Detección de Ataques en Redes IoT mediante Aprendizaje Automático usando el dataset CIC-BCCC-NRC TabularIoTAttack-2024

Juan Pablo González Blandón
Juan Carlos Murillo Florez
Juan José Balvin Torres

Noviembre 2025

Proyecto de Machine Learning aplicado a Ciberseguridad de Redes IoT

Universidad de Antioquia
Facultad de Ingeniería
Programa de Ingeniería Electrónica y Telecomunicaciones

Profesor: Jaime Alberto Vergara

Fecha: 17 de noviembre de 2025

Índice

1. Introducción

En la actualidad, el rápido crecimiento del Internet de las Cosas (IoT) ha impulsado la conectividad de millones de dispositivos en diversos entornos domésticos, industriales y urbanos. Sin embargo, este aumento en la superficie de exposición ha traído consigo nuevos desafíos de ciberseguridad, debido a las limitadas capacidades de procesamiento, almacenamiento y protección de los dispositivos IoT. Entre las principales amenazas se encuentran los ataques distribuidos de denegación de servicio (DDoS), ransomware, exfiltración de datos y accesos no autorizados, que comprometen la integridad, disponibilidad y confidencialidad de la red.

El presente trabajo tiene como propósito desarrollar un modelo de aprendizaje automático (Machine Learning) que permita detectar comportamientos maliciosos en el tráfico de red IoT, utilizando el conjunto de datos *CIC-BCCC-NRC TabularIoTAttack-2024*, publicado por el Canadian Institute for Cybersecurity (CIC). Este dataset contiene flujos de red con características ya extraídas y etiquetadas como benignas o maliciosas, lo cual facilita el entrenamiento de modelos supervisados para la identificación de ataques.

De esta manera, el trabajo busca contribuir al desarrollo de sistemas de detección de intrusiones (IDS) eficientes y adaptados al entorno IoT, promoviendo la seguridad y confiabilidad en redes compuestas por dispositivos inteligentes.

2. Objetivos

2.1. Objetivo general

Implementar y evaluar un modelo de aprendizaje automático capaz de identificar ataques en tráfico de red IoT utilizando el dataset *CIC-BCCC-NRC TabularIoTAttack-2024*, con el fin de mejorar la detección temprana de intrusiones en entornos de Internet de las Cosas.

2.2. Objetivos específicos

- **Analizar y Preprocesar** los datos del dataset *CIC-BCCC-NRC TabularIoTAttack-2024* mediante limpieza, normalización etc, con el objetivo de identificar sus principales variables, tipos de ataques y balance de clases,
- **Implementar y Comparar** distintos algoritmos de clasificación supervisada (como Random Forest, SVM, o redes neuronales), evaluando su desempeño con métricas como precisión, recall, F1-score y matriz de confusión.
- **Documentar y discutir** los hallazgos del estudio, destacando las fortalezas y limitaciones del modelo propuesto, así como posibles líneas de mejora futura.

3. Marco teórico

El Internet de las Cosas (IoT) se define como la interconexión de objetos físicos capaces de recopilar, procesar y transmitir información a través de redes digitales. Esta tecnología ha transformado sectores como la salud, la industria, la domótica y el transporte, pero también ha ampliado las vulnerabilidades en la infraestructura de red.

Para mitigar estos riesgos, se han desarrollado los sistemas de detección de intrusiones (IDS), los cuales pueden basarse en firmas o en comportamiento. Los modelos basados en comportamiento utilizan algoritmos de aprendizaje automático para reconocer patrones anómalos en el tráfico de red, lo que les permite identificar ataques previamente desconocidos.

El conjunto de datos *CIC-BCCC-NRC TabularIoTAttack-2024* es una fuente reciente diseñada específicamente para el entrenamiento de modelos IDS en entornos IoT. Este dataset contiene más de un millón de registros derivados de flujos de red generados en escenarios controlados, con ataques simulados y tráfico benigno real. Las características fueron extraídas mediante la herramienta *CICFlowMeter*, proporcionando un formato tabular que incluye atributos como duración del flujo, cantidad de bytes y paquetes, direcciones IP, protocolos y etiquetas de clase.

En el campo del aprendizaje automático, los modelos más utilizados para detección de intrusiones incluyen métodos supervisados como Árboles de Decisión, Random Forest, Support Vector Machines (SVM), K-Nearest Neighbors (KNN) y redes neuronales. Estos algoritmos son evaluados mediante métricas como la exactitud (accuracy), la tasa de verdaderos positivos (recall), la precisión (precision) y la puntuación F1, que permiten medir la efectividad de la detección.

El uso de datasets modernos como el TabularIoTAttack-2024 representa un avance frente a conjuntos tradicionales como UNSW-NB15 o CICIDS2017, ya que refleja mejor los patrones de tráfico y ataques propios del ecosistema IoT actual.

4. Referencias

- Canadian Institute for Cybersecurity. (2024). *CIC-BCCC-NRC TabularIoTAttack-2024 Dataset*. University of New Brunswick. Recuperado de: `https://www.unb.ca/cic/datasets/tabular-iot-attack-2024.html`
- Maji, S. (2023). *IDS-UNSW-NB15*. GitHub Repository. Recuperado de: `https://github.com/SubrataMaji/IDS-UNSW-NB15`