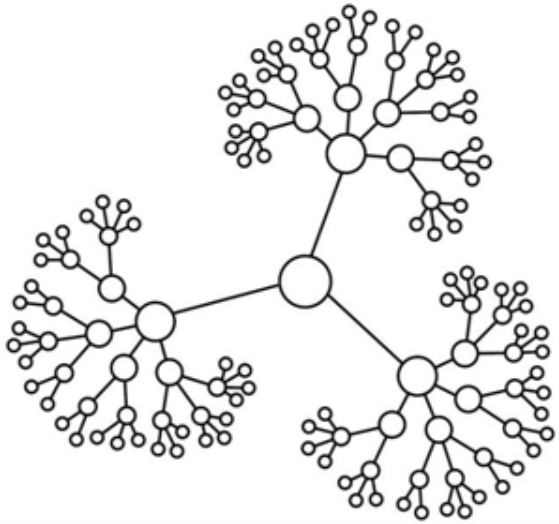
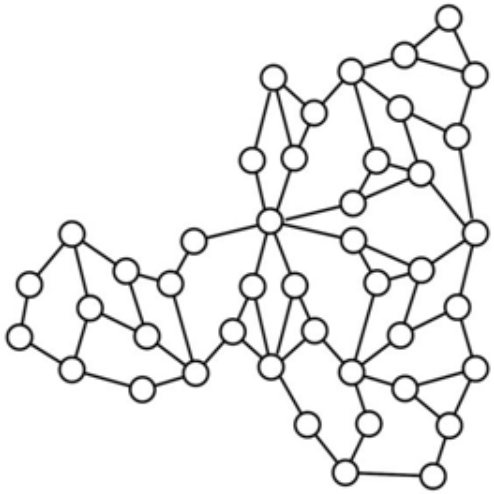
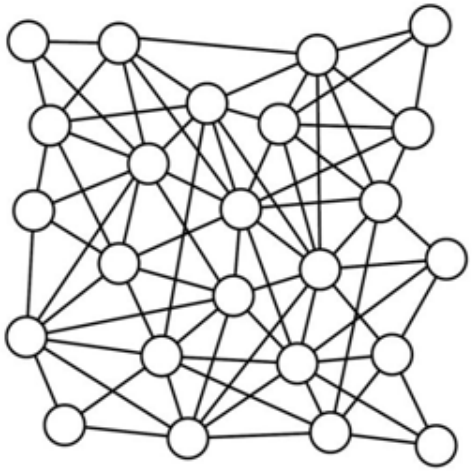
Análisis de Redes Complejas

Identificación y análisis de vulnerabilidades
en infraestructuras de hardware y software







Felipe Ramírez Herrera
Jefe, Unidad de Informática
Instituto Costarricense sobre Drogas

Temas de interés

- **CNA** – Complex Network Analysis
- **SNA** – Social Network Analysis
- **WCNA** – Weighted Complex Network Analysis
- **DNA** – Dynamic Network Analysis
- **GM** – Graph Mining
- **ML** – Machine Learning

Presentación

- Crecimiento constante en la complejidad e interconexión de las infraestructuras de energía, telecomunicaciones, transporte y financieras.
- El reto es de forma segura y confiable administrar y operar dichas infraestructuras.
- Es necesario modelar la infraestructura como un *sistema de sistemas* para conocer la amplitud del mismo y, por ende, determinar las principales vulnerabilidades.

Presentación

- Los problemas relacionados con inoperancia o desestabilización de un sistema de interacción complejo:
  - Situaciones emergentes por descuido, mediocridad o desconocimiento
  - Síndrome de la complejidad tecnológica
  - Sabotaje
  - Ataque cibernético / ataque físico de infraestructura crítica para un negocio, una comunidad o una nación

Presentación

- Desde el **Instituto Costarricense sobre Drogas (ICD)** se ha diseñado una metodología y una herramienta de software fundamentada en un campo científico relativamente nuevo, el análisis de redes complejas.
- Con el fin, de estudiar estructuras de crimen organizado, cibercrimen y modelar escenarios complejos para la toma de decisiones en materia de seguridad.

Límites de la ciencia

- Cottrel y Pettifor (2000) propusieron tres límites para la ciencia:
  - La ciencia de lo muy extenso (el estudio del universo).
  - La ciencia de lo muy pequeño (partículas elementales de la materia).
  - La ciencia de lo muy complejo (principios de ingeniería mediante ciencias sociales, psicología, biología, geología y economía).

Complejidad

- Bonacich y Lu (2012) definen complejidad de dos formas:
  - La forma *menos controversial*, es utilizado como sinónimo de emergencia, es decir, los conjuntos de actores que interactúan entre sí tienden a presentar propiedades a nivel macro que son *impredecibles*.
  - La forma *más controvertida* subraya la posibilidad de que existen *reglas* subyacentes y procesos que ocurren en todos los sistemas complejos, independiente de su contenido.

Contexto

- Los sistemas de software y hardware consisten en ***redes*** compuestas de múltiples entidades y relaciones, que difícilmente pueden ser controlados como una única entidad.
  - Las ***entidades*** pueden ser***:***
    - ***Software:*** paquetes, bibliotecas, archivos, clases, espacios de nombres y funciones.
    - ***Hardware:*** servidores, computadoras de escritorio, enrutadores, conmutadores y centrales de telefonía.
  - Las ***relaciones*** pueden codificar la estructura, como la contención física o determinación del alcance, y dependencias, tales como llamadas, usos, acceso a datos, líneas de comunicaciones, buses, cableado, entre otros.

Contexto

- La visualización de los datos y la estructura de interdependencia es una tarea desafiante y computacionalmente intensiva.
- Incluso los sistemas de tamaño moderado contienen miles de entidades y relaciones.
- Existen métodos de investigación para extraer datos de bases de código fuente y presentarla de manera que facilite la exploración y análisis.

Análisis de redes complejas

- Las redes son la base estructural de muchos fenómenos naturales, organizaciones y procesos sociales.
- Se sustenta en la premisa de que los actores individuales están conectados por relaciones complejas pero comprensibles en forma de red.
- Estas redes están en todas partes, con un orden subyacente y reglas simples (omnipresencia).
- Escenarios no determinísticos.

Análisis de redes complejas

- Creciente y acumulativo cuerpo de conocimientos.
- Método de investigación, inteligencia (seguridad nacional, criminal y militar).
- Referido a veces como análisis de vínculos o relaciones, análisis organizativo.
- Disciplina definida y formal para analizar la estructura de sistemas complejos.
- Forma **comprehensiva** y **paradigmática** a partir del estudio directo de la forma en que los patrones de vinculación asignan los recursos en un sistema.
- Aplicación integrada de conceptos teóricos, maneras de obtener y analizar los datos.

Ejemplos de fenómenos complejos

- Desestabilización de estructuras de crimen complejo: crimen organizado, trata de personas, lavado de activos y financiamiento al terrorismo, ciberterrorismo y cibercrimen.
- Análisis de adversario (militar) para la desestabilización de organizaciones militares, paramilitares y terrorismo internacional y doméstico.

Ejemplos de fenómenos complejos

- Comprensión de dinámicas sociales, estructuras formales e informales de poder e influencia.
- Detección de vulnerabilidades del negocio, por ejemplo, salud del conjunto de clientes y comprensión del ecosistema del negocio.
- Detección de vulnerabilidades de estructuras físicas o lógicas que interoperan (interactúan) entre sí (interdependencia).

Insuficiencia del análisis tradicional

- El abordaje metodológico basado estadísticas y probabilidades tiene un gravísimo inconveniente: se asume que las variables estudiadas poseen cierto nivel de **independencia**.
- Resulta insuficiente al estudiar fenómenos donde la cooperación e **interdependencia** son piezas claves para la comprensión del mismo.
- Evaluar el nivel de perturbación o desestabilización de todo un sistema complejo de interacción.

Desestabilización de las redes

- En un sistema complejo, la vulnerabilidad se determina en función de la desestabilización o perturbación que pueda sufrir un componente de la red que lo describe.
- Dos posibles escenarios o estados de desestabilización de una red:
  - No se puede difundir el conocimiento.
  - Pérdida de *eficiencia* y aumento de la *fragmentación*.

Metodología

1. Describir la estructura de la red, definir los actores o nodos y la vinculación entre cada uno de estos.
2. Identificar las características globales del sistema.
3. Identificar la importancia posicional de cada uno de los nodos de la red.
4. Simular la desestabilización del sistema mediante la supresión de uno o más nodos y la cuantificación del "daño" producido a la red en términos de fragmentación y reducción de la eficiencia.

Hitos

- *Visualización de* una infraestructura compleja de comunicaciones, servicios o interoperabilidad de aplicaciones.
- Detección de los *componentes clave* para la infraestructura.
- Cuantificación del *impacto* ante la pérdida de un componente de la red.

Aplicaciones

- Se ofrece un enfoque análisis alternativo para la vulnerabilidad estructural de sistemas complejos como aquellos que describen una infraestructura de comunicaciones o de servicios.
- Permite abordar el estudio de la dependencia de código, bibliotecas o aplicaciones en un entorno complejo de negocios.

Propuesta básica

- Se proponen las siguientes medidas básicas para el estudio de una red compleja:
  - Nivel global:
    - Eficiencia
    - Fragmentación
    - Distancia promedio
    - Centralización
  - Nivel local:
    - Grado
    - Cercanía
    - Intermediación
    - Eficiencia
    - Robustez estructural / espectral

Nivel global

- Describe la capacidad actual de la red.
- Conocer el entorno que puede ser vulnerado, atacado, intervenido o perturbado por un agente externo o interno.

Métricas

Medida	Fórmula
Fragmentación Proporción de nodos que no están directamente conectados	$F_G = 1 - 2 \times \sum_{u \in V} \sum_{v \in V} A_{u,v} \times \frac{1}{\lvert V \rvert \times (\lvert V \rvert - 1)}$
Distancia promedio Mayor dependencia en la comunicación o flujo de datos	$\overline{D}_G = \frac{1}{\frac{1}{2} \times \lvert V \rvert \times (\lvert V \rvert - 1)} \times \sum_{u \in V} \sum_{v \neq u \in V} d_{(u,v)}$
Eficiencia global Capacidad de intercambio de información y recursos	$E_g = \frac{1}{\lvert V \rvert \times (\lvert V \rvert - 1)} \times \sum_{(u,v) \in V^2} \frac{1}{d_{(u,v)}}$

Nivel local

- Uno de los análisis típicos en las redes sociales consiste en determinar quiénes son los **actores más importantes**.
- *No existe una única definición o indicador* para la importancia o prominencia.
- El estudio de la posición que cada uno de los actores ocupa en el conjunto de la red.
- Se hace habitualmente a través del análisis de la centralidad de los actores participantes en la misma.

Métricas

Medida	Fórmula
Grado Accesibilidad directa, actividad y visibilidad	$C_d(u) = \frac{k_u}{\lvert V\rvert - 1} = \frac{\sum_{v \in V} A_{u,v} + \sum_{v \in V} A_{v,u}}{\lvert V\rvert - 1}, u \in V$
Cercanía Importancia funcional, acceso indirecto a recursos.	$C_c(u) = \frac{\lvert V\rvert - 1}{\sum_{v \in V} d_{(u,v)}}, u \in V$
Intermediación Control del flujo, corretaje.	$C_b(u) = \frac{1}{(\lvert V\rvert - 1) \times (\lvert V\rvert - 2)} \times \sum_{s,t \in V} \frac{\sigma_{s,t}(u)}{\sigma_{s,t}}, u \in V$
Eficiencia local Capacidad de intercambio de información	$l_e(u) = \frac{1}{\lvert V\rvert - 1} \times \sum_{v \in V} \frac{1}{d_{u,v}}$

Métricas

Robustez estructural Resistencia a fallas aleatorias múltiples	$C^*(i) = \frac{1}{L_{ii}^{+}}, \forall i \in V$
Coeficiente de interconexión Pertenencia a grupos cohesivos	$B_c(u) = \frac{{k_u}^{-1}}{\sum_{v \in N_u} {k_v}^{-1}}$

Desde la perspectiva del cibercriminal

- Aprovechar los nodos con altos niveles de intermediación para la interrupción de toda la operación.
- Difundir u obtener datos desde los nodos con alta centralidad de grado.
- Atacar nodos con altos niveles de eficiencia local para reducir la eficiencia global.
- Incrustar código adicional en programas o servicios con alta centralidad de cercanía.

SICORE Metabase 11 R/2012

¡VEAMOS EL MODELO EN ACCIÓN!

Bibliografía

- ARQUILLA J., Ronfeldt D., ***Networks and Netwars: The Future of Terror, Crime, and Militancy***. Santa Mónica, California, EUA: RAND, MR-1382-OSD, 2001.
- ARQUILLA J., Ronfeldt D., ***The Advent of Netwar***. Santa Mónica, California, EUA: RAND, MR-789-OSD, 1996.
- BONACICH, P.; Lu, P. (2012), **Introduction to Mathematical Sociology**, Princeton University Press. Reino Unido.
- ESTRADA, E. (2012). **The Structure of complex networks**. Oxford University Press. New York, EUA.

Bibliografía

- Johansson, J., Jönsson, H., Johansson H., (2007), ***Analysing the Vulnerability of Electric Distribution Systems: A Step Towards Incorporating the Societal Consequences of Disruptions***, International Journal of Emergency Management, Vol. 4, No .1, pp. 4-17.
- Johansson, J., Jönsson, H., Johansson H., (2008). I***dentifyng Critical Components in technical Infraestructure Networks***, Journal of Risk and Reliability, Vol. 222, Part O, pp. 235-243.

Bibliografía

- NEWMAN, M. (2010). **Networks: An Introduction**. Oxford University Press. New York, EUA.
- SCOTT, J. (2000). **Social Network Analysis: A Handbook**, 2nd ed., Sage Publications, London, Reino Unido.
- WASSERMAN, S., Faust, K., (1994). **Social Network Analysis**, Cambridge University Press, Cambridge, Reino Unido.

Preguntas / comentarios