/UCIENCIA/.21
IV Conferencia Científica Internacional
Universidad de las Ciencias Informáticas

Temática: Aplicaciones de la Inteligencia Artificial y Ciencias de Datos a la ciberseguridad.

Técnicas de Inteligencia Artificial para Sistemas de Detección de Intrusiones

Artificial Intelligence Techniques for Intrusion Detection Systems

Ing. Darvis Dorvigny Dorvigny[1*], Esp. Dennis Barrera Pérez[2], Lic. Lester Rodríguez Vallejo[3]

[1]Departamento de Sistemas Digitales, Facultad 2, Universidad de las Ciencias Informáticas. ddorvigny@uci.cu
[2]Departamento de Sistemas Digitales, Facultad 2, Universidad de las Ciencias Informáticas. dbperez@uci.cu
[3]Departamento de Informática, Facultad 2, Universidad de las Ciencias Informáticas. lesterr@uci.cu

[*]Autor para correspondencia: ddorvigny@uci.cu

Resumen
El vertiginoso desarrollo de las Tecnologías de la Información y la Comunicación ha propiciado que cada vez más personas y organizaciones se conecten a Internet. El volumen de información disponible en las redes cada vez es mayor. Al mismo tiempo aumentan las amenazas y la actividad maliciosa de los ciberdelincuentes, expresada en ciberataques cada vez más sofisticados que afectan las redes y los sistemas informáticos, poniendo en riesgo la confidencialidad, integridad y la disponibilidad de la información. Los Sistemas de Detección de Intrusiones constituyen una importante línea de defensa para los sistemas informáticos frente a estas amenazas. Diferentes técnicas de la Inteligencia Artificial como el aprendizaje automatizado, o el aprendizaje profundo, han permitido importantes avances en el desarrollo de este mecanismo de seguridad. En este trabajo se realiza una revisión de los trabajos más relevantes que aplican las técnicas de Inteligencia Artificial para el desarrollo de Sistemas de Detección de Intrusiones de red basados en anomalías. Se abordan los conjuntos de datos más utilizados, y se plantean los retos fundamentales que constituyen líneas de trabajo futuro.

Palabras claves: Sistemas de Detección de Intrusiones de red basados en anomalías, Inteligencia Artificial, Aprendizaje Automatizado, Aprendizaje profundo, redes neuronales, Conjuntos de datos

Abstract
The rapid development of Information and Communication Technologies has led more and more people and organizations to connect to the Internet. The volume of information available on the networks is increasing. At the same time, threats and malicious activity by cybercriminals are increasing, expressed in increasingly sophisticated cyberattacks that affect networks and computer systems, putting the confidentiality, integrity and availability of information at risk. Intrusion Detection Systems represent an important line of defense for computer systems against these threats. Different techniques of Artificial Intelligence such as Machine Learning, or Deep Learning, have allowed important advances in the development of this security mechanism. In this paper a review of the most relevant works that apply Artificial Intelligence techniques for the development of Network Intrusion Detection Systems based on anomalies is carried out. The most widely used data sets are addressed, and the fundamental challenges are raised as lines of scientific research work.

Keywords: *Anomaly based Network Intrusion detection system, Artificial Intelligence, Machine Learning, Deep Learning, neural networks, datasets*

Introducción

Gracias al vertiginoso desarrollo de las Tecnologías de la Información y la Comunicación (TIC), cada vez más personas y organizaciones se conectan a Internet. El volumen de información disponible en las redes cada vez es mayor. Al mismo tiempo aumentan las amenazas y la actividad maliciosa de los ciberdelincuentes. Esto justifica el desarrollo de nuevas técnicas que permitan fortalecer la ciberseguridad.

La protección de los sistemas informáticos y las redes generalmente se realiza restringiendo el acceso a los recursos disponibles mediante sistemas antivirus, cortafuegos, mecanismos de control de acceso, técnicas criptográficas, protocolos de red seguros, entre otros; mediante distintos modelos de seguridad. Debido a la naturaleza dinámica de los datos en las redes, los mecanismos anteriores para proteger la información de los ciberataques no son suficientes. El tráfico de red es una fuente inagotable de conocimiento, que se puede explotar para complementar los mecanismos de seguridad. (Sengupta and Sil, 2020)

Se entiende por intrusión a cualquiera de las formas que utilizan los ciberdelincuentes para atacar a los sistemas informáticos conectados en red con el objetivo de afectar la disponibilidad, integridad, o la confidencialidad de la información. Es amplia la diversidad de tipos de intrusiones, desde ataques con malware, ransomware, denegación de servicio (DoS), phishing o ingeniería social, ataques de inyección SQL, ataques de hombre en el medio, explotación de vulnerabilidades conocidas o de Día Cero, escalada de privilegios no autorizados, desfiguración de sitios web, alteración del contenido de bases de datos, entre otros.(Sarker et˜al., 2021) Todas estas intrusiones, de efectuarse con éxito, pueden afectar a organizaciones e individuos, causar interrupciones y pérdidas devastadoras, y dañar considerablemente infraestructuras críticas.

Los sistemas de detección de intrusiones (IDS) constituyen una importante línea de defensa para los sistemas informáticos frente a estas amenazas.(Ferrag et˜al., 2020) Los IDS son diseñados para monitorear el tráfico de la red o las actividades de las estaciones de trabajo, y para emitir alertas o alarmas a los administradores cuando se detectan intrusiones. Se puede usar un cortafuegos junto con un IDS para bloquear el tráfico malicioso identificado con el fin de proteger las computadoras internas de los ataques detectados. (Fung and Boutaba, 2013)

Según el origen de los datos, pueden estar basados en host o en red. Los IDS de host (HIDS) analizan el comportamiento del sistema operativo de la computadora o estación de trabajo. Su ámbito de detección es reducido. En cambio, el IDS de red (NIDS), se despliega en un nodo donde pueda inspeccionar todo el tráfico de la red. Contienen sensores para la escucha de paquetes, y un analizador de datos para procesar y correlacionar

datos obtenidos. Emiten alarmas cuando detectan una intrusión en la red, pero no tienen información sobre la actividad interna en las computadoras.

Los IDS basados en firmas comparan los paquetes de datos con atributos de intrusiones conocidas para decidir cuando el tráfico observado es malicioso o no; en cambio su eficiencia decae en la detección de intrusiones desconocidas o con firmas polimórficas. Los IDS basados en anomalías observan el tráfico para detectar actividades distintas al comportamiento habitual; por esta razón pueden detectar intrusiones nuevas o desconocidas. Ambos tipos de IDS presentan altas tasas de falsos positivos, y mantenerlos actualizados con los nuevos tipos de intrusiones es un reto. En (Sarker et˜al., 2021) se plantea que se han desarrollado soluciones híbridas para aprovechar las potencialidades de los IDS basados en firmas o en anomalías.

El gran volumen de tráfico de red que se genera constantemente ha motivado a varios autores a plantear soluciones basadas en diversas técnicas de la Inteligencia Artificial. Se han abierto importantes nichos de investigación en esta fusión con la Ciberseguridad para el desarrollo de nuevos IDS con resultados interesantes. Especialmente las técnicas de aprendizaje automatizado o Machine Learning han acaparado la atención de los investigadores, por la capacidad de generar conocimiento a partir de los datos. Su aplicación ha tenido mayor impacto en los NIDS basados en anomalías.

En este trabajo se pretende hacer una revisión de los aportes más relevantes donde se aplican intensivamente las técnicas de Inteligencia Artificial para el desarrollo de Sistemas de Detección de Intrusiones de red basados en anomalías. Se plantean los retos fundamentales que constituyen líneas de trabajo futuro.

Materiales y métodos

El Aprendizaje Automatizado o Machine Learning (ML) es el proceso de extraer conocimiento a partir de grandes cantidades de datos. Los modelos de ML comprenden conjuntos de reglas, métodos, funciones de transferencia complejas, que pueden ser aplicadas para encontrar patrones en los datos, o para reconocer o predecir comportamiento. Los modelos pueden ser supervisados, que requieren conocimiento de expertos, no supervisados, o semisupervisados. (Liu and Lang, 2019)

El Aprendizaje Profundo o Deep Learning (DL) es un nuevo campo del aprendizaje automático, que se basa en redes neuronales artificiales. Se ha aplicado en muchas áreas, como el reconocimiento de voz y de imágenes, el procesamiento del lenguaje natural, el descubrimiento de fármacos y los sistemas recomendados. En los últimos años, el aprendizaje profundo ha demostrado su eficacia en el campo de la detección de intrusiones y en el área de la ciberseguridad en general. (Louati and Ktata, 2020) Estas técnicas tienden a ser más eficientes que el ML tradicional debido a su estructura profunda y su capacidad para aprender las características importantes

del conjunto de datos. (Ahmad et˜al., 2021)

El empleo de métodos de Machine Learning y Deep Learning para desarrollar NIDS generalmente implica seguir tres fases principales: preprocesamiento de datos, entrenamiento y validación del modelo propuesto. Para todas las soluciones propuestas, primero se preprocesa el conjunto de datos para transformarlo en el formato adecuado que requiere el algoritmo. Esta etapa generalmente implica codificación y normalización. El conjunto de datos puede requerir un proceso de limpieza, en términos de eliminar entradas con datos faltantes o entradas duplicadas. Los datos preprocesados luego se dividen aleatoriamente en dos subconjuntos, uno para entrenamiento y otro para prueba o validación. (Imamverdiyev and Abdullayeva, 2018), (Alsughayyir et˜al., 2019) Luego, en la próxima fase el algoritmo ML o DL se entrena utilizando el conjunto de datos de entrenamiento. El tiempo que tarda el algoritmo en aprender depende del tamaño del conjunto de datos y de la complejidad del modelo propuesto. Normalmente, los modelos de DL requieren más tiempo de entrenamiento debido a su estructura profunda y compleja. Una vez que se entrena el modelo, se valida con el conjunto de datos de prueba y se evalúa en función de las predicciones que hizo. El NIDS estará entonces en capacidad de detectar si la instancia del tráfico de red pertenece a una clase benigna (normal) o de ataque.

Los métodos más utilizados de Machine Learning para el desarrollo de Sistemas de Detección de Intrusiones se resumen en la figura 1. En (Liu and Lang, 2019) puede consultarse una taxonomía completa sobre los métodos y técnicas de ML y DL.

Los conjuntos de datos juegan un papel fundamental en el desarrollo de NIDS con modelos de ML/DL. En la literatura se reportan varios trabajos que caracterizan los conjuntos que están públicos y disponibles para la comunidad de investigadores. Estos son útiles para el entrenamiento y la evaluación de las soluciones que se proponen. (Leyva and Borroto, 2020) Se han obtenido gracias al conocimiento de expertos en ciberseguridad que etiquetaron las instancias de tráfico ya reconocidas como intrusiones. Otra fuente de obtención ha sido en ambiente controlado simulando distintos tipos de ataques, registrando los eventos, y etiquetándolos luego. Se pueden citar como ejemplos DARPA98, KDD-99, UNSW-NB15, NSL-KDD, UNM, Caida DDoS, ADFA Linux. (Hamid et˜al., 2018) Los más recientes conjuntos de datos disponibles, que un gran número de autores están utilizando para evaluar sus modelos de NIDS basados en ML/DL, son CICIDS2017 y CICIDS2018. (Panigrahi and Borah, 2018)

Para mostrar el nivel de aplicabilidad de las técnicas de Inteligencia Artificial en el desarrollo de NIDS, los autores de esta investigación han seleccionado una muestra representativa de los trabajos que han sido publicados en los últimos tres años. Se tuvo en cuenta para la selección que describieran una o varias técnicas de IA aplicadas para la construcción de NIDS, y que hayan sido referenciados por otros autores en artículos de revisión.

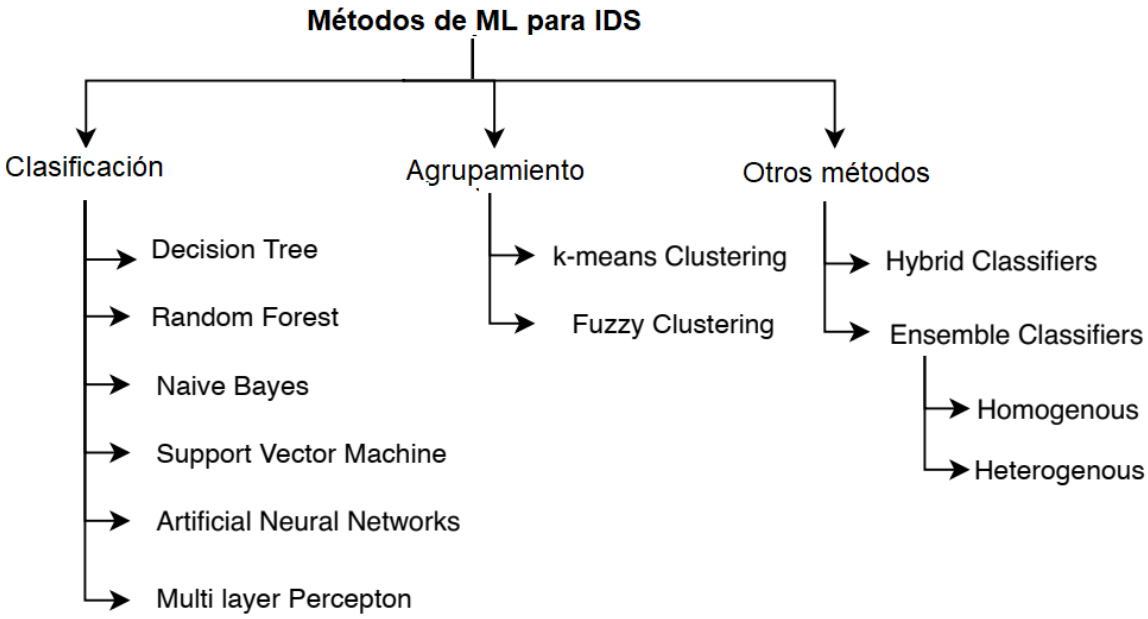

Figura 1: Métodos de Machine Learning para IDS. Adaptado de (Thakkar and Lohiya, 2020)

En (Kabir et˜al., 2018) se propuso una técnica basada en el muestreo con Máquina de Vector de Soporte de Mínimos Cuadrados (LS-SVM) para la detección de intrusiones en la red. Esta técnica consta de dos fases. En la primera fase, el conjunto de datos se dividió en subgrupos arbitrarios. Luego, se eligieron las características más discriminatorias de estos subgrupos. Se encontró que las características seleccionadas se parecen a todo el conjunto de datos. Finalmente, se exploró un esquema óptimo de asignación de acuerdo con la variabilidad de las observaciones dentro de los subgrupos. En la segunda fase de la técnica propuesta, se utilizó LS-SVM para extraer las muestras utilizadas en la detección de intrusiones en una red. El conjunto de datos utilizado para la validación fue KDD-99.

Un nuevo modelo de aprendizaje profundo de dos etapas para la detección de intrusiones se propuso en (Khan et˜al., 2019). Inicialmente, el valor de la puntuación de probabilidad se calculó para categorizar el tráfico de red como normal o anormal. Se consideró este valor de puntuación de probabilidad como una métrica adicional para clasificar las instancias de tráfico (normal o anormal) en la segunda etapa. La puntuación de probabilidad utilizada permitió que, al ejecutar la segunda etapa del modelo, se evitase el problema de sobreajuste del algoritmo. Este modelo de dos etapas es capaz de manejar gran cantidad de datos sin etiquetar, y aprender las características de manera efectiva y automática. Para la validación de la propuesta se utilizaron los conjuntos de datos KDD-99 y UNSW-NB15.

(Zhang et˜al., 2019a) ofreció un modelo de detección de intrusiones basado en Redes de Creencia Profunda (DBN). Se optimizó mediante un algoritmo genético mejorado (GA). El número de capas ocultas en DBN y el número de neuronas en cada capa se decidió mediante GA. Los resultados de la GA se utilizaron en DBN para detectar las intrusiones con una estructura compacta y una alta tasa de detección. El conjunto de datos utilizado para la validación fue KDD-99.

Un enfoque más complejo que el anterior se plantea en (Wei et˜al., 2019), donde se describe un método optimizado Deep Belief Network (DBN) para la detección y clasificación de intrusiones. Inicialmente, se utilizó una optimización de enjambre de partículas (PSO) en DBN para decidir el factor de aprendizaje y el peso de inercia adaptativa. La solución de optimización inicial de PSO se optimizó mediante el algoritmo de comportamiento de los peces. Una vez que se generaron las mejores soluciones poblacionales iniciales de PSO, se buscaron las mejores soluciones globales de PSO utilizando operadores genéticos. Por lo tanto, el algoritmo PSO se optimizó mediante algoritmos genéticos y de enjambre de peces para obtener las mejores soluciones óptimas para decidir el mejor modelo DBN para la clasificación de intrusiones. El conjunto de datos utilizado fue NSL-KDD.

En (Xiao et˜al., 2019) se plantea un modelo de detección de intrusiones de red basado en la red neuronal convolucional (CNN) con un método de reducción de características. El proceso de detección de intrusiones se inició con la eliminación de las características redundantes e irrelevantes mediante métodos de reducción de dimensionalidad. Después de eso, se empleó CNN para extraer las características de los datos reducidos. Además, la información más eficaz para identificar intrusiones se extrajo mediante aprendizaje supervisado. El conjunto de datos utilizado para la validación fue KDD-99.

En (Zhang et˜al., 2019a) se propuso una red jerárquica profunda para la detección de intrusiones en la red. Esta red integró LeNet-5 y LSTM mientras aprendía las características espaciales y temporales del flujo. La red jerárquica profunda se entrenó al mismo tiempo en lugar de dos redes de entrenamiento mediante el diseño de un método de conexión en cascada de red razonable. Se examinaron las características del flujo para identificar el flujo irregular de la red. El conjunto de datos utilizado para la validación fue KDD-99.

(Yang et˜al., 2019) propuso un modelo combinado de detección basado en un modelo de aprendizaje profundo. Se generó una base de datos mediante el mapeo de características, la codificación one-hot y el procesamiento de normalización. Se construyó una red de creencia profunda (DBN) con la máquina de Boltzmann de múltiples restricciones (RBM) y retropropagación (BP) para la detección de intrusiones. Como capa adicional, la capa de red de BP se adjuntó al final de RBM. Se utilizó SVM para preparar el sistema para la detección de intrusiones. El conjunto de datos utilizado fue NSL-KDD.

En (Feng et˜al., 2019) se describe un dispositivo plug and play que emplea una herramienta de captura de paquetes y un modelo de detección de aprendizaje profundo para detectar denegación de servicio (DoS) y ataques a la privacidad en redes ad hoc. Para detectar ataques XSS y SQL, el modelo propuesto utiliza dos enfoques de aprendizaje profundo, a saber, red neuronal convolucional (CNN) y memoria a corto plazo (LSTM). Para detectar ataques DoS, el modelo propuesto utiliza una red neuronal profunda. El estudio utilizó el conjunto de datos KDD-99, que se divide en un 30 % para pruebas y un 70 % para entrenamiento. Además, el estudio informó una precisión de 0,57 % y 0,78 % para la detección de ataques XSS utilizando la red neuronal profunda y la red neuronal convolucional, respectivamente.

El trabajo propuesto por (Kasongo and Sun, 2019) utiliza una red neuronal profunda de alimentación hacia adelante (FFDNN). Consiguen hacer la selección de características basada en filtros para generar subconjuntos óptimos de características con una redundancia mínima en redes inalámbricas. Utilizan el conjunto de datos NSL-KDD. Con una tasa de aprendizaje de 0,05 y 30 neuronas repartidas con 3 capas ocultas, la evaluación de rendimiento muestra que el sistema propuesto alcanza una precisión del 99,69 %.

(Otoum et˜al., 2019) introdujo un sistema de detección de intrusiones agrupadas en redes de sensores inalámbricos, llamado RBC-IDS, que se basa en la máquina de Boltzmann restringida. El sistema RBC-IDS utiliza los N grupos con C nodos de sensores en cada grupo. El estudio utiliza el conjunto de datos Network Simulator-3 (NS-3) y KDD-99 en la evaluación de desempeño. En comparación con el IDS basado en aprendizaje automático adaptativo (ASCH-IDS), el sistema RBC-IDS alcanza la tasa de precisión más alta del 99,91 % cuando el número de capas ocultas es 3, mientras que el ASCH-IDS archiva el 99,83 % .

Otra red de creencia profunda fue utilizada para la detección de intrusiones por (Thamilarasu and Chawla, 2019). Utilizan una red de creencia profunda para fabricar la red neuronal profunda de retroalimentación para el Internet de las cosas. Específicamente, los autores propusieron una función binaria de pérdida de entropía cruzada para minimizar el costo total en el modelo IDS. Para la evaluación del rendimiento utilizan la biblioteca Keras, el simulador de red Cooja y las etiquetas de sensor CC2650 de Texas Instruments. La biblioteca de Keras se utiliza para crear un modelo secuencial de aprendizaje profundo. El modelo propuesto se prueba contra cinco tipos de ataques. Los resultados muestran una mayor precisión del 96 % y una tasa de recuperación del 98,7 % para la detección de ataques DDoS.

El estudio de (Zhang et˜al., 2019b) es un buen ejemplo de la combinación de un algoritmo genético mejorado y una red de creencia profunda para la detección de intrusiones. El estudio utiliza múltiples máquinas de Boltzmann restringidas, que principalmente ejecutan el aprendizaje no supervisado de datos preprocesados. El módulo de la red de creencia profunda se divide en dos pasos en la fase de entrenamiento: (1) cada máquina de Boltzmann restringida se entrena por separado y (2) la última capa de la red de creencia profunda se

establece como la red neuronal de retropropagación. La evaluación del desempeño utilizando el conjunto de datos NSL-KDD muestra una tasa de detección del 99 % en la detección de ataques de inyección de datos falsos en el sistema de control de supervisión y adquisición de datos.

En (Khan et˜al., 2019) se propuso un sistema de detección de intrusiones basado en el modelo de aprendizaje profundo de dos etapas, llamado TSDL. El modelo TSDL utiliza un codificador automático apilado con un clasificador soft-max, que se compone de tres capas principales, a saber, (1) la capa de entrada, (2) las capas ocultas y (3) la capa de salida. Estas tres capas emplean una red neuronal de retroalimentación similar a un perceptrón multicapa. El estudio utiliza dos conjuntos de datos públicos, incluidos los conjuntos de datos KDD-99 y UNSW-NB15. Los resultados en el conjunto de datos KDD-99 alcanzan altas tasas de reconocimiento, hasta el 99,996 %. Además, los resultados del conjunto de datos UNSW-NB15 alcanzan altas tasas de reconocimiento, hasta un 89,13 %.

(Yang et˜al., 2019) plantea la combinación de un autocodificador variacional condicional mejorado y una red neuronal profunda para la detección de intrusiones. El estudio propuesto consta de tres fases: (1) entrenamiento, (2) generación de nuevos ataques y (3) detección de ataques. La fase de entrenamiento consiste en optimizar la pérdida del codificador y del decodificador. La fase de generación de nuevos ataques utiliza una distribución gaussiana multivariante como distribución. La fase de detección de ataques emplea una red neuronal profunda para detectar ataques. Para validar el modelo propuesto, se utilizan los conjuntos de datos NSL-KDD y UNSW-NB15, cuya tasa de aprendizaje predeterminada del optimizador Adam es 0,001. Los resultados muestran la mayor precisión del 89,08 % y la tasa de detección del 95,68 % en el conjunto de datos UNSW-NB15.

En (Jiang et˜al., 2020) se propuso un algoritmo de detección de intrusiones en la red mediante la integración de muestreo híbrido y una red jerárquica profunda. Se empleó un método de selección unilateral (OSS) en el algoritmo para eliminar las muestras de ruido en la categoría mayoritaria. Las muestras minoritarias se incrementaron aplicando la Técnica de sobremuestreo de minorías sintéticas (SMOTE). Después de resolver el problema de desbalance en el conjunto de datos, se utilizó una red neuronal convolucional (CNN) y una memoria bidireccional a largo plazo a corto plazo (BiLSTM) para extraer características espaciales y temporales, respectivamente. Esas características se utilizaron para la detección de intrusiones. Se emplearon los conjuntos de datos NSL-KDD y UNSW-NB15 para simulación y evaluación.

Discusión y conclusiones

Varios de los trabajos analizados hacen alusión a problemas fundamentales como: la inexistencia de conjuntos de datos suficientes, que contengan la mayor variedad de tipos de intrusiones; su nivel limitado de actualización. Por otra parte, los conjuntos de datos empleados, o bien fueron recolectados en años anteriores, en períodos

cortos, o bien son resultado de simulaciones de ataques. La mayoría fueron recolectados y almacenados en ficheros de disco, lo cual hace que su procesamiento no ocurra en ambiente real, por las características propias del acceso a disco en una computadora. En otro orden, otra limitación es que al mezclar distintos tipos de intrusiones, hace que en cada fichero exista un alto número de instancias, no pocas veces repetidas.

Muchas metodologías de IDS propuestas por los investigadores son basadas en modelos complejos que requieren gran cantidad de tiempo de procesamiento y recursos de computación (al menos el 80 % de los métodos basados en ML o DL/ML). Esto implica una sobrecarga para la unidad de procesamiento, y afecta el rendimiento del IDS. En muchos casos se requiere el uso de GPU multinúcleos de alto rendimiento para aumentar la velocidad del proceso de entrenamiento y operación, siendo muy costoso.

La mayoría de las metodologías propuestas para IDS exhiben menor precisión en la detección de ciertos tipos de ataques. Este problema es causado por la naturaleza no balanceada del conjunto de datos. Es decir, el número de instancias etiquetadas como intrusiones es muchas veces menor que las etiquetadas como tráfico normal. Este asunto continúa siendo un problema de investigación. La precisión en la detección de clases de ataques poco frecuentes es menor que ataques con mayor número de instancias.

La capacidad de detección ante ataques de Día Cero no es suficientemente abordada en estos trabajos, por lo que se mantiene abierto un campo de investigación importante. Otra problemática común es la dificultad de poner en producción estas soluciones, que algunas se mantienen en escenarios controlados, a nivel de laboratorio, y no ha podido demostrarse su capacidad de respuesta en ambientes reales, particularmente en redes grandes con alto volumen de tráfico.

Son múltiples las aristas que constituyen retos para el desarrollo de modelos de Inteligencia Artificial para los Sistemas de Detección de Intrusiones de red.

Referencias

Ahmad, Z., Shahid Khan, A., Wai Shiang, C., Abdullah, J., and Ahmad, F. (2021). Network intrusion detection system: A systematic study of machine learning and deep learning approaches. *Transactions on Emerging Telecommunications Technologies*, 32(1):e4150. Publisher: Wiley Online Library.

Alsughayyir, B., Qamar, A. M., and Khan, R. (2019). Developing a network attack detection system using deep learning. In *2019 International Conference on Computer and Information Sciences (ICCIS)*, pages 1–5. IEEE.

Feng, F., Liu, X., Yong, B., Zhou, R., and Zhou, Q. (2019). Anomaly detection in ad-hoc networks based on

deep learning model: A plug and play device. *Ad Hoc Networks*, 84:82–89. Publisher: Elsevier.

Ferrag, M. A., Maglaras, L., Moschoyiannis, S., and Janicke, H. (2020). Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study. *Journal of Information Security and Applications*, 50:102419.

Fung, C. and Boutaba, R. (2013). *Intrusion Detection Networks: A Key to Collaborative Security*. CRC Press.

Hamid, Y., Balasaraswathi, V. R., Journaux, L., and Sugumaran, M. (2018). Benchmark Datasets for Network Intrusion Detection: A Review. *IJ Network Security*, 20(4):645–654.

Imamverdiyev, Y. and Abdullayeva, F. (2018). Deep learning method for denial of service attack detection based on restricted boltzmann machine. *Big data*, 6(2):159–169.

Jiang, K., Wang, W., Wang, A., and Wu, H. (2020). Network intrusion detection combined hybrid sampling with deep hierarchical network. *IEEE Access*, 8:32464–32476. Publisher: IEEE.

Kabir, E., Hu, J., Wang, H., and Zhuo, G. (2018). A novel statistical technique for intrusion detection systems. *Future Generation Computer Systems*, 79:303–318. Publisher: Elsevier.

Kasongo, S. M. and Sun, Y. (2019). A deep learning method with filter based feature engineering for wireless intrusion detection system. *IEEE Access*, 7:38597–38607. Publisher: IEEE.

Khan, F. A., Gumaei, A., Derhab, A., and Hussain, A. (2019). A novel two-stage deep learning model for efficient network intrusion detection. *IEEE Access*, 7:30373–30385. Publisher: IEEE.

Leyva, O. C. and Borroto, M. G. (2020). AnÃ¡lisis y caracterizacion de conjuntos de datos para deteccion de intrusiones. *Serie Cientifica de la Universidad de las Ciencias Informaticas*, 13(4):39–52.

Liu, H. and Lang, B. (2019). Machine learning and deep learning methods for intrusion detection systems: A survey. *applied sciences*, 9(20):4396.

Louati, F. and Ktata, F. B. (2020). A deep learning-based multi-agent system for intrusion detection. *SN Applied Sciences*, 2(4):1–13. Publisher: Springer.

Otoum, S., Kantarci, B., and Mouftah, H. T. (2019). On the feasibility of deep learning in sensor network intrusion detection. *IEEE Networking Letters*, 1(2):68–71. Publisher: IEEE.

Panigrahi, R. and Borah, S. (2018). A detailed analysis of CICIDS2017 dataset for designing Intrusion Detection Systems. *International Journal of Engineering & Technology*, 7(3.24):479–482.

Sarker, I. H., Furhad, M. H., and Nowrozy, R. (2021). Ai-driven cybersecurity: an overview, security intelligence modeling and research directions. *SN Computer Science*, 2(3):1–18. Publisher: Springer.

Sengupta, N. and Sil, J. (2020). *Intrusion Detection: A Data Mining Approach*. Springer Nature.

Thakkar, A. and Lohiya, R. (2020). A review of the advancement in intrusion detection datasets. *Procedia Computer Science*, 167:636–645. Publisher: Elsevier.

Thamilarasu, G. and Chawla, S. (2019). Towards deep-learning-driven intrusion detection for the internet of things. *Sensors*, 19(9):1977. Publisher: Multidisciplinary Digital Publishing Institute.

Wei, P., Li, Y., Zhang, Z., Hu, T., Li, Z., and Liu, D. (2019). An optimization method for intrusion detection classification model based on deep belief network. *IEEE Access*, 7:87593–87605. Publisher: IEEE.

Xiao, Y., Xing, C., Zhang, T., and Zhao, Z. (2019). An intrusion detection model based on feature reduction and convolutional neural networks. *IEEE Access*, 7:42210–42219. Publisher: IEEE.

Yang, H., Qin, G., and Ye, L. (2019). Combined Wireless Network Intrusion Detection Model Based on Deep Learning. *IEEE Access*, 7:82624–82632. Publisher: IEEE.

Zhang, H., Yu, X., Ren, P., Luo, C., and Min, G. (2019a). Deep adversarial learning in intrusion detection: A data augmentation enhanced framework. *arXiv preprint arXiv:1901.07949*.

Zhang, Y., Li, P., and Wang, X. (2019b). Intrusion detection for IoT based on improved genetic algorithm and deep belief network. *IEEE Access*, 7:31711–31722. Publisher: IEEE.