



Alicia Mayor Bal

presenta el resumen del trabajo

## On dynamic network security:

### A random decentering algorithm on graphs

M. T. Trobajo, J. Cifuentes-Rodríguez, M. V. Carriegos

Open Math, 2018; 16: 656-668.

15 de abril de 2024

## SERIE DE RESÚMENES EN ESPAÑOL

**Palabras clave:** Algoritmos, Análisis de redes, Centralidad, Ciberseguridad, Grafos de escala libre.

## Introducción

El campo de investigación del análisis de redes se ve relacionado hoy en día con multitud de áreas científicas entre las que se encuentra la ciberseguridad.

Además de las redes cuyos nodos son objetos físicos reales, existen **redes tecnológicas** en las que los nodos pueden ser ordenadores, máquinas virtuales o clientes de email entre otros, y las aristas representan el intercambio de datos entre ellos. Dentro de estas redes se producen **brechas de seguridad** que pueden ser de identidad, de enlace o de contenido, dependiendo de qué elemento de la comunicación se ve expuesto.

Estas brechas implican diferentes retos que pueden ser abordados desde el campo de las redes complejas:

- Modelar el conocimiento y capacidad del ciberatacante a la hora de explotar un grafo mediante su estructura topológica.
- Cuantificar la información en base a diferentes medidas de los grafos.
- Definir algoritmos de modificación de grafos para equilibrar la privacidad.
- Modelar el comportamiento de los participantes de una red colaborativa en entornos tecnológicos.

Desafortunadamente, cada tipo de ataque necesita una técnica o combinación de técnicas diferente, por lo que no se puede encontrar una solución óptima para cualquier situación. Este artículo se focaliza en las propiedades topológicas relacionadas con la **centralidad de la red**, concepto que puede asociarse con la capacidad de compartir información de forma segura. Cuando el flujo de información se centra en unos pocos nodos (hubs), la red es más vulnerable frente a ataques maliciosos dirigidos. El objetivo de este

trabajo es esconder la estructura central de la red haciendo uso de nodos auxiliares para hacerla menos vulnerable.

## 1. Metodología

Las redes con las que se trabaja en este estudio se rigen por las siguientes suposiciones:

- Los nodos son dispositivos computacionales conectados y sólo se consideran conectados en la red si hay intercambio de información entre ellos.
- Los grafos son no dirigidos y no ponderados.
- No existen nodos aislados ni bucles.

Se trabaja con **extensiones dinámicas** en las redes, añadiendo nodos auxiliares, lo cual resulta barato y posible en entornos virtuales. Es necesario tener en cuenta que esta operación puede alterar propiedades topológicas de la red. Una extensión dinámica de un grafo  $G$  resultará en un nuevo grafo cuyo número de nodos y aristas será igual o mayor al original.

Para conseguir esto, se propone un **algoritmo de descentrado dinámico aleatorio (RDA)**, que sigue los principios:

- Coste mínimo. Se añade un solo nodo auxiliar en cada paso.
- Preservación de propiedades topológicas, en particular se mantiene invariante su conectividad o densidad.
- Reducción de centralidad y centralización.
- Protección del algoritmo, no reversible mediante aleatorización.

Siendo  $A$  la matriz de adyacencia del grafo original  $G=(V,E)$ , con  $n=\#V$  el tamaño de  $A$ ,  $m=\frac{1}{2} \|A\|_1$  el

número de aristas y  $p$  la proporción de nodos auxiliares a añadir; se obtiene una sucesión de extensiones dinámicas partiendo de  $G$ . Siguiendo los principios anteriores se obtienen los parámetros en cada paso  $t$ :

- Número de nodos añadidos para una extensión:

$$n(t) = n(0) + t \quad (1)$$

- Número de aristas añadidas para una extensión:

$$\Delta m(t) = \frac{2m(0)(n(0) + t - 1)}{n(0)(n(0) - 1)} \quad (2)$$

- Probabilidad de enlace de un nuevo nodo auxiliar a otro nodo  $i$ :

$$p_i = \frac{\frac{1}{d_i}}{\sum_j \frac{1}{d_j}} \quad i = 1, 2, \dots, n(t-1) \quad (3)$$

## 2. Experimentos

Se llevan a cabo extensiones dinámicas sobre redes simuladas y se analizan cambios en centralidad y centralización. Los experimentos son realizados sobre datos simulados que modelan redes de datos tecnológicos.

Existen diferentes modelos para generar redes de mundo real\*, entre los que se encuentran:

- **Redes aleatorias:** caracterizadas por nodos con mismo grado aproximadamente y bajo nivel de centralización. Son robustas ante ataques específicos pero vulnerables ante ataques aleatorios.
- **Redes de escala libre:** caracterizadas por unos pocos nodos con gran número de conexiones, teniendo la mayoría de ellos bajo grado.

Los datos de estudio fueron generados por simulación mediante el algoritmo BA de generación de redes con un modelo de escala libre con Matlab. Estas redes se caracterizan por contar con diferente tamaño pero conservar una densidad similar. Se aplica entonces el algoritmo de descentralización para obtener las redes extendidas, con parámetros de densidad similar en torno a 0.1 y con una proporción  $p=1$  de nodos auxiliares. Se mide el índice de grado de centralidad de cada nodo para todas las redes, tanto originales como extendidas, y se representan gráficas del grado de distribución para instantes desde el 0% al 100% de nodos añadidos. Las redes originales se generaron con diferentes número de nodos, siendo estos: 40, 80, 100, 150, 200 y 250.

## 3. Resultados

Haciendo una comparación de la distribución del grado, se observa que las redes originales presentan formas de decrecimiento exponencial, mientras que las redes extendidas tienden a converger en formas de

campana, típicas de redes aleatorias que son más robustas a ataques dirigidos.

Las medidas de centralidad, tras ser normalizadas, eliminan el efecto que puede tener el tamaño de la red sobre ellas, dejando ver que la centralización disminuye a medida que  $t$  aumenta.

Debido a que las redes originales son generadas aleatoriamente con el algoritmo BA, sus valores de **centralización** y **cercanía** son similares a las extendidas. Sin embargo, el valor de **intermediación** tiende a disminuir a medida que aumenta el tamaño de las redes extendidas.

Analizando las variaciones de las medidas de centralidad en función de  $t$  se observa que **RDA obtiene valores significativamente menores de índices de centralización** en todos los casos. A modo general, las centralidades de cercanía y intermediación de la red tienden a disminuir más rápidamente para redes originales con un tamaño mayor, mientras que la centralidad de la red no. Además, RDA muestra mayor variación de valores relativos de la centralidad de intermediación. La variación más grande se da con el 100% de nodos auxiliares añadidos.

## 4. Discusión/Conclusiones

El algoritmo propuesto en este estudio se encarga de modificar redes añadiendo nodos auxiliares, consiguiendo con eso superar los retos explicados en la introducción.

Por un lado, se disminuyen los valores de centralización de las redes, ofreciendo así protección sobre redes de comunicación vulnerables a ataques dirigidos. Además, el algoritmo mejora la privacidad de los nodos, escondiendo los nodos principales con nuevos nodos auxiliares.

Finalmente, cabe destacar que esta solución es fácilmente implementable sobre máquinas virtuales en la nube, lo que puede suponer un avance en la protección de redes, protegiendo el intercambio de información y escondiendo su estructura real con bajo coste.

## 5. Valoración del documento original

Este artículo proporciona una solución a un problema de seguridad en redes, desgranando los retos derivados del mismo, y propone de forma sencilla un algoritmo para su respectiva solución. Se explican de forma clara todos los conceptos que son necesarios para el posterior entendimiento de la metodología y los resultados, los cuales se exponen de forma bien categorizada y con gráficas que dejan ver de forma directa los resultados obtenidos.

\* Real World Networks