene más prioridad que los hijos.

En la actividad integradora primero tenemos un arreglo desordenado, para tener un Binary Heap lo tendremos que ordenar. Para esto se usó un Heap Sort, un algoritmo de ordenamiento con tiempo de ejecución de $O(n \log n)$.

Usando los números de la situación problema, son 16807 entradas, por lo que tardaría $O(16807 \cdot \log 16807)$.

$O(163,524)$

En caso de usar el Quick Sort el caso promedio sería el mismo, pero en el peor caso sería $O(n^2)$ que en el caso de la situación problema sería 2.8×10^8 .

Como se puede ver este es mucho más rápido.

Esta estructura nos permite tener una fila prioritaria donde siempre tenemos al elemento de más entradas hasta arriba y nos permite tener las operaciones:

insert(), delete() and extractmax(), decreaseKey() en $O(\log n)$.

Sabiendo que son entradas de diferentes IPs es claro que la inserción será constante es importante tener un tiempo bajo de ejecución.

¿Cómo podrías determinar si una red está infectada o no?

Me parece que se podría determinar si una red está infectada dependiendo de la cantidad de intentos a una IPs en una cantidad de tiempo muy corta. Esto podría decir que hay algún tipo de malware que está intentando perjudicar la red. En este caso las 5 IPs con más entradas son:

Cantidad IP

38 10.15.187.246:5268

38 10.15.176.241:6550

37 10.15.183.241:5300

37 10.15.177.224:4253

37 10.15.176.230:6804

Treinta y ocho y treinta y siete entradas podrían parecer como bastantes, pero me parece que es importante los tiempos de estos intentos. Treinta y ocho intentos en un periodo largo podrían ser totalmente normal en un IP, además de ver cuál es la razón.

Para este ejemplo en particular tenemos 38 intentos diferentes en un margen de 5 meses, esto haría un promedio de 7.6 intentos por mes y con 5 diferentes razones de fallas. Debido a lo anterior no me parece la red este infectada. Si realmente estuviera infectada habría muchos más intentos en la cantidad de tiempo. 7 fallas por mes me parece que es un numero extremadamente y fácilmente podría ser por otras condiciones.

Otra forma de detectar si un IP está infectado es observar algún tipo de patrón, dentro del IP con más accesos no parece haber ningún patrón, los días de entrada cambian, el mes igual. Todo parece ser totalmente aleatorio lo que aumenta mi seguridad en la hipótesis de que ese IP no está infectado.