Deteción de anomalías en el tráfico de red en los dispositivos IoT*

*Note: Sub-titles are not captured in Xplore and should not be used

Rocio Alvarado
Centro de Investigación en Matemáticas Aplicadas, Universidad Autónoma de Coahuila,
Saltillo, Coahuila, México

I. Introduction

El Internet de las cosas (IoT) se refiere a dispositivos, instrumentos, vehículos y edificios compuestos por componentes como software y sensores que permiten la conexión a una red, mediante la cual pueden ser controlados de forma remota, facilitando la recopilación y el intercambio de datos [1]. El uso del IoT busca simplificar tareas y actividades, minimizando la intervención humana y promoviendo la creación de hogares, ciudades, infraestructuras y sistemas de transporte inteligentes [2].

En los últimos años, el IoT ha cobrado mayor relevancia debido a su amplia gama de aplicaciones en la industria, la biomedicina, la agricultura, las ciudades inteligentes, el monitoreo ambiental y otros campos, ya que proporciona mejores servicios a los usuarios finales mediante el procesamiento, las comunicaciones y la visualización de datos en tiempo real. Sin embargo, debido a que estos dispositivos operan bajo arquitecturas y protocolos propios, que aún se encuentran en desarrollo, la conexión entre ellos es insegura y presenta problemas de interoperabilidad e integración [3]. Debido a que estos dispositivos recopilan información personal, como direcciones, correos, cuentas bancarias, entre otros, lo que los convierte en un recurso invaluable, pero también en un objetivo atractivo para ciberdelincuentes. Sin embargo, estos dispositivos suelen tener un alto grado de vulnerabilidad, debido a la falta de estandarización en los protocolos de seguridad y a su capacidad limitada para implementar medidas avanzadas de protección, convirtiéndose en el objetivo de diversos ataques [4].

En estos años se ha incrementado el número de ataques dirigidos a empresas y entidades gubernamentales con el fin de obtener información valiosa para diversos propósitos, como el espionaje industrial, la manipulación política o el fraude financiero. Estos ataques pueden tomar múltiples formas, desde el robo de datos sensibles, la suplantación de identidad, la alteración de información crítica, hasta la interrupción de servicios esenciales [5].

II. Trabajo Relacionado

Se ha propuesto el uso de modelos de machine learning para la detección de ataques en redes IoT. Se menciona la utilización de seis algoritmos (LR, NB, MLP, DT, RF, MLP), los cuales fueron entrenados con el dataset CICIoT2023, dando como resultado que el algoritmo RF presenta los mejores resultados en F1 score, precisión, recall y exactitud. Sin embargo, se resalta que este tipo de algoritmo suele tener un mayor tiempo de ejecución en comparación con los demás [6]. En otros trabajos [7], se propone el uso del modelo LSTM Neural Network para evaluar el comportamiento del modelo en la detección de ciberataques, obteniendo una precisión del 98.66%. Sin embargo, los autores recomiendan realizar mejoras en la interpretabilidad y escalabilidad. [8] propone utilizar los algoritmos (RF, DT, SVM, KNN, GB, NB) para generar una predicción de ataques en entornos IoT. En su análisis, sugieren que los algoritmos más adecuados para realizar esta predicción, basándose en la precisión y el tiempo de ejecución, son RF y GB. Sin embargo, dado que los ataques se vuelven cada vez más sofisticados, también sugieren que los algoritmos deben ser capaces de adaptarse a estos nuevos desafíos. En [9] se propone la creación de un sistema para la detección de intrusos mediante el uso de un algoritmo GSK, el cual fue capaz de obtener una precisión del 99.26% en la clasificación binaria. También se propone el uso de modelos de detección de anomalías mediante ensambles como ECDD, BIFAD y NFBoost, cuyo objetivo es identificar ataques DDoS. Al comparar dichos modelos, se encontró que ECDD obtuvo una precisión del 96% y un promedio de falsos positivos del 9%. Sin embargo, esto se limita a un solo tipo de ataque, por lo que se sugiere ampliar el modelo [10]. En proponen el uso de Deep learning mediante el uso de tres algoritmos DNN, LSTM y CNN para la detección de intrusos donde plantean que los algoritmos de DL suelen superar a otros algoritmos en la detección de intrusiones en redes IoT [11] ,mientras [12] que en otras investigaciones se plantea el uso de un algoritmo hibrido de DL para la detección de ataques en el cual se encontró que dicho modelo tiene una precisión del 99.995% sin embargo los autores menciona que para obtener valores de precisión altos es importante tener una gran cantidad de datos como la que proporciona el data set CICIoT2023.

III. Métodos

A. Descripción del dataset

Para este trabajo se empleará el dataset ”CICIOT2023”, creado por el Canadian Institute for Cybersecurity (CIC). Este

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

dataset simula el tráfico de red generado por dispositivos IoT en diferentes escenarios, incluyendo tanto situaciones de tráfico benigno como de ataques.

El dataset está compuesto por las siguientes características, que describen diversos aspectos del tráfico de red:

- **Header Length**: Longitud de la cabecera del paquete de red.
- **Protocol Type**: Tipo de protocolo utilizado (por ejemplo, TCP, UDP, ICMP).
- **Time To Live (TTL)**: Tiempo de vida del paquete antes de ser descartado.
- **Rate**: Tasa de transferencia de paquetes.
- **fin flag number, syn flag number, rst flag number, psh flag number, ack flag number, ece flag number, cwr flag number**: Contadores de las banderas de control utilizadas en las conexiones TCP (FIN, SYN, RST, PSH, ACK, ECE, CWR).
- **ack count, syn count, fin count, rst count**: Número de paquetes con las banderas ACK, SYN, FIN, y RST.
- **HTTP, HTTPS, DNS, Telnet, SMTP, SSH, IRC, TCP, UDP, DHCP, ARP, ICMP, IGMP, IPv, LLC**: Indicadores de la presencia de tráfico asociado a distintos protocolos y servicios de red.
- **Tot sum, Min, Max, AVG, Std**: Estadísticas de los valores medidos, incluyendo suma total, valor mínimo, valor máximo, promedio (AVG), y desviación estándar (Std).
- **Tot size**: Tamaño total de los paquetes.
- **IAT (Inter Arrival Time)**: Tiempo entre la llegada de paquetes.
- **Number**: Contador de eventos o paquetes.
- **Variance**: Varianza de los valores registrados en un conjunto de características.

B. Entrenamiento del modelo

Para la detección de anomalías, se seleccionó el algoritmo *Isolation Forest*, el cual se utiliza para identificar valores atípicos en conjuntos de datos con un predominio de muestras normales. *Isolation Forest* construye varios árboles de decisión aleatorios que aíslan las muestras de datos, y aquellas muestras que se aíslan más fácilmente son identificadas como anomalías.

El modelo fue configurado con una proporción de contaminación del 5%, indicando que aproximadamente el 5% del conjunto de datos se espera que corresponda a tráfico anómalo. Esta proporción se calcula a través de la siguiente fórmula:

$$\text{Contaminación} = \frac{\text{Muestras anormales}}{\text{Total de muestras}}$$

Se definió el parámetro `random_state` en 42 para controlar la aleatoriedad de los datos; sin embargo, esta semilla puede cambiarse a cualquier número entero, ya que no existe un criterio establecido para la elección de este. Después de esto, se procedió a predecir si una muestra era anormal o no. En esta fase, se creó una columna llamada Anormal, en la que se guardaron las predicciones de cada dato. Para ello, se asignaron valores de -1 para las anomalías y 1 para los datos normales. Dado que el conjunto de datos utilizado tiene definida en la columna label la palabra ”benigno” para los datos normales y ”ataque” para las anomalías, se procedió a ajustar las predicciones para que coincidieran con los valores del conjunto de datos, donde ataque = -1 y benigno = 1, de manera que las columnas quedaran alineadas.

IV. Resultados

En la Figura 1 podemos observar la distribución de los datos. Se puede notar que el conjunto de datos empleado contiene un mayor número de tráfico anómalo, lo cual podría generar un desbalance en los datos.

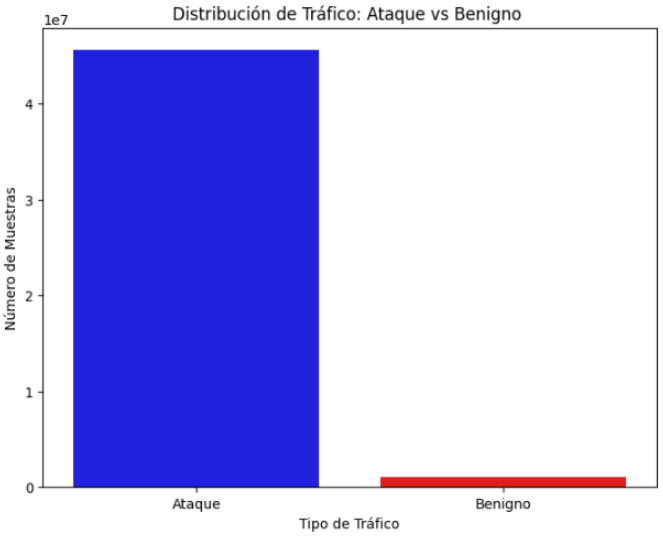

Fig. 1. Distribución de los datos.

En la Tabla I se presentan los resultados obtenidos del entrenamiento. Se puede observar que el modelo tiene una precisión relativamente baja, especialmente si se compara con otros trabajos en los que se reportan valores de accuracy superiores al 90%.

TABLE I
Resultados del modelo

Métrica	Resultado
`Accuracy`	0.6833
`Recall`	0.0519
`F1 Score`	0.0964

V. Conclusión

Se ha evaluado el rendimiento del algoritmo IsolationForest en el conjunto de datos CICIoT 2023 en cual cuenta con un desbalance entre tráfico normal y anómalo. Los resultados obtenidos, presentados en la Tabla I, indican que, aunque el modelo alcanza una precisión de 0.6833, su capacidad para identificar correctamente las instancias de tráfico anómalo es limitada, como lo demuestra su bajo recall de 0.0519 y su F1 score de 0.0964.

Como trabajo futuro, se recomienda explorar técnicas para balancear las clases, aplicar un análisis de correlación para eliminar variables irrelevantes, e incluso considerar el uso de un modelo diferente y evaluar su comportamiento.

REFERENCES

[1] P. Gokhale, O. Bhat, and S. Bhat, "Introduction to IOT," *International Advanced Research Journal in Science, Engineering and Technology*, vol. 5, no. 1, pp. 41–44, 2018.

[2] T. Yousuf, R. Mahmoud, F. Aloul, and I. Zualkernan, "Internet of things (IoT) security: current status, challenges and countermeasures," *International Journal for Information Security Research (IJISR)*, vol. 5, no. 4, pp. 608–616, 2015.

[3] L. Farhan, S. T. Shukur, A. E. Alissa, M. Alrweg, U. Raza, and R. Kharel, "A survey on the challenges and opportunities of the Internet of Things (IoT)," in *Proc. 2017 Eleventh International Conference on Sensing Technology (ICST)*, 2017, pp. 1-5, doi: 10.1109/ICSensT.2017.8304465.

[4] W. L. Garzón and J. C. López, "Tecnología Internet of Things (IoT) y el Big Data," *Mare Ingenii*, vol. 1, no. 1, pp. 73–79, 2019.

[5] C. D. Daniel, "Ciberseguridad como herramienta fundamental, ante la inminente amenaza global," in *Revista Ensayos Militares*, vol. 8, no. 1, pp. 33–50, 2022.

[6] F. C. Mejías Espinosa, "Intrusion detection in IoT networks using machine learning," Master's thesis, Universitat Politècnica de Catalunya, 2023.

[7] A. I. Jony and A. K. B. Arnob, "A long short-term memory based approach for detecting cyber attacks in IoT using CIC-IoT2023 dataset," *Journal of Edge Computing*, vol. 3, no. 1, pp. 28–42, 2024.

[8] A. C. German Nelson, "Modelo predictivo de ciberataques en entornos de Internet de las cosas," 2024.

[9] H. Q. Gheni and W. L. Al-Yaseen, "Two-step data clustering for improved intrusion detection system using CICIoT2023 dataset," *e-Prime: Advances in Electrical Engineering, Electronics and Energy*, vol. 9, p. 100673, 2024.

[10] D. S. Eswari and P. V. Lakshmi, "DDoS attacks in traffic flow streams using ensemble classifiers," *Computación y Sistemas*, vol. 28, no. 3, 2024.

[11] J. Jose and D. Jose, "Deep learning algorithms for intrusion detection systems in Internet of Things using CIC-IDS 2017 dataset," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 13, no. 1, 2023.

[12] S. Yaras and M. Dener, "IoT-based intrusion detection system using new hybrid deep learning algorithm," *Electronics*, vol. 13, no. 6, p. 1053, 2024.