Colaboración Efectiva para Investigación Aplicada
2021-2025

Identificación de ataques DDoS y Ransomware e Identificación de Anomalías de BGP

Resumen de la investigación

En los últimos años hemos utilizado la Inteligencia Artificial (IA) para la detección y mitigación de ataques DDoS en redes definidas por software enfocándonos no sólo en DDoS de tasas altas, sino también en DDoS de tasas bajas (slow rate). Hemos creado datasets y utilizado datos públicos para entrenar modelos de aprendizaje automático (ML), aprendizaje profundo (DL) y aprendizaje por refuerzo (RL) a modo de lograr nuestros objetivos. Logramos desplegar estos modelos en entornos simulados haciendo uso de mininet y en entornos físicos para lograr la detección y/o mitigación. Adicionalmente, hemos realizado un trabajo similar para la identificación de ransomware entrenando modelos de IA y desplegando entornos simulados.

De igual manera, utilizamos la IA para la detección de anomalías en BGP, las cuales pueden ser producidas por ataques o configuraciones erróneas. Finalmente, desarrollamos un modelo híbrido para detectar las anomalías de BGP que hace uso de estadísticas con énfasis en la desviación absoluta de la media combinada con Inteligencia Artificial.

Dr. Jesús Arturo Pérez Díaz

Dr. Marcelo Yungaicela N.

Dr. José Antonio Cantoral

Dr. Cesar Vargas Rosales

Ing. Carlos Martínez Cagnazzo MSc. **(en curso)**

.

Antecedentes, problemática y relevancia del estudio

De acuerdo a la agencia de la Unión Europea para la Ciberseguridad ENISA, en su reporte *ENISA thead landscape 2023*, el ransomware es el ataque con mayor incidencia a nivel global, siendo superados en 2024 por los ataques DDoS (ENISA, 2023). Latinoamérica es la cuarta zona de mayor incidencia de estos ataques. Por lo tanto, detectar anomalías en BGP resulta particularmente relevante para la ciberseguridad, debido al papel crítico que desempeña este protocolo en la infraestructura de Internet. Las vulnerabilidades en BGP pueden provocar interrupciones importantes y fallos de conectividad, lo que resalta la necesidad de una detección temprana para mantener los servicios de Internet estables y seguros.

Metodología y diseño del estudio

Hemos creado datasets que posteriormente hemos hecho públicos, de igual forma indagamos los mejores datasets públicos para DDoS y ransomware, con el objetivo de que contribuyan a entrenar modelos para identificar y mitigar ataques DDoS y ransomware. Los modelos se han probado offline y posteriormente en despliegues SDN simulados o físicos. Los despliegues se han hecho en los planos de control y de datos de la SDN. Para la detección de anomalías de BGP, inicialmente diseñamos la técnica estadística de MAD, la cual luego fue mejorada con el uso de IA. Asimismo, todas las pruebas se realizaron con datasets de uso abierto de RIPE.

Gráficos, datos y principales resultados

En la detección de DDoS se alcanzaron precisiones del 99.97% (KNN) para la clasificación binaria y del 99.84% (LSTM) para la clasificación multiclase. En despliegues simulados se obtuvo una precisión *(accuracy)* promedio alrededor del 95% mientras que en entornos físicos entre 90 y 92%. La Figura 1 muestra la arquitectura SDN en despliegues simulados. Para la detección de anomalías los mejores modelos fueron XG Boost y Extra Trees que alcanzaron una precisión de 99% y 98% respectivamente. Adicionalmente, random forest presentó una precisión del 99% y 97% respectivamente. La Figura 2 muestra el periodo de la ocurrencia de la anomalía provocada por slammer y la detección lograda. *NOTA: La Figura 1 y 2 se encuentran en el idioma original en el cual fueron generadas originalmente en el marco de la investigación.*

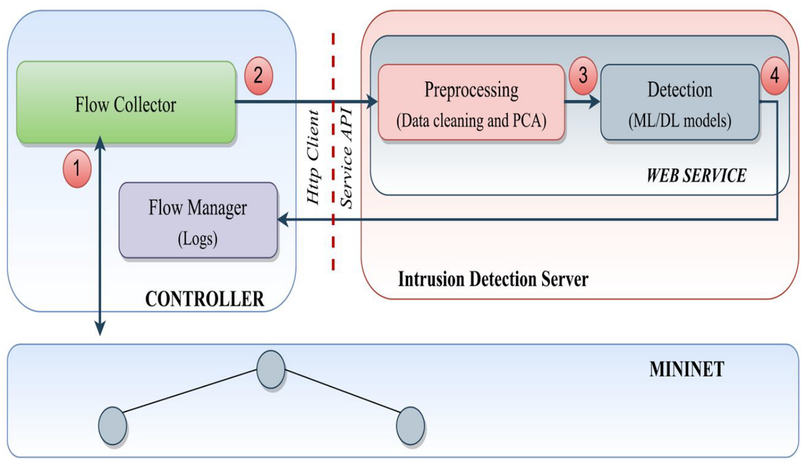

FIGURE 1. Proposed architecture for intelligent SDN-based DoS/DDoS attacks detection.

Potencial uso y aplicación de los resultados

El uso de un sistema de IA automático en la región de Latinoamérica puede ayudar a mejorar los servicios prestados por los proveedores de servicios de Internet y en la nube, ya que les ayudará a abordar potenciales reducciones en personal técnico especializado. Esto podría incidir en mitigar un porcentaje más alto de ataques DDoS y de ransomware, aumentando también su competitividad al no tener que realizar contrataciones adicionales de capital humano. El principal uso y beneficio está enfocado en las pequeñas y medianas empresas, las cuales muchas veces no cuentan con sistemas de seguridad robustos debido a un presupuesto limitado, lo que implica que podrían ser más susceptibles a los ciberataques. De igual manera, la detección temprana de anomalías de BGP podría ayudar a ISP, IXPs y proveedores para detectar oportunamente ataques o algunas otras problemáticas en la red (como errores de configuración, secuestro de rutas o apagones), derivados del ruteo con BGP.

Potenciales líneas de desarrollo futuro/recomendaciones y conclusiones

Principales conclusiones de la investigación:

• Los ataques DDoS de tasa baja son mucho más complejos de detectar que los DDoS de tasa alta.

• Los modelos de DL son ligeramente mejores para detectar DDoS y ransomware que los de ML, sin embargo, es necesario evaluar el costo computacional que esto implica.

• En despliegues físicos o simulados siempre decrece el nivel de precisión *(accuracy)* de los modelos de detección de DDoS o ransomware, por tratarse de tráfico diferente al que fue usado para entrenar los modelos. Por lo tanto, siempre se recomienda entrenar los modelos con tráfico de la red que puede defender o al menos incluir parte de dicho tráfico en el dataset.

• Los modelos híbridos que usan estadística e IA evidencian mejor desempeño para la detección de anomalías de BGP respecto al uso de una única técnica independiente.

Como línea de desarrollo continuaremos trabajando en la detección de ransomware y DDoS en combinación con empresas. Además, nos centraremos en la identificación de secuestro de rutas de BGP.

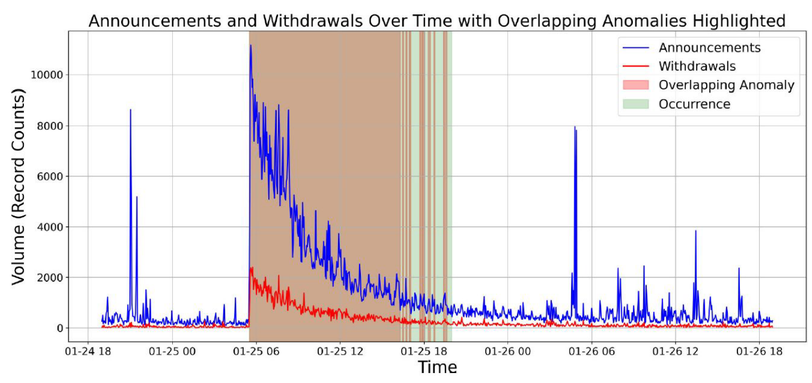

FIGURE 2. MAD anomaly detection system with dynamic threshold over Slammer Attack: visual representation of Announcements and Withdrawals volumes over time with anomalies marked in pink/brown and high-activity occurrence periods in green.

Afiliación

Instituto Tecnológico y de Estudios Superiores Monterrey (ITESM)

LACNIC

Contactos

jesus.arturo.perez@tec.mx

investigacionaplicada@lacnic.net

Reconocimientos

Agradecemos al Programa FRIDA por financiar parcial e inicialmente la investigación que dió origen a los resultados aquí presentados. Asimismo, esta investigación es parte de la colaboración desarrollada por LACNIC con grupos de investigación e instituciones académicas regionales en el marco del **Proyecto de Colaboración Efectiva para Investigación Aplicada (LACNIC)**, junto a las líneas e investigaciones desarrollados por el Instituto Tecnológico de Monterrey (México).

Agradecemos también a LACNIC por proporcionar apoyo en la formación y capacitación a los alumnos que realizaron las investigaciones y por brindar su apoyo técnico en las actividades de intercambio.

Citación de esta publicación

J. A. Pérez Díaz, M. Yungaicela N., J.A. Cantoral, C. Vargas Rosales, C. Martínez Cagnazzo. “Identificación de ataques DDoS y Ransomware e Identificación de Anomalías de BGP” [Presentación de póster]. Presentado en: LACNIC 44-LACNOG 2025, 6-10 de octubre de 2025, San Salvador, El Salvador.