Tecnológico de Monterrey

Programación de estructuras de datos y algoritmos fundamentales (Gpo 602)

Act 4.3 - Actividad Integral de Grafos (Evidencia Competencia) investigación y reflexión de la importancia y eficiencia del uso grafos en una situación problema de esta naturaleza

Fecha
21/11/2025

Profesor
Daniel Perez Rojas

Alumno
Santiago Amir Rodríguez González A01739942

Las bitácoras de red documentan el comportamiento interno de un sistema: conexiones establecidas, solicitudes rechazadas, procesos iniciados, fallas, autenticaciones y rutas de comunicación. En organizaciones con infraestructura distribuida, estos registros pueden acumularse a un ritmo difícil de procesar manualmente. El reto no es solo almacenar la información, sino interpretarla con precisión y en tiempos razonables. En este contexto, los grafos se han posicionado como una herramienta clave para analizar relaciones dentro de grandes volúmenes de datos.

A diferencia de estructuras tradicionales como listas o arreglos, un grafo describe conexiones. Cuando cada dirección IP, servidor, servicio o usuario se representa como un nodo, y cada interacción como una arista, las bitácoras dejan de ser una secuencia cronológica y se convierten en una red de relaciones. Esto permite identificar rutas frecuentes, comunicaciones inesperadas, concentraciones de actividad o flujos dirigidos hacia un mismo destino—indicios relevantes en mantenimiento y ciberseguridad.

Además, los grafos permiten aplicar algoritmos clásicos que revelan comportamientos importantes. Por ejemplo, el cálculo de centralidad puede mostrar dispositivos críticos, mientras que algoritmos de detección de comunidades pueden identificar agrupamientos de hosts que comparten patrones. Estas técnicas agilizan el reconocimiento de patrones sin procesar línea por línea, y proporcionan información útil para auditorías, prevención de ataques o diagnóstico de fallas.

La eficiencia también es determinante. La combinación de grafos con estructuras como tablas hash permite crear, consultar y actualizar nodos en tiempos cercanos a O(1), lo cual es indispensable para sistemas que reciben miles de eventos por segundo. Esta capacidad de respuesta es indispensable en plataformas de monitoreo continuo, donde un retraso en el análisis puede implicar pérdida de servicio o exposición a riesgos.

Finalmente, el valor de los grafos no se limita al análisis técnico. Su representación visual facilita la comunicación entre administradores, analistas, desarrolladores o equipos de seguridad. Un diagrama de nodos y conexiones puede explicar en segundos lo que una bitácora tardaría miles de líneas en mostrar.

En síntesis, los grafos permiten transformar registros extensos en conocimiento estructurado, mejoran la eficiencia del análisis y ofrecen una representación fiel del comportamiento real de la red. Por ello, su uso se ha extendido en sistemas de monitoreo, prevención de amenazas y administración de infraestructura moderna.

Reflexión personal

Antes de trabajar con grafos, una bitácora parecía simplemente un conjunto enorme de mensajes sin conexión aparente. Sin embargo, al organizar esa misma información como nodos y relaciones, el archivo adquiere una estructura lógica y comprensible. Esta

transformación evidencia que, detrás de cada línea registrada, existe una historia de interacción dentro de la red.

Modelar bitácoras como grafos cambia la manera en que se piensa el análisis. En lugar de enfocarse en eventos aislados, se empieza a observar el sistema como un ecosistema interconectado. Esto permite identificar cuáles hosts tienen más interacción, qué redes generan mayor tráfico y cómo fluye la información dentro de la infraestructura. Esa perspectiva revela dinámicas que de otra forma pasarían desapercibidas.

También resulta sorprendente cómo los grafos permiten cuestionar ideas preconcebidas. A veces uno espera encontrar un único nodo dominante, pero el grafo puede mostrar una distribución equilibrada, indicando un sistema sano. En otras ocasiones, un nodo con muchas conexiones puede ser señal de mal funcionamiento o incluso actividad maliciosa. Esa capacidad para descubrir lo inesperado convierte al grafo en una herramienta valiosa.

El componente de eficiencia también deja una enseñanza importante. Si bien un análisis manual o lineal puede funcionar para archivos pequeños, deja de ser viable cuando el volumen crece. El uso de tablas hash, recorridos optimizados y estructuras dinámicas demuestra que la forma en que modelamos los datos influye directamente en nuestra capacidad para procesarlos. Comprender esto no solo mejora el análisis de bitácoras, sino la forma de abordar cualquier problema computacional.

Finalmente, trabajar con grafos recuerda que la informática no es solo código o datos: es la representación correcta del problema. Elegir la estructura adecuada puede simplificar lo complejo, acelerar lo lento y revelar lo oculto. En el análisis de bitácoras, esa diferencia puede ser crucial para mantener sistemas seguros, estables y confiables.

Referencias

- PyPro. (s. f.). *Grafos dirigidos y no dirigidos* [Curso online]. Recuperado de https://www.pypro.mx/app/curso/analisis-de-grafos-con-python-y-networkx/grafos-dirigidos-y-no-dirigidos
- Böhm, F., Menges, F., & Pernul, G. (2018). Graph-based visual analytics for cyber threat intelligence. *Cybersecurity, 1*, Article 16. https://doi.org/10.1186/s42400-018-0017-4