Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Vicepresidencia Primera del Gobierno · Ministerio de Asuntos Económicos y Transformación Digital · Secretaría de Estado de Digitalización e Inteligencia Artificial
Plan de Recuperación, Transformación y Resiliencia
España | digital 2026
incibe_ Instituto Nacional de Ciberseguridad

Alicia Mayor Bal
presenta el resumen del trabajo

A comparative study of network robustness measures

Jing LIU, Mingxing ZHOU, Shuai WANG, Penghui LIU
Front. Comput. Sci., 568-584, (2017).

12 de julio de 2024

SERIE DE RESÚMENES EN ESPAÑOL

Palabras clave: Algoritmo Hill Climbing, Ataques maliciosos, Medidas de robustez, Redes de escala libre.

Introducción

La robustez evalúa la capacidad de las redes a resistir fallos o ataques. Es una característica ampliamente estudiada en los últimos años debido a la aparición de muchos casos de fallos de redes causados por ataques en un número pequeño de sus nodos o enlaces. Estos **ataques** pueden ser aleatorios, atacando cada nodo o enlace con la misma probabilidad, o maliciosos, eliminando secuencialmente el nodo o enlace más importante en cada ataque hasta que solo quedan nodos aislados.

En este artículo el foco está sobre las **Redes de escala libre**, las cuales son robustas ante ataques aleatorios pero frágiles ante ataques maliciosos. Son generadas mediante el modelo Barabási-Albert, dando como resultado redes sin peso y no dirigidas.

Este trabajo tiene dos objetivos principales:

- **Evaluar la robustez de redes**: para lo cual, es necesario medir la sensibilidad de las medidas tanto en la red inicial como en la optimizada.
- **Guiar procesos de optimización para encontrar redes más robustas**: diferentes medidas de robustez pueden guiar este proceso, por lo que la red optimizada puede resultar robusta en términos de una medida pero frágil respecto a otras.

El algoritmo de **Hill Climbing** es utilizado para optimizar la robustez ajustando la topología de las redes iniciales, sin modificar el grado de distribución y la conectividad de cada nodo.

1. Marco uniforme para ataques maliciosos

Los estudios existentes sobre ataques maliciosos se centran con frecuencia en dos tipos de ataque:

- **Ataque adaptativo a nodos de alto grado(HDA)**: en cada paso el nodo con grado más alto es eliminado, recalculando de nuevo el grado para iniciar el paso siguiente.
- **Ataque de alta centralidad de intermediación a los enlaces (HBA)**: el enlace con mayor centralidad de intermediación es eliminado en cada paso. Puede ser adaptativo o no, al igual que los ataques de nodo.

Se puede generar un marco unificado para ataques maliciosos basado en la importancia tanto de nodos como de enlaces, como en el **Ataque adaptativo de alta importancia (HIA)**. En este tipo de ataques, se calcula en primer lugar la importancia de nodos y enlaces, eliminando el más importante de todos ellos. Una vez eliminado, se recalculan las importancias y se repite el proceso hasta que quedan solamente nodos aislados.

En este trabajo se consideran seis tipos de ataques, tanto a nodos como a enlaces, en base a tres medidas: el grado, la centralidad de intermediación y la centralidad de cercanía.

2. Medidas de robustez

2.1. Medidas basadas en conectividad

La **conectividad de enlaces** v(G) y la **conectividad de nodos** w(G) miden el número mínimo de enlaces y nodos, respectivamente, que es necesario eliminar de un grafo conexo para que deje de serlo. Cuanto mayor sea su valor, más robusta es la red. Sin

embargo, ambas medidas son menores que el mínimo grado de nodos en la red, por lo que es un valor que no puede ser cambiado demasiado mediante métodos de optimización sin cambiar la distribución de grado o el grado de los nodos.

2.2. Medidas basadas en la teoría de grafos aleatorios

La **fracción de eliminación crítica de enlaces** es una medida estadística para la desintegración de redes, la cual suele medirse en términos de rendimiento. Esta medida caracteriza la robustez estructural de las redes.

Esta fracción puede ser aplicada tanto a ataques aleatorios (p_c^r) como a ataques dirigidos (p_c^t) y, cuanto más alto sea su valor, mayor robustez implica.

2.3. Medida R y sus extensiones

R es una medida única de robustez que considera el tamaño de la mayor componente conexa frente a ataques secuenciales.

Existen diferentes extensiones de esta medida como la R_l, que toma de base R pero la aplica a ataques de enlaces en vez de a nodos o la medida $IntE$, que se centra en la eficiencia de la comunicación después de cada ataque. Cuanto mayor es este valor de eficiencia, más robusta es la red.

2.4. Medidas basadas en autovalores

Destacan dos medidas basadas en autovalores:

- **Conectividad algebráica** ($\alpha(G)$): basada en la matriz Laplaciana. Es el segundo autovalor más pequeño de la matriz Laplaciana. Es una medida que no consigue capturar características importantes de la robustez estructural.
- **Conectividad natural** ($\bar{\lambda}$): basada en el autovalor promedio de la matriz de adyacencia. Caracteriza la redundancia de rutas alternativas en una red cuantificando el número ponderado de caminos cerrados de todos los tamaños.

3. Sensibilidad de las medidas de robustez

De esperar que las medidas sean sensibles ante modificaciones en la red, de modo que si un enlace es añadido, la robustez debería incrementar o al menos no disminuir.

Se aplican cuatro estrategias de **selección de enlaces**: aleatoria (se seleccionan enlaces de forma aleatoria), rico-rico (se seleccionan enlaces de forma descendente según k_i x k_j, siendo k_i y k_j los grados de los nodos que unen los enlaces), pobre-pobre (igual a rico-rico pero ordenados de forma ascendente) y rico-pobre(se seleccionan enlaces de forma descendente según $|k_i - k_j|$).

Para los procesos de optimización se siguen los pasos:

1. Calcular robustez red original.
2. Seleccionar un enlace con una de las estrategias y recalcular la robustez.
3. Repetir paso 2 hasta añadir o eliminar número de enlaces deseados.
4. Repetir pasos 1-3 diez veces para calcular valores medios.

Siguiendo este procedimiento para cada estrategia, se generan gráficos de todas las medidas de robustez tanto para la red original como para cada una de las optimizaciones centradas en una medida cada vez.

4. Rendimiento de las medidas en la optimización

Una funcionalidad importante de las medidas de robustez es guiar el proceso de optimización para encontrar redes más robustas. Para esto, se estudia el rendimiento de las medidas en tres experimentos basados en:

- **Cambio de características de la red durante la optimización**: la longitud de camino más corto y la asortatividad son medidas capaces de reflejar la topología de una red, por lo que la relación entre cada una de ellas y el resto de medidas de robustez es calculada.
- **Robustez de redes optimizadas en términos de diferentes medidas**: se observa si redes robustas para una determinada medida mantienen su robustez con otras medidas.
- **Robustez de redes optimizadas contra ataques maliciosos**: se atacan las redes optimizadas, calculando a posteriori el mayor subgrafo conectado y la eficiencia de comunicación.

5. Conclusiones

Tras realizar análisis comparativos en las nuevas medidas de robustez, se observa que estas medidas muestran diferente sensibilidad a los cambios en la robustez; $v(G)$ y $w(G)$ prácticamente no reflejan estos cambios, mientras que el resto de medidas muestran los cambios con diferentes intensidades.

En las redes optimizadas se observa que la longitud promedio del camino más corto cambia mucho al optimizar R, $IntE$, $\alpha(G)$ y especialmente $\bar{\lambda}$. Además, la optimización de R, p_c^t y $\bar{\lambda}$ siempre causan un ligero aumento en la asortatividad.

A pesar de que al optimizar una medida el resto pueden verse afectadas negativamente, se ha observado

que si las medidas están correlacionadas entre sí, pueden ser optimizadas de forma conjunta.

6. Valoración del documento original

En este artículo se exponen de forma extensa y detallada las medidas de robustez que se analizan a lo largo de todas las secciones, lo que sienta las bases para entender posteriormente los análisis comparativos llevados a cabo entre ellas.

Un recurso muy utilizado son las gráficas, haciendo que, a pesar de ser un artículo más extenso que otros, su lectura se haga amena.