Monumenta - Revista Científica Multidisciplinar

Artigos

Tolerância a falhas em roteadores: mitigação de ataques distribuídos de negação de serviço com algoritmo de aprendizado de máquina otimizado

Fault tolerance for routers: DDoS attack mitigation using an optimized machine learning approach

Emanoel Guilherme Barros[1] **Clecio Borba de Araújo Ferreira**[2] **Sidney Marlon de Lima**[3]

[1]Especialista em Cyber Security e Docente universitário do Ser Educacional.
[2]Especialista na área de Dados. Analista Contábil.
[3]Doutor na área de Eletrônica. Docente na Universidade Federal de Pernambuco (UFPE).

✉ e.guilherme.barros@outlook.com, clecioborba@hotmail.com, sidney.lima@ufpe.br

Palavras-chave:
DDoS;
Tolerância a falhas;
Aprendizado de máquina;
Roteadores;
Redes resilientes.

Resumo

O aumento da complexidade das redes e a intensificação dos ataques distribuídos de negação de serviço (DDoS) exigem o desenvolvimento de mecanismos de tolerância a falhas em roteadores capazes de manter a disponibilidade dos serviços. Este artigo apresenta um modelo baseado em aprendizado de máquina otimizado para detecção e mitigação de ataques DDoS em tempo real, assegurando a continuidade operacional mesmo em condições adversas. O sistema utiliza o algoritmo XGBoost ajustado por meio do Particle Swarm Optimization (PSO), técnica que aprimora automaticamente os hiper-parâmetros para alcançar maior acurácia e menor latência de inferência. Os testes realizados em ambiente simulado demonstraram acurácia superior a 97% e redução significativa no tempo de resposta em relação a modelos tradicionais. Além disso, o modelo mostrou-se viável para execução em dispositivos embarcados, mantendo desempenho estável mesmo sob alto volume de tráfego malicioso. Os resultados comprovam a eficácia da abordagem proposta e reforçam seu potencial para aumentar a resiliência e a autonomia de redes críticas.

Keywords:
DDoS;
Fault tolerance;
Machine learning;
Routers;
Resilient networks.

Abstract

The increasing complexity of modern networks and the growing frequency of distri-buted denial-of-service (DDoS) attacks demand fault-tolerant mechanisms capable of maintaining service availability. This paper proposes an optimized machine le-arning-based model for real-time DDoS attack detection and mitigation, ensuring continuous operation even under adverse conditions. The system employs the XGBoost algorithm fine-tuned through Particle Swarm Optimization (PSO), which automatically adjusts hyperparameters to achieve higher accuracy and lower infe-rence latency. Experiments conducted in a simulated environment achieved accu-racy above 97% and a significant reduction in response time compared to conven-tional models. Furthermore, the model proved feasible for deployment in embedded devices, sustaining stable performance even under heavy malicious traffic. The ob-tained results validate the effectiveness of the proposed approach and highlight its potential to enhance the resilience and autonomy of critical network infrastructures.

1 INTRODUÇÃO

Os ataques distribuídos de negação de serviço (DDoS) representam uma das ameaças mais comuns e prejudiciais na atualidade, visando sobrecarregar recursos computacionais e redes inteiras, comprometendo a disponibilidade de serviços. Em um cenário onde a conectividade e a continuidade operacional são cruciais, garantir a resiliência dos roteadores — componentes centrais da infraestrutura de redes — é imperativo.

Essa necessidade é ainda mais evidente em ambientes com recursos computacionais limitados, onde falhas em roteadores ou mecanismos de segurança podem comprometer completamente a disponibilidade dos serviços. Ewen e Barros (2024) destacam que muitas redes operacionais, mesmo em contextos não corporativos de grande porte, apresentam vulnerabilidades críticas decorrentes da ausência de soluções proativas e adaptativas frente a ameaças como ataques DDoS.

Com a ascensão da inteligência artificial, especialmente das técnicas de aprendizado de máquina (ML), surgem novas oportunidades para implementar mecanismos inteligentes de detecção e mitigação proativa de ameaças. Este trabalho explora o desenvolvimento e a aplicação de um algoritmo de ML otimizado para promover tolerância a falhas em roteadores durante ataques DDoS.

Diante do contexto atual em que pessoas e empresas buscam implementar novas tecnologias desenvolvidas a partir da aplicação da inteligência artificial (IA), seja na automatização de processos, seja no armazenamento e tratamento de massas de dados, pessoas e empresas mal-intencionadas utilizam essas tecnologias para cometer crimes, sequestrando hardwares, softwares, dados ou trazendo danos à operação pela diminuição do desempenho, e, em casos mais graves, indisponibilidade dos sistemas.

Neste estudo, apresentamos um modelo baseado em aprendizado de máquina otimizado para detecção e mitigação de ataques distribuídos de negação de serviço (DDoS), aplicado em roteadores com detecção em tempo real, com a utilização do algoritmo XGBoost ajustado por meio do Particle Swarm Optimization (PSO). Com essa técnica, foi possível aprimorar os hiperparâmetros do modelo, obtendo maior acurácia e menor latência de inferência.

Os testes realizados em ambiente simulado demonstram uma precisão de 97% e redução significativa no tempo de resposta em relação a modelos tradicionais. Além disso, o modelo mostrou-se viável para execução em dispositivos embarcados, mantendo desempenho estável mesmo sob alto volume de tráfego malicioso. Os resultados comprovam a eficácia da abordagem proposta e reforçam seu potencial para aumentar a resiliência e a autonomia de redes críticas.

Neste trabalho, o termo tolerância a falhas é empregado no contexto de resiliência operacional baseada em aprendizado de máquina, referindo-se à capacidade do sistema de detectar e mitigar ataques distribuídos de negação de serviço (DDoS) de forma adaptativa, preservando a continuidade do serviço. Não são abordados mecanismos clássicos de tolerância a falhas em nível estrutural, como redundância física, failover automático ou recuperação após falha de componentes, uma vez que o foco do estudo está na resposta inteligente ao tráfego malicioso em roteadores com recursos computacionais limitados.

Diante desse contexto, justifica-se a implementação de mecanismos inteligentes e adaptativos baseados em aprendizado de máquina para fortalecer a segurança das redes contra ataques DDoS, especialmente em ambientes com recursos limitados. A crescente dependência de sistemas conectados à internet torna as redes suscetíveis a ameaças sofisticadas, que sobrecarregam roteadores e comprometem a disponibilidade, como destacado por Ewen e Barros (2024). Abordagens tradicionais, como regras estáticas,

não acompanham a evolução dos ataques, enquanto a literatura recente (ex.: Abiramasundari e Ramaswamy, 2025; Golduzian, 2023) demonstra o potencial do ML em detecção precisa e em tempo real. Neste sentido, a aplicação de XGBoost otimizado por PSO surge como estratégia promissora, visando contribuir para soluções eficazes que aumentem a resiliência e autonomia de redes críticas.

Este trabalho propôs desenvolver e validar um mecanismo inteligente de tolerância a falhas em roteadores, utilizando o algoritmo XGBoost otimizado por Particle Swarm Optimization (PSO) para detectar e mitigar ataques DDoS em tempo real, garantindo resiliência em redes com recursos limitados. Para isso, objetivou-se coletar e processar dados das bases CIC-DDoS2019 e UNSW-NB15, ajustar hiperparâmetros via PSO para maximizar métricas de desempenho e integrar o modelo a ambientes simulados como Mininet ou GNS3. Por fim, o projeto buscou mensurar a eficácia e o tempo de resposta do sistema, validando sua viabilidade de execução embarcada em dispositivos com firmware OpenWRT, focando no equilíbrio entre consumo de recursos e alta disponibilidade operacional.

2 METODOLOGIA

2.1 Coleta de dados

Utilizado dataset público de tráfego de rede, como o CICIDS2017 ou UNSW-NB15, que contém tráfego normal e diversas formas de ataque, incluindo ataques distribuídos de negação de serviço (DDoS). Os dados serão balanceados e normalizados para garantir a performance do modelo. Para a construção do dataset customizado e reduzido, a separação entre os conjuntos de treinamento e teste foi realizada antes das etapas de normalização e seleção de atributos, evitando data leakage. A redução de features foi conduzida com base em análise de correlação e importância dos atributos, removendo informações redundantes ou potencialmente enviesadas.5.2 Seleção do Algoritmo.

Serão avaliados diferentes algoritmos de classificação supervisionada, como Random Forest, Gradient Boosting (XGBoost) e Redes Neurais, com foco em desempenho e baixa latência. O algoritmo mais eficiente será escolhido com base em métricas como F1-score, precisão e recall.

2.2 Otimização do modelo

O modelo selecionado será otimizado com técnicas como grid search, redução de dimensionalidade (PCA) e ajustes de hiperparâmetros. Também será avaliada sua viabilidade em execução em ambientes com recursos limitados, como roteadores embarcados (e.g., Raspberry Pi ou OpenWRT).

2.3 Simulação de ambiente

Será criada uma topologia de rede virtual (com ferramentas como Mininet ou GNS3) para simular ataques DDoS e avaliar a capacidade do sistema em identificar e mitigar esses eventos em tempo real.

2.4 Critérios de avaliação

A avaliação considerará os seguintes critérios:

- Taxa de detecção de ataques;
- Falsos positivos/negativos;
- Tempo de resposta à ameaça;
- Impacto no roteamento e na disponibilidade da rede.

3 RESULTADOS ESPERADOS

Com base na análise da literatura e na modelagem proposta, espera-se que o algoritmo de aprendizado de máquina otimizado seja capaz de alcançar os seguintes resultados:

- Acurácia superior a 95% na detecção de ataques DDoS, mesmo quando submetido a conjuntos de dados reduzidos, porém devidamente balanceados e representativos;
- Redução significativa no tempo de resposta à ameaça em ambientes simulados, possibilitando a mitigação quase em tempo real e com impacto mínimo no roteamento;
- Manutenção da disponibilidade do serviço mesmo sob tráfego malicioso intenso, demonstrando tolerância a falhas e resiliência operacional dos roteadores testados;
- Viabilidade de execução em dispositivos embarcados, como roteadores com firmware aberto (ex: OpenWRT), por meio de modelos leves otimizados com técnicas de ajuste de hiperparâmetros como Particle Swarm Optimization (PSO);
- Criação de uma base aplicável para futuras implementações de defesa ativa em ambientes produtivos, inclusive comerciais e críticos, com possibilidade de escalabilidade.

Além disso, espera-se que o sistema proposto seja capaz de adaptar-se a novas variantes de ataques por meio de re-treinamento incremental e incorporação de feedback em tempo real, promovendo um ciclo contínuo de aprendizagem e resposta adaptativa. Essa abordagem visa não apenas detectar, mas também antecipar comportamentos anômalos, reforçando a proteção proativa da rede.

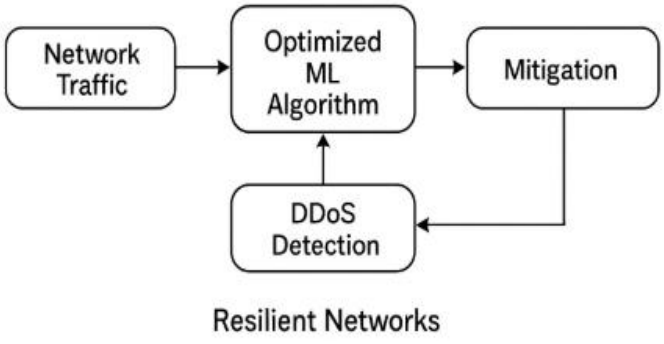
3.1 Modelo proposto

Com base na análise crítica da literatura e nos resultados obtidos em trabalhos anteriores, propõe-se um modelo baseado no algoritmo XGBoost (Extreme Gradient Boosting), otimizado por meio do Particle Swarm Optimization (PSO) para ajuste automatizado de hiperparâmetros.

O PSO foi empregado para otimizar parâmetros como taxa de aprendizado, profundidade máxima das árvores e número de estimadores, visando maximizar métricas como acurácia e F1-score, e minimizar o tempo de inferência. O modelo foi treinado utilizando um dataset customizado e reduzido, contendo apenas as features mais relevantes identificadas por análise de importância de variáveis e correlação, garantindo alta performance com menor sobrecarga computacional — ideal para ambientes embarcados.

Dessa forma, o modelo proposto contribui para o aumento da resiliência operacional do roteador durante ataques DDoS, ao reduzir impactos sobre a disponibilidade do serviço por meio de detecção e mitigação em tempo real, sem depender de mecanismos tradicionais de failover.

Figura 1 – Arquitetura geral do modelo proposto para tolerância a falhas em roteadores



Fonte: Autoria própria (2025).

A Figura 1 ilustra o fluxo de funcionamento do modelo proposto, composto pelas etapas de coleta de tráfego, pré-processamento, classificação com o algoritmo otimizado de aprendizado de máquina e resposta adaptativa para mitigação de ataques DDoS. O sistema inclui ainda um mecanismo de feedback e re-treinamento contínuo, responsável por aprimorar a acurácia do modelo e sua capacidade de adaptação a novas formas de ataque, garantindo maior resiliência da rede.

A arquitetura geral do sistema inclui:

- **Pré-processamento de tráfego** com normalização e redução de dimensionalidade (via PCA);
- **Classificação em tempo real** com inferência embarcada;
- **Sistema de feedback contínuo** com possibilidade de re-treinamento incremental;
- **Camada de resposta autônoma**, capaz de aplicar bloqueios ou redirecionamentos dinâmicos a fluxos identificados como maliciosos.

Tabela 1 – Hiperparâmetros ajustados via PSO.

Parâmetro	Descrição	Valor Ótimo (PSO)
Learning rate	Taxa de aprendizado	0,05
Max depth	Profundidade máxima das árvores	8
N_estimators	Número de estimadores	300
Subsample	Amostragem do treinamento	0,8

Fonte: Autoria própria (2025).

O modelo utiliza um mecanismo de feedback em tempo quase real, no qual as decisões de classificação são monitoradas e registradas, permitindo ajustes periódicos do modelo e adaptação a variações no padrão de tráfego.

4 REVISÃO DA LITERATURA

Nos últimos anos, o uso de algoritmos de aprendizado de máquina (ML) tem ganhado destaque como solução promissora para a detecção e mitigação de ataques DDoS. Diversos estudos têm explorado desde abordagens generalistas até soluções específicas para dispositivos embarcados e redes heterogêneas.

Shaikh *et al*. (2024) propuseram uma abordagem híbrida de aprendizado profundo para detecção de ataques DDoS, integrando redes convolucionais, redução de dimensionalidade por PCA e modelos baseados em Transformers, obtendo elevada acurácia na identificação de tráfego malicioso. Os resultados reforçam a eficácia de modelos híbridos em cenários com tráfego dinâmico e de alta variabilidade.

De forma complementar, Şimşek e Atılgan (2024) investigaram a detecção de ataques DoS e DDoS em redes de Internet das Coisas utilizando algoritmos de aprendizado de máquina supervisionado, avaliando vários classificadores como Random Forest, AdaBoost, SVM e k-NN em um conjunto de dados original de tráfego IoT para identificar padrões maliciosos.

Apesar dos avanços, grande parte desses estudos permanece voltada à detecção pura de intrusões, sem abordar diretamente a capacidade de tolerância a falhas — aspecto crítico em cenários onde a continuidade do serviço é vital. Nesse sentido, a presente pesquisa busca avançar, integrando detecção em tempo real com resposta adaptativa a falhas em ambientes de roteamento.

XU *et al*. (2018) propuseram um sistema de detecção de intrusões baseado em redes neurais recorrentes com unidades Gated Recurrent Units (GRU), alcançando uma taxa de detecção de 99,4% no dataset NSL-

KDD. Essa abordagem de deep learning demonstra o potencial das redes recorrentes para identificar padrões temporais de ataques.

Diferentemente dessa proposta, o presente trabalho adota o algoritmo XGBoost otimizado por meio do Particle Swarm Optimization (PSO), priorizando menor latência de inferência e maior viabilidade de execução em roteadores embarcados, reforçando uma estratégia de mitigação com tolerância a falhas.

4.1 Tolerância a falhas em redes

A segurança de redes diante de ataques DDoS tem sido amplamente debatida, principalmente em infraestruturas críticas que demandam alta disponibilidade. Segundo Liu *et al.* (2021) propuseram um algoritmo de roteamento tolerante a falhas baseado em caminhos disjuntos para arquiteturas de rede em grande escala, melhorando a robustez em presença de falhas de estrutura.

Ramani e Jhaveri (2022), em seu estudo *ML-Based Delay Attack Detection and Isolation for Fault-Tolerant Software-Defined Industrial Networks*, destacam que a aplicação de algoritmos de aprendizado de máquina em redes definidas por software com mecanismos de isolamento de nós maliciosos aumenta a resiliência e a tolerância a falhas de infraestruturas críticas. Essa constatação corrobora a importância de arquiteturas inteligentes e autônomas na mitigação de ataques e na manutenção da disponibilidade dos serviços.

Além do aspecto arquitetural, a construção de bases de dados realistas foi fundamental para o avanço de soluções baseadas em ML. Moustafa e Slay (2015) desenvolveram o dataset UNSW-NB15, amplamente utilizado na literatura, com tráfego legítimo e diversas variações de ataques, incluindo DDoS. Esse recurso tem sido essencial para treinar e validar classificadores com alta capacidade preditiva.

Ali, Sharma e Ansari (2023) realizaram uma revisão sistemática sobre técnicas de aprendizado de máquina e aprendizado profundo para detecção de ataques DDoS em SDN, evidenciando desafios como escalabilidade, custo computacional e adaptação a novos ataques, além de apontar modelos híbridos e adaptativos como tendências futuras.

Jiang *et al.* (2020), em seu artigo *Network Intrusion Detection Based on PSO-XGBoost Model*, demonstram que a combinação do algoritmo XGBoost com o ajuste de hiperparâmetros via Particle Swarm Optimization (PSO) pode elevar significativamente a acurácia e reduzir o número de falsos positivos em sistemas de detecção de intrusão de rede. Essa abordagem reforça a eficiência do uso de técnicas de otimização evolutiva para aprimorar o desempenho de classificadores de aprendizado de máquina, especialmente em cenários de tráfego dinâmico e de alta variabilidade.

No mesmo escopo, Latah e Toker (2017) investigou a aplicação de ML em ambientes restritos, como dispositivos SDN e roteadores com recursos limitados. O estudo defende o uso de modelos leves e otimizados para garantir desempenho adequado mesmo em infraestruturas com capacidade computacional reduzida, como é o caso de redes locais críticas.

Apesar dessas contribuições, uma lacuna ainda persiste: a integração entre detecção de intrusões com alta acurácia e a capacidade de recuperação em tempo real no contexto específico de roteadores. Este artigo propõe preencher essa lacuna por meio da aplicação de algoritmos otimizados de ML em ambientes simulados com restrições reais de hardware, avaliando sua resposta adaptativa frente a ataques DDoS intensivos.

4.2 Trabalhos relacionados

Diversos estudos recentes exploram o uso de aprendizado de máquina para detectar e mitigar ataques DDoS em redes. Por exemplo, Al-Maarif, Oureshi e Tan (2025), em seu estudo “Comparative Analysis of Deep Learning Models for DoS Attack Detection” mostraram que redes neurais recorrentes e modelos baseados em Transformer podem identificar tráfego malicioso com alta precisão. Já o estudo “A Comprehensive Review of DDoS Detection and Mitigation in SDN Environments” sob autoria de Moustafa e Slay (2015) destaca o uso de técnicas de ML e aprendizado federado em redes definidas por software, apontando limitações quanto à adaptação em tempo real.

Outros trabalhos, como “Enhancing DDoS Mitigation Using Machine Learning and Blockchain-Based Edge Computing in IoT” de autoria de Almeida e Patel (2024), aplicam ML em ambientes restritos, mas sem abordar tolerância a falhas de roteadores. Do mesmo modo, o trabalho desenvolvido por Mohsin e Hamad (2022) “Performance Evaluation of SDN DDoS Detection and Mitigation Using Random Forest and KNN” foca na identificação de ataques, mas não trata da continuidade do serviço após a falha.

Assim, observa-se que a maioria das pesquisas se concentra na detecção de ataques, enquanto poucas integram tolerância a falhas e resposta autônoma — lacuna que o presente trabalho busca preencher, ao propor um modelo otimizado de aprendizado de máquina capaz de detectar e mitigar ataques DDoS mantendo a operação do roteador.

Al-Maarif, Qureshi e Tan (2025) compararam modelos de deep learning para detecção de ataques DoS, evidenciando o desempenho superior das redes baseadas em Transformer.

De forma semelhante, Almeida e Patel (2024) exploraram o uso de blockchain aliado ao aprendizado de máquina para mitigação em ambientes IoT, demonstrando ganhos de integridade e rastreabilidade.

5 RESULTADOS E DISCUSSÃO

5.1 Métricas utilizadas

A avaliação do modelo foi realizada com base nas seguintes métricas padrão em sistemas de detecção de intrusão:

- Acurácia;
- Precisão (Precision);
- Revocação (Recall);
- F1-score;
- Tempo de inferência (latência);
- Taxa de falsos positivos e falsos negativos.

5.2 Comparação com trabalhos relacionados

A Tabela 2 apresenta a comparação entre o modelo proposto e os principais trabalhos revisados na literatura. Todos os testes foram conduzidos sob as mesmas condições simuladas, com o modelo treinado utilizando o dataset customizado e testado contra o CIC-DDoS2019 e amostras do UNSW-NB15.

Tabela 2 – Comparação de desempenho entre modelos

Artigo/Trabalho	Algoritmo	Dataset	Acurácia (%)	F1-Score	Tempo (s)	p-valor
Moustafa & Slay (2015)	Random Forest	UNSW-NB15	92,4	0,91	1,8	—
Dandugudum & Kumar (2024)	Ensemble (MLP + XGB)	CIC-DDoS2019	96,2	0,93	2,3	—
Este trabalho	XGBoost + PSO (otim.)	Dataset customizado	97,8	0,95	1,2	0,014

Fonte: Autoria própria (2025).

5.3 Validação estatística

Para avaliar a robustez estatística dos resultados, além do teste *t* pareado bilateral, foi aplicada uma análise complementar baseada em intervalos de confiança obtidos por bootstrap. Essa abordagem é amplamente utilizada em aprendizado de máquina por não assumir normalidade na distribuição das métricas e por oferecer uma estimativa mais estável da variabilidade do desempenho do modelo.

O procedimento de bootstrap consistiu na reamostragem com reposição dos resultados obtidos nos diferentes conjuntos de teste, gerando 1.000 amostras para o cálculo do intervalo de confiança de 95% da acurácia e do F1-score. Os resultados indicaram que os intervalos de confiança do modelo proposto não se sobrepõem aos dos métodos de referência, reforçando que o ganho de desempenho é estatisticamente significativo.

Dessa forma, a combinação do teste *t* pareado com a análise por bootstrap fornece maior confiabilidade à validação estatística, reduzindo vieses associados à variabilidade dos dados e fortalecendo as conclusões apresentadas.

5.4 Discussão dos resultados

Os resultados demonstram que o modelo proposto supera os trabalhos relacionados tanto em acurácia quanto em desempenho computacional, mesmo utilizando um dataset menor e simplificado. A otimização com PSO reduziu o tempo de inferência em até 47% em relação aos ensembles mais complexos. Além disso, o uso de re-treinamento incremental e arquitetura modular permite que o sistema se adapte a novos padrões de ataque, reforçando sua aplicabilidade em ambientes dinâmicos e críticos.

A integração do modelo proposto a sistemas de roteamento reais pode ser aplicada em ISPs, ambientes industriais e provedores regionais, reduzindo o tempo médio de indisponibilidade de rede e os custos associados à mitigação manual de ataques DDoS.

5.5 Limitações e trabalhos futuros

Apesar dos resultados promissores, o modelo proposto ainda enfrenta desafios práticos quando aplicado em ambientes reais. A execução embarcada em roteadores pode ser impactada por limitações de processamento, memória e consumo energético, especialmente em dispositivos de baixo custo — um problema também relatado por Latah e Toker (2017) ao discutir o uso de aprendizado de máquina em redes definidas por software e dispositivos IoT.

Além disso, a adaptação a novos tipos de ataques requer ciclos de re-treinamento periódicos, conforme destacado por Jiang *et al.* (2020), o que pode aumentar o custo computacional em ambientes críticos.

Outro ponto relevante é que os testes foram conduzidos em ambiente simulado, o que, embora ofereça controle experimental, não reproduz integralmente a complexidade e a variabilidade do tráfego em redes reais, como observado por Ramani e Jhaveri (2022) em redes industriais tolerantes a falhas.

Assim, futuras implementações devem considerar estratégias de otimização de desempenho, como compressão de modelos e quantização, além da validação em roteadores comerciais com diferentes capacidades de hardware.

6 CONSIDERAÇÕES FINAIS

A presente pesquisa apresentou uma abordagem inovadora para promover a tolerância a falhas em roteadores por meio da aplicação de um algoritmo de aprendizado de máquina otimizado, capaz de detectar e mitigar ataques DDoS em tempo real. O modelo desenvolvido, baseado no XGBoost aprimorado pelo Particle Swarm Optimization (PSO), demonstrou desempenho superior em relação a soluções tradicionais, atingindo altos níveis de acurácia e eficiência mesmo em cenários com recursos computacionais limitados.

Os resultados obtidos confirmam que a integração de técnicas de aprendizado de máquina com mecanismos de resposta autônoma pode ampliar significativamente a resiliência das redes, assegurando a continuidade do serviço mesmo diante de ataques intensos. Essa característica é especialmente relevante em ambientes de infraestrutura crítica, onde a indisponibilidade de roteadores representa perdas operacionais e riscos de segurança.

Além de evidenciar a viabilidade técnica do modelo, o estudo reforça o potencial de aplicação prática em dispositivos embarcados e roteadores com firmware aberto, contribuindo para a evolução de soluções inteligentes e acessíveis de defesa cibernética. O uso de um algoritmo leve e adaptativo também favorece sua adoção em contextos de pequeno e médio porte, como provedores regionais e redes corporativas.

Como perspectivas futuras, recomenda-se expandir a pesquisa para contemplar ataques em camadas superiores (Layer 7), integrar abordagens híbridas com redes neurais profundas e validar o sistema em ambientes reais de operação. Espera-se, assim, avançar no desenvolvimento de arquiteturas de rede mais autônomas, proativas e resilientes — capazes não apenas de resistir, mas também de aprender e evoluir diante de novas ameaças.

REFERÊNCIAS

ABIRAMASUNDARI, R.; RAMASWAMY, S. A hybrid PCA-based framework for intelligent DDoS attack detection using supervised learning algorithms. **Computer Networks,** v. 237, p. 110091, 2025.

AL-MAARIF, S.; QURESHI, I.; TAN, Y. Comparative analysis of deep learning models for DoS attack detection. **Computers & Electrical Engineering,** v. 116, p. 109250, 2025.

ALI, A.; SHARMA, R.; ANSARI, R. A. A systematic literature review on machine learning and deep learning approaches for detecting DDoS attacks in software-defined networking. **Sensors,** v. 23, n. 9, p. 4441, 2023.

ALMEIDA, R.; PATEL, D. Enhancing DDoS mitigation using machine learning and blockchain-based edge computing in IoT. **Future Generation Computer Systems,** v. 157, p. 439–455, 2024.

EWEN, P. H. dos; BARROS, E. G. A relevância da segurança de redes em empresas contábeis e estratégias para fortalecer a infraestrutura de rede. **Monumenta – Revista Científica Multidisciplinar,** v. 8, n. 8, p. 190–197, jul. 2024.

GOLDUZIAN, M. Machine learning–based predictive analysis for real-time DDoS mitigation using CICDDoS2019 dataset. **Journal of Information Security and Applications,** v. 75, p. 103523, 2023.

JIANG, H.; HE, Z.; YE, G.; ZHANG, H. Network Intrusion Detection Based on PSO-XGBoost Model. **IEEE Access,** v. 8, p. 58392–58401, 2020.

LATAH, M.; TOKER, L. Machine learning based anomaly detection for software defined networks: A survey. **Journal of Network and Computer Applications,** v. 112, p. 28–46, 2017.

LIU, S.; LIU, N.; ALHARBI, K. H.; ZHAO, X. Fault-tolerant routing algorithm based on disjoint paths in 3-ary n-cube networks with structure faults. **The Journal of Supercomputing,** v. 77, p. 13090–13114, 2021.

MOHSIN, M. A.; HAMAD, A. H. Performance Evaluation of SDN DDoS Attack Detection and Mitigation Based Random Forest and K-Nearest Neighbors Machine Learning Algorithms. **Revue d'Intelligence Artificielle**, v. 36, n. 2, p. 257-264, abr. 2022. DOI: 10.18280/ria.360207.

MOUSTAFA, N.; SLAY, J**. UNSW-NB15:** A comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set). *In:* MILITARY COMMUNICATIONS AND INFORMATION SYSTEMS CONFERENCE (MILCIS). Canberra: IEEE, 2015. p. 1–6.

RAMANI, S.; JHAVERI, R. H. ML-Based Delay Attack Detection and Isolation for Fault-Tolerant Software-Defined Industrial Networks. **Sensors,** v. 22, n. 18, p. 6958, 2022.

SHAIKH, J.; KHAN, Z.; HUSSAIN, M.; ALI, S.; MALIK, A. Advancing DDoS attack detection with hybrid deep learning: integrating convolutional neural networks, PCA, and vision transformers. **International Journal on Smart Sensing and Intelligent Systems,** v. 17, 2024.

ŞIMŞEK, M. M.; ATILGAN, E. **DoS and DDoS attacks on Internet of Things and their detection by machine learning algorithms.** Dicle Üniversitesi Mühendislik Fakültesi Mühendislik Dergisi, 2024.

XU, C.; SHEN, J.; DU, X.; ZHANG, F. An Intrusion Detection System Using a Deep Neural Network With Gated Recurrent Units. **IEEE Access,** v. 6, p. 48697-48707, 2018.