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

M.V. Carriegos
presenta el resumen del trabajo

Dynamical Immunization of Data Network Controllability Processes Against Centrality Attacks on Temporal Networks.

P. Arebi
Research Square (2024).
22 de marzo de 2024

SERIE DE RESÚMENES EN ESPAÑOL

Palabras clave: Lista de cuatro a ocho términos clave relacionados con el contenido del artículo en orden alfabético.

Introducción

El problema que aborda el trabajo es la protección de la controlabilidad de una red frente a ataques basados en la centralidad de una red dinámica (es decir, cuyas conexiones varían con el tiempo). Se introducen los principales tipos de ataques a la controlabilidad de redes temporales (dinámicas) y se proponen métodos para restaurar la controlabilidad de las redes basados en la introducción de nodos y en la introducción de aristas. Los métodos de introducción de nodos presentan mejoras frente a otros métodos basados en la introducción de capas. Quizá las contribuciones más significativas del artículo sean: la definición de lo que son ataques externos a la controlabilidad de redes temporales (dinámicas), la definición de las estrategias de ataque basadas en la centralidad de la redtemporal (grafo), proponer un método de adición de un número mínimo de nodos (vértices) y enlaces (aristas) para restaurar la controlabilidad de la red temporal.

1. Redes temporales

Una red temporal T se define como un conjunto finito de nodos $V = \{v_1, v_2, \ldots, v_n\}$ conectados por un conjunto de enlaces $E = \{\varepsilon_{ij}(t)\}$ donde $\varepsilon_{ij}(t) = w$ es el peso del enlace entre los nodos v_i y v_j en tiempo t. Los enlaces $\varepsilon_{ij}(t)$ y $\varepsilon_{kl}(\tau)$ se dice que son sucesivos si $j = k$ y $\tau = t + 1$.

Desde el punto de vista de la teoría de control de sistemas lineales una red temporal es un sistema lineal de eventos discretos

$$x(t+1) = A(t)x(t) + B(t)d(t)$$

donde $x(t) \in \mathbf{R}^n$ es el vector de estados de los nodos v_i en tiempo t y $A(t)$ es la matriz de adyacencia del digrafo de enlaces subyacente en tiempo t. Las entradas de la matriz son los pesos de los enlaces en tiempo t. El vector $d(t) \in \mathbf{R}^{N_d(t)}$ es el vector de estados de los nodos conductores en tiempo t. Se permite que el número de nodos conductores cambie con el tiempo. Finalmente $B(t)$ es la matriz de impulsos del sistema. Así, una red temporal es controlable en tiempo t_f si es controlable como sistema lineal; es decir si la red puede pasar de un estado inicial $x_0(t_0)$ al estado final que queremos $x_f(t_f)$ en $t_f - t_0$ pasos. La meta al controlar una red temporal es encontrar el número mínimo de nodos conductores (MDS) para que la red sea completamente controlable.

2. Ataques por centralidad a redes temporales

Quizá los ataques a redes temporales mas importantes sean los *ataques en cascada* basados en que el fallo de un nodo de la red temporal lleva a una cascada de fallos sucesivos en los demás nodos. Los ataques en cascada pueden ser de dos tipos: aleatorios e inteligentes.

Los ataques aleatorios ocurren cuando eventos accidentales modifican los enlaces o los estados de los nodos de la red. Estos atques son raros. Mas importantes son los ataques inteligentes, que están orientados a modificar las redes a voluntad y se basan en explotar características de la red como pueden ser el grado, la centralidad y otros. Generalmente se atacan los nodos mas influyentes de la red.

Las principales características de la red son: la centralidad de los nodos, la centralidad intermedia de los nodos (*betweenness centrality*), la centralidad por cercanía de los nodos; y en cuanto a los enlaces se tiene, el grado de centralidad de un enlace y el grado de centralidad intermedia de un enlace.

Se proponen diversas estrategias de atque para su

análisis, basadas principalmente en la anulación de nodos en una proporción variable, que es un hiperparámetro del ataque. Se considera también que la elección de esa proporción de nodos anulados por el ataque pueda ser aleatoria o guiada por parámetros de centralidad de la red.

3. Estrategias de recuperación de un ataque

Si una red temporal es totalmente controlable en tiempo t_f pero en algún tiempo posterior $T > t_f$ falla en ser totalmente controlable, bien por errores internos o por ataques inteligentes, una *estrategia de recuperación de controlabilidad* está dada por la adición de nuevos nodos o nuevos enlaces tales que la red temporal recupera su condición de controlabilidad en algún tiempo $t_d > T$.

Así, la principal estrategia de recuperación de controlabilidad en este trabajo es la adición de nuevos nodos y de nuevos enlaces.

Se proponen efectivamente dos algoritmos de recuperación: algoritmo 1 mediante adición de nuevos nodos, y algoritmo 2 mediante la adición de nuevos enlaces.

4. Evaluación de los algoritmos

El artículo evalúa la capacidad de los algoritmos propuestos sobre conjuntos de datos experimentales y sobre una red concreta con 407 nodos y 1022 enlaces en un conjunto temporal limitado $\{0, 1, \ldots, 20\}$. Los experimentos son iniciales pues fijan el hiperparámetro probabilidad de ataque; pero aún así muestran que los ataques de centralidad en esa red provocan que se necesite una mayor proporción de nuevos nodos para la recuperación.

5. Valoración del documento original

El documento presenta un experimento ilustrativo sobre ataques inteligentes sobre redes temporales. Para las propiedades dinámicas de las redes temporales, así como para las definiciaones formales de las que este artículo adolece, se aporta bibliografía sobre el tema.

Referencias

· P. Arebi, A. Fatemi, R. Ramezani, Event stream controllabillity on event-based complex networks *, Expert systems with applications,* , 213 (2023), 118886.
· F. Li, Improving the efficiency of network controllability processes on temporal networks *, J. King Saud Univ. Computer & Inform. Sci.* , 36 (2024), 101976.
· M.T. Trobajo, J. Cifuentes, M.V. Carriegos, On dynamic network security: a random decentering algorithm on graphs *, Open Mathematics* , 16 (2018), 656-668.