Universidad Nacional de Colombia

Matemáticas Discretas I

Proyecto Final: "DDoS: Detrás del Grafo"

María Catalina Rodríguez Cardona
Juan Diego Rozo Álvarez
Omar Alejandro Blanco Pineda

Programa de Ingeniería de Sistemas y Computación

Docente: Arles Ernesto Rodríguez Portela

Julio de 2025

Introducción 1

Desarrollo matemático 2

Aplicaciones lógica proposicional 4

Referencias 7

Introducción

Esta idea de proyecto final gira en torno a la simulación de una red de comunicación entre usuarios y servidores, modelada mediante un grafo bipartito no dirigido. El objetivo principal del mismo consistía en caracterizar el comportamiento de un ataque DDoS, aplicando las herramientas aportadas por las temáticas vistas en las clases de Matemáticas Discretas I a lo largo del semestre a un contexto relativo a la ciberseguridad.

Contemplando que en un ataque DDoS, múltiples usuarios generan grandes cantidades de solicitudes hacia uno o varios servidores a fin de sobrecargar e interrumpir el servicio del servidor, este fenómeno se puede modelar empleando grafos de manera efectiva: los usuarios y servidores se modelan como vértices, mientras que las conexiones entre ellos se representan con aristas que indican la intensidad del tráfico.

Asimismo, como se describirá más adelante, es posible hacer uso de la lógica proposicional para formular y evaluar reglas que ayuden a detectar comportamientos sospechosos, como la sobrecarga de un servidor o el patrón repetitivo de un usuario específico. Esto permite complementar el enfoque gráfico con mecanismos lógicos de inferencia.

El desarrollo teórico a continuación se enfoca en integrar estos conceptos para implementar este modelo capaz de representar y analizar, desde una perspectiva estructural y lógica, el fenómeno de los ataques de denegación de servicio (DDoS).

Desarrollo matemático

Inicialmente definimos nuestro grafo de forma convencional, esto es, definiendo un conjunto de vértices V, de aristas E y de pesos asociados a las aristas W tal que:

$$G = \{V, E, W\}$$

Cabe resaltar que V se encuentra dividido en dos subconjuntos, los cuales nos ayudan a mantener la correspondencia con la definición y estructura de grafo bipartito, tal como se aprecia en la Fig. 1.

$$V = \{U, S\}$$

$$U \cap S = \varnothing$$

Donde U es el conjunto de nodos usuario, y S el conjunto de nodos servidor.

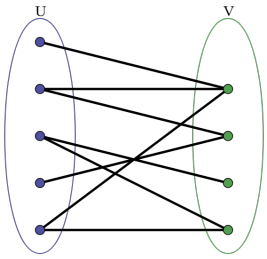

Figure 1: Grafo bipartito.

f es una función total que mapea a cada arista $e \in E$ con un elemento $w \in W$ el cual es el peso de esa arista.

$$f : E \to W \subset \mathbb{N}$$
$$e \mapsto w(e)$$

La definición de grafo bipartito nos indica que ningún vértice $u_1 \in U$ es adyacente a otro vértice $u_2 \in U$, un caso similar ocurre con los vértices $s \in S$

$$\nexists \{u, v\} \in E \text{ con } u, v \in U \quad \text{y} \quad \nexists \{u, v\} \in E \text{ con } u, v \in S.$$

El grado de un vértice $\delta(u) = p$, p representa con cuántos servidores se ha conectado un usuario. Similarmente, el grado de un vértice $\delta(s) = p$ representa la cantidad de usuarios que se han conectado a un servidor determinado.

Sean $X_s = \{e \in E \mid \exists u \in U \text{ tal que } (e, \{u, s\}) \in \Gamma\}$ un subconjunto de E tal que todas las aristas inciden en un nodo servidor particular. Si la sumatoria de los pesos de las aristas

que pertenecen a X_v supera un valor determinado, puede ser un indicativo de que un ataque DDoS está ocurriendo.

$$\sum_{e \in X_s} w(e) = L, \quad \text{donde } X_s \text{ es el conjunto de aristas incidentes a } s.$$

L es la métrica que se usa para medir si un servidor está bajo riesgo.
Similarmente

$$\sum_{e \in X_u} w(e) = L, \quad \text{donde } X_u \text{ es el conjunto de aristas incidentes a } u.$$

Si L es mayor a un valor determinado, esto representa un comportamiento anormal de parte de un usuario. esta sumatoria es la idea central detrás de la identificación de usuarios peligrosos y de servidores en riesgo en nuestro modelo.

Aplicaciones lógica proposicional

Además del aprovechamiento de lo aprendido respecto a la teoría de grafos, algunas de las temáticas vistas en Matemáticas Discretas I que también están estrechamente relacionadas con esta posible solución para la identificación de un posible ataque DDoS son aquellas relativas a la lógica proposicional.

Esto se debe a que es posible interpretar el filtro inicial de los patrones de tráfico inusuales mediante el planteamiento de enunciados que pueden ser evaluados con un valor de verdad.

Definición de proposiciones

Para analizar el comportamiento de los nodos y conexiones se pueden definir proposiciones como:

- p: "El servidor s_i está siendo sobrecargado."
- q: "El usuario u_i está involucrado en el ataque."

Esto permite aplicar operadores lógicos y herramientas como reglas de inferencia para relacionar a los actores involucrados en el análisis de un posible ataque.

Ejemplos con reglas de inferencia

Modus Tollens

$$\begin{array}{ll} & P \to Q \\ & \neg Q \\ \hline \therefore & \neg P \end{array}$$

Figure 2: Simbología modus tollens.

Proposiciones:

- p: "El usuario u_i está involucrado en un ataque DDoS."
- q: "El usuario u_i tiene una conexión con un servidor."

Premisas:

- $p \rightarrow q$: Si el usuario u_i está involucrado en un ataque, entonces tiene una conexión con un servidor.
- $\neg q$: El usuario u_i no tiene conexión con un servidor.

Conclusión:

$$\therefore \neg p \quad \text{(El usuario } u_i \text{ no está involucrado en un ataque)}$$

Modus Ponens

$$\begin{array}{l} p \\ \underline{p \rightarrow q} \\ \therefore q \end{array}$$

Figure 3: Simbología modus ponens.

Proposiciones:

- p: "Un usuario está posiblemente involucrado en un ataque DDoS."
- q: "El sistema ha lanzado una alerta."
- r: "El sistema realiza un análisis más detallado del tráfico."

Premisas:

- $(q \wedge r) \rightarrow p$: *"Si el sistema lanza una alerta y realiza un análisis del tráfico más detallado, un usuario está posiblemente realizando un ataque DDoS."*
- $q \wedge r$: *"El sistema ha lanzado una alerta y está realizando un análisis del tráfico más detallado"*

Conclusión:

$$\therefore p \quad \text{(Un usuario está posiblemente realizando un ataque DDoS)}$$

Anotación

Aunque la lógica proposicional es útil para diseñar sistemas de detección automática de amenazas, cuando se genera una alerta suele ser necesaria la intervención de un analista humano, ya que los datos pueden ser ambiguos o inciertos. En tales casos, se requiere lógica más sofisticada que va más allá del alcance de este proyecto.

Representación proposicional aplicada

En el código fuente, la función `obtener_max_conexiones_multiple` puede representarse lógicamente de la siguiente forma:

Dado un diccionario $D = \{(k_1, v_1), (k_2, v_2), \ldots, (k_n, v_n)\}$, donde k_i son claves y v_i sus respectivos valores:

1. Se define:
$$V_{\max} = \max(v_1, v_2, \ldots, v_n)$$

2. Se proponen las proposiciones:
   - $p(k_i, v_i)$: "El valor asociado a la clave k_i es v_i."
   - $q(k_i)$: "El valor asociado a k_i es igual a $V_{\max}$."
   - r: "Se agrega k_i a la lista $K_{\max}$ de claves con valor máximo."

3. Evaluación lógica:
$$(p(k_i, v_i) \land q(k_i)) \to r$$
   Si la conjunción es verdadera, se agrega k_i a $K_{\max}$; si es falsa, no se agrega.

Referencias

ISMS Forum. (s.f.). *Grupo de trabajo sobre inteligencia artificial – Documento técnico*.
Recuperado de: https://www.ismsforum.es/ficheros/descargas/isms-gt-ia-021707141605.pdf

Wikipedia. (s.f.). *Grafo bipartito*.
Recuperado de: https://es.wikipedia.org/wiki/Grafo_bipartito

Wikipedia. (s.f.). *Imagen: Modus ponendo ponens*.
Recuperado de: https://es.m.wikipedia.org/wiki/Archivo:Modus_ponendo_ponens.png

AcademiaLab. (s.f.). *Modus Tollens*.
Recuperado de: https://academia-lab.com/enciclopedia/modus-tollens/

Links del proyecto

Colab

https://colab.research.google.com/drive/1NeM45ThK89zHFiJ6_c4xOcf7VN5TKzCj?authuser=5

Repositorio en Github

https://github.com/jdrsajonia/discretas1_proyecto