**Antecedentes**

La detección de tráfico de red malicioso en sistemas de detección de intrusiones (IDS) ha sido un desafío persistente, especialmente con la evolución de las amenazas que eluden los métodos basados en firmas. En 2018, Shenfield et al. (2018) propusieron un enfoque innovador que utiliza redes neuronales artificiales (ANN), adaptadas para la inspección profunda de paquetes. Este método se distinguió por ser no basado en firmas y auto-adaptativo, lo que le permitió identificar con precisión el tráfico maligno, como el shellcode, logrando una precisión promedio del 98% y una tasa de falsos positivos inferior al 2%. La investigación se motivó por la alta tasa de falsos positivos en herramientas convencionales, que a menudo clasificaban erróneamente archivos benignos, como DLLs de Windows Update, como amenazas. La capacidad de las ANN para capturar relaciones complejas y no lineales en los datos, sin necesidad de conocimiento previo del modelo de probabilidad subyacente, subraya su potencial para mejorar la utilidad de los IDS en la clasificación de tráfico de red, incluso en entornos simulados.

La evolución de las redes de telecomunicaciones ha hecho que la detección de anomalías en el tráfico sea cada vez más compleja debido a las propiedades dinámicas de los datos. En este sentido, Lebedev y Rzayev (2023) propusieron un método que busca optimizar la precisión de clasificación mediante la segmentación de muestras de datos de tráfico de red. La premisa central es que las características de los datos, como el volumen o la frecuencia de los mensajes, son tan determinantes como el algoritmo clasificador en sí para lograr indicadores cualitativos óptimos. El método implica la detección de puntos de cambio en las series temporales para dividir el flujo continuo de datos en segmentos homogéneos, asignando a cada uno el clasificador que demuestre el mejor rendimiento. Los experimentos realizados con el conjunto de datos NSL-KDD demostraron que esta estrategia puede mejorar la calidad general del procesamiento de la muestra en aproximadamente un 5%, evitando el efecto de los algoritmos más débiles en el resultado global y siendo menos intensivo en recursos que los enfoques de ensemble tradicionales.

Enfrentando el resurgimiento de ataques de escaneo por malware como WannaMine y Mirai, Jafarian et al. (2023) desarrollaron un mecanismo de defensa innovador para proteger redes empresariales contra el escaneo, tanto interno como externo. El fundamento de su enfoque es que la comunicación legítima entre dos máquinas se precede típicamente por una resolución DNS; por lo tanto, cualquier comunicación que no cumpla con esta política es marcada como un escaneo. Para contrarrestar escáneres sigilosos y adaptativos, la investigación introdujo la manipulación de los valores TTL (Time-to-Live) en las respuestas DNS, reduciendo drásticamente su validez (de 24 horas a unos pocos minutos) para limitar la capacidad de los atacantes de aprovechar los registros DNS en caché. Mediante simulaciones a gran escala utilizando conjuntos de datos de flujo de red del Laboratorio Nacional de Los Álamos, el método demostró ser altamente efectivo, ralentizando el éxito del escaneo hasta 20,000 veces y logrando precisiones superiores al 96% para escaneos internos y más del 98% para escaneos externos. Este enfoque también se mostró eficaz contra una nueva técnica de escaneo adaptativo basada en caché DNS, que había eludido métodos previos.

En el ámbito de la ciberseguridad, la detección temprana de ataques de PortScan es vital para mantener la integridad de la red. Kareem et al. (2023) propusieron un enfoque basado en Machine Learning que utiliza los algoritmos JRip y OneR para mejorar la precisión de la detección de estos ataques. Su investigación se centró en el desarrollo de una estrategia de selección de características híbrida que combina el filtrado por varianza y la razón de ganancia de información (IGR), lo cual es crucial para construir modelos de clasificación eficientes. Al aplicar este método al conjunto de datos CICIDS2017, lograron distinguir eficazmente el tráfico normal de los ataques de PortScan, con el algoritmo JRip alcanzando una precisión sobresaliente del 99.84%. Este estudio enfatiza que los algoritmos basados en reglas, como JRip y OneR, no solo son efectivos sino que también ofrecen una alta interpretabilidad, un aspecto fundamental en la seguridad de redes para entender el proceso de toma de decisiones del clasificador.

La proliferación de dispositivos del Internet de las Cosas (IoT) ha traído consigo un aumento en las ciberamenazas, haciendo esencial la implementación de sistemas de detección de intrusiones (IDS) robustos. Arabiat y Altayeb (2024) abordaron esta preocupación evaluando la capacidad de clasificadores de Machine Learning (ML) y Deep Learning (DL) para predecir ataques en entornos IoT. Su estudio propuso un modelo IDS que integra Random Forest (RF), Redes Neuronales Artificiales (ANN), Regresión Logística (LR) y Support Vector Machine (SVM) para detectar una variedad de ataques, incluyendo ARP\_poisoning, DOS\_SYN\_Hping y NMAP\_FIN\_SCAN. Utilizando el conjunto de datos RT-IoT2022 y la herramienta de minería de datos Orange3, el modelo RF alcanzó una precisión de clasificación del 99.9%, mientras que el modelo ANN logró un 99.8%. La alta precisión se atribuyó al uso de validación cruzada de 10 pliegues y a la reducción de datos mediante análisis discriminante lineal, lo que también ayudó a prevenir el sobreajuste. La investigación resalta la resiliencia, interpretabilidad y explicabilidad del RF en escenarios IoT con recursos limitados.

Para mejorar los sistemas de detección de intrusiones (IDS), es fundamental comprender las características específicas del tráfico de red malicioso. Al-Khazaali et al. (2025) llevaron a cabo un estudio de caso sobre las características del tráfico de escaneo de puertos generado por Nmap, una herramienta común de reconocimiento. La investigación identificó varios "Indicadores de Escaneo" (IoS), como la distribución de puertos de origen y destino, medidas estadísticas y atributos temporales, que pueden servir como características distintivas para la detección. Al utilizar Nmap y Wireshark en un entorno simulado, los autores demostraron que Nmap, por defecto, selecciona puertos de manera aleatoria, a diferencia de otras herramientas como Metasploit, que a menudo emplean patrones ascendentes. La capacidad de reconocer estas "huellas digitales" no solo permite identificar un escaneo, sino también la herramienta específica utilizada, lo que es crucial para que los analistas de ciberseguridad tomen decisiones más informadas y precisas.

Los entornos del Internet de las Cosas Médicas (IoMT) y el Internet Industrial de las Cosas (IIoT) enfrentan crecientes y complejos desafíos de ciberseguridad que exponen datos sensibles y operaciones críticas. Gueriani et al. (2025) introdujeron BiGAT-ID, un sistema de detección de intrusiones (IDS) basado en transformadores, diseñado para ofrecer una defensa robusta y de dominio cruzado. Este modelo híbrido integra unidades recurrentes bidireccionales con gating (BiGRU), redes de memoria a largo corto plazo (LSTM) y un mecanismo de atención multi-cabeza (MHA) para capturar dependencias temporales, modelar patrones secuenciales y mejorar la representación contextual de las características. Evaluado en los conjuntos de datos de referencia CICIoMT2024 y EdgeIIoTset, BiGAT-ID demostró una robustez excepcional con precisiones de detección del 99.13% y 99.34%, respectivamente. Además, el modelo exhibió una eficiencia en tiempo de ejecución notable, con tiempos de inferencia tan bajos como 0.0002 segundos por instancia en IoMT y 0.0001 segundos en escenarios IIoT, lo que lo hace idóneo para la detección de amenazas en tiempo real en entornos IoT heterogéneos y con recursos limitados.

Con el objetivo de fortalecer la protección de las redes, Guo et al. (2025) propusieron una tecnología dinámica de seguridad anti-mapeo de red que utiliza Modelos Ocultos de Markov (HMM) y redes de Memoria Larga a Corto Plazo (LSTM) para combatir el escaneo ilegal. Su modelo Bi-LSTM+Attention demostró ser particularmente efectivo, logrando una precisión del 98% en el conjunto de datos UNSW-NB15 y reduciendo la tasa de falsas alarmas en un 30% en comparación con los modelos LSTM tradicionales. La investigación resalta la importancia de los mecanismos de defensa inteligentes y la capacidad de los modelos para adaptarse dinámicamente a entornos de red complejos y cambiantes. Este enfoque avanzado es capaz de aprender y adaptarse automáticamente a nuevos patrones de amenazas, lo que es crucial para mantener capacidades de detección eficientes en un panorama de seguridad en constante evolución. Aunque el modelo presenta altos requisitos de recursos computacionales, sus ventajas significativas en la mejora de la precisión de detección justifican su implementación, y las pruebas se realizaron en un entorno de red simulado.

El Internet de las Cosas (IoT) ha revolucionado la vida humana, pero el crecimiento exponencial de sus dispositivos (proyectados en 55.7 mil millones para 2025) presenta desafíos significativos debido a sus limitaciones inherentes en recursos como el almacenamiento, la capacidad computacional y la batería. En respuesta, Kushwaha et al. (2025) realizaron una revisión exhaustiva de los Sistemas de Detección de Intrusiones (IDS) inteligentes, destacando el uso de Inteligencia Artificial (IA), Machine Learning (ML) y Deep Learning (DL) como soluciones efectivas para la seguridad en IoT. Identificaron desafíos clave como la complejidad computacional, la adaptabilidad en tiempo real y la eficiencia energética en la computación de borde (Edge Computing). Para abordar estas brechas, propusieron futuras direcciones de investigación, incluyendo IDS auto-evolutivos impulsados por IA, aprendizaje continuo y Explainable AI (XAI) para la colaboración entre humanos e IA, y el aprendizaje federado para una seguridad que preserve la privacidad. La revisión subraya la necesidad de enfoques adaptativos para asegurar el ecosistema IoT dinámico y en constante evolución.

En el contexto de la seguridad en redes Edge-IoT, Sahoo et al. (2026) introducen Choir-IDS, un marco de aprendizaje federado (FL) diseñado para mejorar la fidelidad y la explicabilidad en los sistemas de detección de intrusiones (IDS). Este sistema aprovecha la sinergia de múltiples modelos de Machine Learning y Deep Learning a través de "Neural Boosting Ensembles", lo que permite una detección robusta y escalable en entornos descentralizados. La investigación subraya la importancia de la fidelidad, que mide la precisión con la que un modelo representa la verdad fundamental de los incidentes de seguridad y clasifica correctamente las amenazas sin falsos positivos o negativos. El marco Choir-IDS se valida extensamente utilizando conjuntos de datos de referencia como UNSW-NB15 y CICIoT2023, y demuestra una notable mejora en el rendimiento de la detección (por ejemplo, una precisión de prueba del 94.44% en UNSW-NB15 y 96.09% en CICIoT2023), incluso frente a datos no independientes e idénticamente distribuidos (non-IID). La integración de herramientas de explicabilidad como LIME y SHAP mejora la transparencia y la confianza en las decisiones del modelo, mientras que el aprendizaje federado garantiza la privacidad y escalabilidad al mantener los datos en el dispositivo.

**Referencias**

Al-Khazaali, Z., Al-Ghabban, A., Al-Musawi, H., Sabah, A., & Al Mahdi, N. (2025). Characteristics of Port Scan Traffic: A Case Study Using Nmap. Journal of Engineering and Sustainable Development, 29(1).

Arabiat, A., & Altayeb, M. (2024). Enhancing internet of things security: Evaluating machine learning classifiers for attack prediction. International Journal of Electrical and Computer Engineering (IJECE), 14(5), 6036–6046.

Gueriani, A., Kheddar, H., Mazari, A. C., & Ghanem, M. C. (2025). A robust cross-domain IDS using BiGRU-LSTM-attention for medical and industrial IoT security. ICT Express.

Guo, M., Ma, D., Jing, F., Zhang, X., & Liu, H. (2025). Dynamic Anti-Mapping Network Security Using Hidden Markov Models and LSTM Networks Against Illegal Scanning. Informatica, 49(2), 207–220.

Jafarian, J. H., Abolfathi, M., & Rahimian, M. (2023). Detecting network scanning through monitoring and manipulation of DNS traffic. IEEE Access, 11, 20267–20283.

Kareem, M. I., Abood, M. J. K., & Ibrahim, K. (2023). Machine learning-based PortScan attacks detection using OneR classifier. Bulletin of Electrical Engineering and Informatics, 12(6), 3690–3696.

Kushwaha, J. P., Bhadauria, S., & Tapaswi, S. (2025). Unveiling IoT ecosystem security: A review of intelligent IDS, trends, challenges, and future directions. Computers and Electrical Engineering, 128, 110626.

Lebedev, I., & Rzayev, B. (2023). Segmentation of data when analyzing the state of telecommunication systems. Indonesian Journal of Electrical Engineering and Computer Science, 29(3), 1473–1479.

Sahoo, J. P., Kar, B., Abdelmoniem, A. M., & Chatzopoulos, D. (2026). Choir-IDS: A federated learning framework for fidelity-calibrated explainable intrusion detection system for edge-IoT networks. Information Fusion, 125, 103473.

Shenfield, A., Day, D., & Ayesh, A. (2018). Intelligent intrusion detection systems using artificial neural networks. ICT Express, 4(2), 95–99.