Detección de ataques de Denegación de Servicio Distribuidos en redes de datos utilizando métodos de Deep Learning

Jorge Buzzio García
Universidad de Antioquia, Medellín, Colombia
Facultad de Ingeniería
jbuzzio410@gmail.com

***Abstract*—Este trabajo es la primera entrega del curso Deep Learning del semestre 2024-2. Consta de la creación de un modelo de Deep Learning para detectar ataques de Denegación de servicios distribuidos (DDoS). Para esto se usó el dataset CICDDoS2019, que contiene ataque DDoS.**

***Index Terms*—Redes neuronales, Ataque de denegación de servicios, Redes de datos, Ciberseguridad.**

I. Contexto

Dado el constante crecimiento de las redes de datos originado por la demanda de las personas de estar cada vez mas conectadas y a mayores velocidades, ha hecho que tecnologias como 5G, Internet de las cosas y la inteligencia artificial, se encuentren en consante evolución a pasos agigantados. En un mundo que cada vez es mas dependiente de la tecnología, es importante que la seguridad de la información como de los dispositivos sea cada vez mas robusta. Constantemente estamos expuestos a multiples tipos de ciberataques, del cual el que esta tomando mayor relevancia son los ataques de denegación de servicio.

Los ataques de denegación de servicio (DoS) y ataques de denegación de servicio distribuido (DDoS) son aquellos que buscan saturar los recursos de computo disponibles en un servicio, imposibilitando que usuarios legitimos puedan acceder a los servicios. Los ataques de denegación de servicio han ido en aumento en los ultimos años y esto se refleja en el reporte de la empresa Vercara, que afirma que hubo un incremento del 184% de DoS en la segunda mitad del 2024. Además de haber detectado alrededor de 10157 ataques DDoS en agosto del 2024, lo que significa para ellos un incremento del 56% en comparación con el mes de julio [1].

Es por este motivo que este trabajo del curso de Deep Learning es de detectar ataques DoS y DDoS utilizando modelos de Deep Learning utilizando datasets que describan un comportamiento anómalo en tráfico de redes de datos.

II. Objetivo

El principal objetivo de este trabajo es clasificar tráfico de red que represente los distintos tipos de DDoS y DoS. Esto se realizará a partir del entrenamiento de un modelo de deep learning que tenga como entrada trafico de red representado en una imagen, y en base a esto determinar de que tipo de ataque de denegación de servicio se trata.

Identify applicable funding agency here. If none, delete this.

III. Dataset

Para realizar este trabajo se tomó como referencia el dataset CICDDoS2019 [2]. Este dataset está etiquetado y cuenta con 80 caracteristicas de trafico de red las cuales se han extraido utilizando la herramienta CICFlowMeter. Este dataset contiene unformación para proponer los mejores conjuntos de características para detectar diferentes tipos de ataques DDoS, incluidos los DDoS reflexivos (como DNS, LDAP, MSSQL y TFTP), UDP, UDP-Lag y SYN. En este caso, el dataset CICDDoS2019 debe pasar por una transformación para convertirlo en imagenes png según el tipo de DDoS. Lo que se hizo primero fue dividir el dataset entre los registros etiquetados como DDoS y los etiquetados como normal. Este proceso se puede apreciar en la figura 1. Cabe resaltar que la cantidad de registros normal es mínimo en comparación con los etiquetados como DDoS.

A partir de la división de registros en base a la etiqueta (DNS, LDAP, MSSQL, TFTP, UDP, UDP-Lag, SYN y normal) se crearon imágenes de 60x60x3 que representa 3 (RGB) capas, cada una de 60x60. Para la etiqueta TFTP no se crearon imágenes ya que era un archivo muy pesado de mas de 9GB y la memoria RAM y no se tenía la memoria RAM disponible para esta operación. Después de la creación de las imágenes se obtuvo un dataset con 161989 imágenes etiquetadas. Se generó un archivo zip que contiene todas las imagenes comprimidas listas para ser llamadas y usadas, este archivo tiene un tamaño de 41.1MB. Este archivo se encuentra en el repositorio [6] . La distribución de las clases se visualiza en la tabla 1. Además se tiene el diagrama de barras de las clases en la figura 2.

IV. Métricas de desempeño

A. Métricas de Machine Learning

Al ser este un problema de clasificación las métricas mas utilizads son Accuracy, Precision, Recall, Factor 1 y la matriz de confusión.

Accuracy (Acc): Es la métrica más básica y mide el porcentaje de imágenes correctamente clasificadas sobre el total de predicciones.

Precision (Pr): Es el ratio de flujos de imágenes correctamente

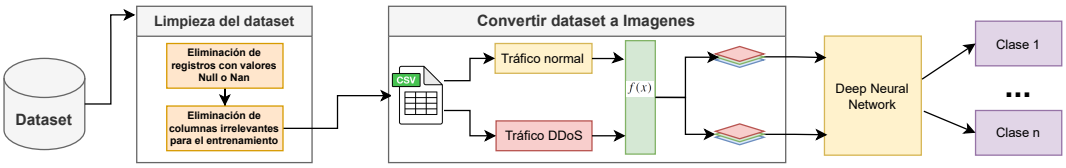

Fig. 1. Proceso de division y creación de imagenes del dataset CICDDoS2019.

TABLE I
DISTRIBUCIÓN DE IMÁGENES

Etiqueta	Cantidad de Imágenes
DrDoS_UDP	17188
DrDoS_SNMP	28607
UDPLag	1836
DrDoS_MSSQL	24422
normal	174
DrDoS_NTP	6642
Syn	7666
DrDoS_LDAP	11896
DrDoS_NetBIOS	22019
DrDoS_SSDP	14269
DrDoS_DNS	27270

clasificadas (TP), frente a todas las imágenes clasificadas (TP+FP).
Recall (Rc): Es el ratio de imágenes correctamente clasificadas (TP), frente a todas las imágenes clasificadas (TP+FN).
F1 Score: Es una combinación armónica de precisión y recall en una sola medida.

$$Acc = \frac{TruePositives + TrueNegatives}{TotalMuestras} \quad (1)$$

$$Rc = \frac{TruePositives}{TruePositives + FalseNegatives} \quad (2)$$

$$Pr = \frac{TruePositives}{TruePositives + FalsePositives} \quad (3)$$

$$F1 - score = 2 \times \frac{Pr \times Rc}{Pr + Rc} \quad (4)$$

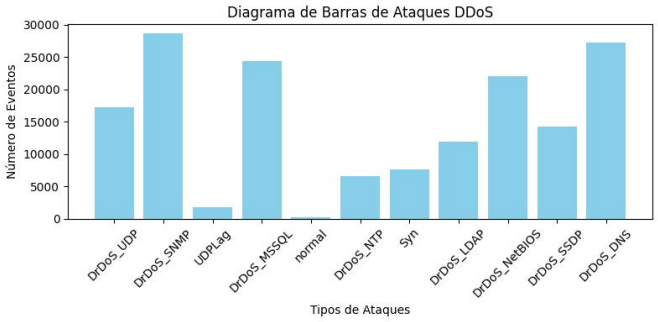

Fig. 2. Diagrama de barras de la distribución de imágenes.

B. Métricas del Negocio

Contar con un dataset mas pequeño como el que se ha generado de 41MB en comparación con el CICDDoS2019 que pesa 30GB podría hacer que el tiempo necesario para entrenar, evaluar, o desplegar un modelo de machine learning se reduzca significativamente. Esto mejora la velocidad de procesamiento, haciendo que el sistema de detección de ataques DDoS sea más eficiente.

V. REFERENCIAS Y RESULTADOS PREVIOS

El trabajo [4] propone el uso de una Red Neuronal Convolucional para detectar ataques distribuidos de denegación de servicio utilizando métricas de tráfico muestreadas de activos de red. El entrenamiento de la red propuesta se basa en imágenes usando una red neuronal convolucional. Logra porcentajes de acierto del 99%. Las imágenes se crearon a partir del dataset ICSXIDS2012. Al igual que el articulo anterior, [3] genera imagenes a partir de un dataset de ataques DDoS. En este caso hace uso del CICDDoS2019. Como modelo de deep learning utiliza la red ResNet, la cual da porcentajes de acierto de alrededor del 87%. En [5], los autores hacen uso de la herramienta netflow para capturar tráfico de red y apartir de este crear imagenes para entrenar una red neuronal convolucional. Los resultados obtenidos es un modelo con una precisión de 95%.

REFERENCES

[1] A. González, "Los ataques DDoS registran un aumento del 186% en la primera mitad de 2024," IT Digital Security, Sep. 20, 2024. [Online]. Available: https://www.itdigitalsecurity.es/endpoint/2024/09/los-ataques-ddos-registran-un-aumento-del-186-en-la-primera-mitad-de-2024. [Accessed: Sep. 28, 2024].

[2] I. Sharafaldin, A. H. Lashkari, S. Hakak and A. A. Ghorbani, ”Developing Realistic Distributed Denial of Service (DDoS) Attack Dataset and Taxonomy,” 2019 International Carnahan Conference on Security Technology (ICCST), Chennai, India, 2019, pp. 1-8, doi: 10.1109/CCST.2019.8888419.

[3] F. Hussain, S. G. Abbas, M. Husnain, U. U. Fayyaz, F. Shahzad and G. A. Shah, ”IoT DoS and DDoS Attack Detection using ResNet,” 2020 IEEE 23rd International Multitopic Conference (INMIC), Bahawalpur, Pakistan, 2020, pp. 1-6, doi: 10.1109/INMIC50486.2020.9318216.

[4] A. A. Freitas Junior, F. Lima Filho, A. Brito Júnior, and L. F. Silveira, ”Detecção de Ataques DDoS com Base em Métricas de Tráfego usando Redes Convolucionais,” in *Anais do XVI Congresso Brasileiro de Inteligência Computacional*, 2023.

[5] X. Liu, Z. Tang and B. Yang, ”Predicting Network Attacks with CNN by Constructing Images from NetFlow Data,” 2019 IEEE 5th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing, (HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS), Washington, DC, USA, 2019, pp. 61-66, doi: 10.1109/BigDataSecurity-HPSC-IDS.2019.00022.

[6] J. Buzzio, ”DeepLearning,” GitHub repository, 2024. [Online]. Available: https://github.com/jbuzzio/DeepLearning/tree/main. [Accessed: Sep. 28, 2024].