INTEGRAÇÃO DE TÉCNICAS DE MACHINE LEARNING AO SNORT PARA DETECÇÃO DE ATAQUES DDoS: UMA REVISÃO BIBLIOGRÁFICA

Autor: Felipe Luis Pereira Paulo; Coautores: Carlos José Nascimento, Alexandre de Paula, Paulo Ricardo Claro, Yam Kevim Claro, Willians Benedito Mendes Brito, Adriano Afonso de Almeida Carvalho

RESUMO

Os ataques de Distributed Denial of Service (DDoS) representam uma das principais ameaças à disponibilidade de serviços em redes de computadores, exigindo mecanismos de detecção cada vez mais adaptativos. Nesse contexto, os Sistemas de Detecção de Intrusão (IDS), como o Snort, apresentam elevada eficiência na identificação de ameaças conhecidas por meio de assinaturas, porém possuem limitações diante de ataques inéditos e variantes comportamentais. Este trabalho teve como objetivo analisar, por meio de uma revisão bibliográfica estruturada, de que forma a integração de técnicas de Machine Learning ao Snort pode contribuir para o aprimoramento da detecção de ataques DDoS. A pesquisa foi conduzida nas bases IEEE Xplore, ACM Digital Library, ScienceDirect e Google Scholar, considerando publicações entre 2018 e 2025, complementadas por documentação técnica da Cisco/Talos. Após aplicação dos critérios de inclusão e exclusão, foram selecionados nove estudos para análise qualitativa comparativa. Os resultados indicam que abordagens híbridas, combinando inspeção por assinaturas com algoritmos de aprendizado de máquina, apresentam maior capacidade de adaptação a padrões desconhecidos, redução das taxas de falsos positivos e melhoria na detecção de ataques em ambientes dinâmicos, como redes definidas por software (SDN) e Internet das Coisas (IoT). Entretanto, observou-se que grande parte das avaliações ainda é realizada em ambientes experimentais, utilizando diferentes datasets e métricas, dificultando comparações diretas e a generalização dos resultados para cenários reais. Conclui-se que a integração entre Snort e Machine Learning representa uma estratégia promissora para fortalecer sistemas de detecção de intrusão, embora sua consolidação dependa de pesquisas com maior padronização metodológica, validação em tráfego real e adoção de técnicas que ampliem a interpretabilidade dos modelos.

Palavras-chave: Detecção de intrusão; Inteligência artificial; Segurança de redes.

1 INTRODUÇÃO

Os ataques de Distributed Denial of Service (DDoS) permanecem entre as principais ameaças à disponibilidade de serviços em redes de computadores, explorando o envio massivo de tráfego para comprometer servidores, aplicações e infraestruturas de comunicação. A expansão de ambientes em nuvem, dispositivos de Internet das Coisas (IoT) e arquiteturas distribuídas ampliou a complexidade do tráfego de rede, tornando mais desafiadora a identificação de comportamentos maliciosos em meio ao tráfego legítimo.

Nesse contexto, os Sistemas de Detecção de Intrusão (IDS), como o Snort, desempenham papel fundamental na proteção de redes por meio da inspeção baseada em assinaturas. Entretanto, essa abordagem apresenta limitações na identificação de ataques inéditos ou variantes de ameaças conhecidas, podendo elevar as taxas de falsos positivos e falsos negativos. Estudos recentes apontam que a integração de técnicas de Machine Learning aos IDS possibilita maior capacidade de adaptação, detecção de anomalias e melhoria no desempenho da identificação de ataques DDoS, especialmente em ambientes dinâmicos e de grande volume de tráfego.

Diante desse cenário, o presente trabalho tem como objetivo analisar, por meio de uma revisão bibliográfica estruturada, de que forma a integração de técnicas de Machine Learning ao Snort pode contribuir para o aprimoramento da detecção de ataques DDoS, considerando seu impacto na acurácia, na redução de falsos positivos e na adaptação a diferentes cenários de rede.

2 MATERIAL E MÉTODOS

Este estudo caracteriza-se como uma revisão bibliográfica estruturada, de natureza qualitativa e descritiva, conduzida com o objetivo de analisar a integração de técnicas de Machine Learning ao sistema de detecção de intrusão Snort para o aprimoramento da detecção de ataques Distributed Denial of Service (DDoS). As buscas foram realizadas nas bases IEEE Xplore, ACM Digital Library, ScienceDirect e Google Scholar, complementadas por documentação técnica oficial da Cisco/Talos para contextualização tecnológica do Snort e do SnortML.

Foram consideradas publicações disponibilizadas entre 2018 e 2025, utilizando combinações dos termos *Snort*, *SnortML*, *Machine Learning*, *Deep Learning*, *Support Vector Machine (SVM)* e *DDoS*, associados por operadores booleanos. Como critérios de inclusão, selecionaram-se estudos que abordassem sistemas de detecção de intrusão, integração entre IDS e técnicas de aprendizado de máquina, além de apresentarem resultados quantitativos ou métricas de desempenho. Foram excluídos trabalhos exclusivamente conceituais, estudos duplicados e publicações sem relação direta com o problema investigado.

O processo de seleção compreendeu três etapas: identificação inicial dos estudos, análise de títulos, resumos e palavras-chave, seguida da leitura integral dos trabalhos elegíveis. Dos 28 estudos inicialmente identificados, nove atenderam aos critérios de inclusão, sendo três considerados o núcleo principal da análise por apresentarem maior aderência ao tema.

A extração dos dados foi realizada por meio de uma matriz padronizada contendo informações sobre objetivos, algoritmos empregados, datasets utilizados, métricas de avaliação, resultados obtidos e limitações dos estudos. Posteriormente, realizou-se análise qualitativa comparativa, considerando indicadores como acurácia, precisão, *recall*, F1-score, taxas de falsos positivos e falsos negativos, bem como aspectos relacionados à adaptabilidade dos modelos e à aplicação em ambientes reais de rede.

3 RESULTADOS E DISCUSSÃO

A análise dos nove estudos selecionados evidenciou uma tendência consistente na literatura: a integração de técnicas de Machine Learning aos Sistemas de Detecção de Intrusão (IDS), especialmente ao Snort, proporciona melhorias na identificação de ataques DDoS quando comparada às abordagens exclusivamente baseadas em assinaturas. Os trabalhos analisados indicam aumento da acurácia, redução das taxas de falsos positivos e maior capacidade de adaptação a padrões de tráfego desconhecidos, principalmente em ambientes caracterizados por elevado volume de dados, como redes definidas por software (SDN) e Internet das Coisas (IoT).

Autor/Ano	Abordagem	Principais resultados
Muhammad et al. (2020)	Rede Neural + Seleção de atributos	97,76% de acurácia utilizando o dataset UNSW-NB15
El Aeraj e Leghris (2024)	Snort + SVM	99% de precisão, 100% de *recall* e baixa taxa de falsos positivos

Tabela 1 – Principais estudos selecionados e resultados quantitativos

Os resultados demonstram que modelos híbridos conseguem complementar as limitações da detecção por assinaturas ao identificar padrões anômalos não previamente conhecidos. Entretanto, a literatura também destaca desafios relacionados à dependência da qualidade dos datasets, ao pré-processamento dos dados, ao custo computacional do treinamento dos modelos e à escassez de avaliações em ambientes reais de produção.

Critério	Snort Tradicional	Snort + Machine Learning
Detecção de ataques conhecidos	Alta	Alta
Detecção de ataques desconhecidos	Limitada	Elevada
Falsos positivos	Maior ocorrência	Redução observada na literatura
Adaptabilidade	Baixa	Alta

Tabela 2 – Comparação entre abordagens de detecção

A comparação entre os estudos confirma que a adoção de arquiteturas híbridas representa uma alternativa promissora para o fortalecimento da segurança de redes. Contudo, os resultados apresentados na literatura ainda são predominantemente obtidos em cenários experimentais, indicando a necessidade de novas pesquisas que validem essas soluções em ambientes operacionais reais e utilizando critérios padronizados de avaliação.

4 CONCLUSÃO

A revisão bibliográfica evidenciou que a integração de técnicas de Machine Learning ao Snort representa uma abordagem promissora para o aprimoramento da detecção de ataques DDoS. Os estudos analisados indicam que arquiteturas híbridas, ao combinarem inspeção baseada em assinaturas com modelos de aprendizado de máquina, podem aumentar a acurácia da detecção, reduzir taxas de falsos positivos e ampliar a capacidade de identificar padrões de tráfego desconhecidos em ambientes dinâmicos.

Entretanto, a literatura também demonstra que esses resultados ainda estão concentrados, em sua maioria, em cenários experimentais, utilizando diferentes datasets, métricas de avaliação e configurações, o que dificulta comparações diretas e limita a generalização dos resultados para ambientes reais de produção.

Conclui-se que a integração entre Snort e Machine Learning possui potencial para fortalecer os sistemas de detecção de intrusão, mas sua consolidação depende de estudos mais padronizados, reprodutíveis e validados em tráfego real. Como perspectivas futuras, recomenda-se a realização de experimentos em ambientes operacionais, a adoção de critérios uniformes de avaliação e a incorporação de técnicas de Inteligência Artificial Explicável (XAI), visando aumentar a transparência, a auditabilidade e a confiança nos modelos empregados.

REFERÊNCIAS

CISCO. *SnortML: Machine Learning-based Exploit Detection*. Cisco Secure Firewall Documentation, 2024.

EL AERAJ, O.; LEGHRIS, C. *Analysis of the SNORT intrusion detection system using machine learning*. International Journal of Information Science and Technology, 2024.

MUHAMMAD, A. W.; FOOZY, C. F. M.; AZHARI, A. *Machine Learning-Based Distributed Denial of Service Attack Detection on Intrusion Detection System Regarding to Feature Selection*. International Journal of Artificial Intelligence Research, v. 4, n. 1, p. 27–35, 2020.

RAMZAN, M. et al. *Distributed Denial of Service Attack Detection in Network Traffic Using Deep Learning Algorithm*. Sensors, v. 23, n. 20, 2023.

SHIRSATH, V. A. et al. *SYNTROPY: TCP SYN DDoS attack detection for Software Defined Network based on Rényi entropy*. Computer Networks, v. 244, 2024.