Revista Pleiade – Centro Universitário Descomplica UniAmérica
ISSN 1980-8666 (Impresso) – ISSN 2674-8231 (Eletrônico) – Classificação Capes B3 (2017-2020)

Detecção de Intrusão em Redes Modernas: Estudo com Método Híbrido de Redes Neurais

Intrusion Detection in Modern Networks: A Study Using a Hybrid Neural Network Method

Laércio Bubiak da Cruz[1] e Wagner Jorcuvich[2]

1. Engenheiro de Software. Especialista. Docente de Engenharia de Software do Centro Universitário Descomplica UniAmérica.
2. Matemático. Mestre. Docente Engenharia de Software da Centro Universitário Descomplica UniAmérica.
laercio.cruz.acad@gmail.com e *jorcuvich@gmail.com*

Palavras-chave
Cibersegurança Detecção de Intrusão
Inteligência Artificial
Redes Neurais Artificiais

Keywords
Cybersecurity Intrusion Detection
Artificial Intelligence
Artificial Neural Networks

Resumo:
Introdução. A área da cibersegurança está em constante evolução. Novas ameaças surgem com a mesma velocidade que as tecnologias de defesa. Métodos híbridos de Inteligência Artificial (IA) têm se mostrado promissores na criação de Sistemas de Detecção de Intrusão (IDS) mais robustos. **Objetivo.** Aplicar método híbrido que combina Redes Neurais Artificiais (RNA) e o algoritmo K-Nearest Neighbors (KNN) em dataset com sinistros de segurança para verificar a relevância e desempenho na detecção das intrusões. **Metodologia.** Foi conduzida pesquisa quantitativa e experimental utilizando a base de dados pública NSL-KDD. Implementados três modelos: RNA, KNN e o modelo Híbrido (RNA+KNN),treinados e testados. O desempenho foi comparado utilizando métricas de acurácia, precisão, recall, F1-score e tempo de processamento. **Resultados.** O modelo híbrido demonstrou superioridade, alcançando acurácia de 99,2%, superando modelos de RNA (97,8%) e KNN (96,5%) isoladamente. Notavelmente, o método híbrido obteve redução significativa na taxa de falsos positivos, com custo computacional marginalmente maior, considerado trade-off aceitável. **Considerações Finais.** O método híbrido mostrou-se abordagem eficaz e robusta para a detecção de intrusão em redes, mesmo seis anos após a proposição inicial. A combinação sinérgica das duas técnicas oferece equilíbrio superior entre precisão e capacidade de detecção, validando a aplicabilidade em ambientes de rede modernos.

Abstract:
Introduction. The field of cybersecurity is constantly evolving. New threats emerge at the same speed as defense technologies. Hybrid Artificial Intelligence (AI) methods have shown promise in creating more robust Intrusion Detection Systems (IDS). **Objective.** To apply a hybrid method combining Artificial Neural Networks (ANN) and the K-Nearest Neighbors (KNN) algorithm to a dataset of security incidents to verify its relevance and performance in intrusion detection. **Methodology.** Quantitative and experimental research was conducted using the public database NSL-KDD. Three models were implemented: ANN, KNN, and the Hybrid model (ANN+KNN), trained, and tested. Performance was compared using metrics of accuracy, precision, recall, F1-score, and processing time. **Results.** The hybrid model demonstrated superiority, achieving an accuracy of 99.2%, surpassing ANN (97.8%) and KNN (96.5%) models in isolation. Notably, the hybrid method achieved a significant reduction in the false positive rate, with a marginally higher computational cost, considered an acceptable trade-off. **Final Considerations.** The hybrid method proved to be an effective and robust approach for network intrusion detection, even six years after its initial proposal. The synergistic combination of the two techniques offers a superior balance between accuracy and detection capability, validating its applicability in modern network environments.

Artigo recebido em: 15.10.2025.
Aprovado para publicação em: 07.11.2025.

INTRODUÇÃO

A CRESCENTE DIGITALIZAção de serviços e a expansão da Internet das Coisas (IoT) ampliaram drasticamente a superfície de ataque para ameaças cibernéticas. Nesse contexto, os Sistemas de Detecção de Intrusão (IDS) são componentes vitais na arquitetura de segurança de qualquer organização, atuando como a primeira linha de defesa contra acessos não autorizados e atividades maliciosas. Tradicionalmente, muitos IDS operavam com base em assinaturas, sendo eficazes contra ameaças conhecidas, mas vulneráveis a ataques de dia zero e a variantes polimórficas de malware (NOGUEIRA, 2024).

Para superar essas limitações, a comunidade de pesquisa tem se voltado para a Inteligência Artificial (IA) e o Aprendizado de Máquina (Machine Learning - ML). Essas tecnologias permitem o desenvolvimento de IDS baseados em anomalias, capazes de aprender o comportamento normal da rede e identificar desvios que possam indicar uma intrusão. Em 2018, um trabalho notável de Cristiano Antonio de Souza propôs um método híbrido que combinava Redes Neurais Artificiais (RNA) e o algoritmo K-Nearest Neighbors (KNN) para melhorar a detecção de intrusões (SOUZA, 2018).

Seis anos se passaram desde essa proposta. Nesse período, tanto as técnicas de ataque quanto as ferramentas de IA evoluíram exponencialmente. Ataques se tornaram mais sofisticados, e o acesso a ferramentas de IA foi democratizado, permitindo que adversários com menor conhecimento técnico lancem ataques complexos (SMITH, 2022). Diante desse novo panorama, surge a questão: a abordagem híbrida de detecção de intrusão proposta por Souza (2008) responde com o mesmo desempenho quanto comparada à realidade das intrusões de 2018 e as que ocorrem em 2025?

Este artigo descreve os resultados do estudo com o método híbrido RNA+KNN. O objetivo foi reaplicar a metodologia e analisar seu desempenho em um ambiente pós-pesquisa, sendo decorrido sete anos e tomando como referência o ano de 2025 quanto aos problemas de cibersegurança.

Para alcançar tal objetivo, este trabalho abordou o seguinte problema de pesquisa: *O método de detecção de intrusão híbrido, baseado na combinação de RNA e KNN, mantém uma superioridade de desempenho (em termos de acurácia, precisão e F1-Score) em relação aos seus modelos constituintes isolados, mesmo diante da evolução das tecnologias e do cenário de ameaças sete anos após os testes realizados, considerando o cenário tecnológico de 2025?*

As principais contribuições deste artigo são: (i) uma implementação e avaliação sistemática do modelo híbrido em um ambiente computacional atualizado; (ii) uma análise comparativa quantitativa detalhada contra modelos de base; e (iii) a validação da durabilidade e relevância de uma arquitetura de IDS híbrida, oferecendo insights para futuras pesquisas na área.

A estrutura deste artigo está organizada da seguinte forma: a Seção 2 apresenta uma revisão dos trabalhos relacionados. A Seção 3 detalha a metodologia experimental. A Seção 4 apresenta e discute os resultados obtidos. Finalmente, a Seção 5 conclui o trabalho, sumarizando os achados e apontando direções futuras.

Este estudo reaplica o método RNA+KNN em um ambiente mais atual para testar se o modelo ainda mantém bom desempenho. Trabalhos recentes mostram que muitos IDS perdem precisão quando usados fora do conjunto de dados (*dataset)* original (CANTONE; MARROCCO; BRIA, 2024). Assim, o objetivo é verificar se o modelo híbrido proposto por Souza (2018) continua eficaz nas condições de 2025.

Estado da Arte e Trabalhos Relacionados

A detecção de intrusão utilizando IA não é um campo novo, mas está em constante renovação. A literatura apresenta diversas abordagens, que podem ser categorizadas em métodos de modelo único e métodos híbridos.

1 Abordagens Baseadas em Modelo Único

Diversos algoritmos de ML foram aplicados com sucesso. As Redes Neurais Artificiais (RNA) são amplamente utilizadas por sua capacidade de aprender padrões complexos e não lineares nos dados de tráfego de rede. O K-Nearest Neighbors (KNN), por sua vez, é um algoritmo baseado em instância que classifica novos dados com base na similaridade com exemplos conhecidos, sendo eficaz na identificação de anomalias locais (PASSOS *et al*., 2021). Outras técnicas como Support Vector Machines (SVM) (LIMA *et al*., 2023) e Árvores de Decisão também são frequentemente empregadas (GUEZZAZ *et al*., 2021).

Mariani *et al*. (2024) apresentam o desenvolvimento de um sistema para detectar anomalias e ataques cibernéticos em Sistemas de Controle Industrial (ICS), que são essenciais para infraestruturas como usinas de tratamento de água e redes elétricas. A abordagem utilizada para a detecção foi um processo de classificação em duas etapas:

Primeira Etapa: O sistema primeiro distingue se a operação do sistema é “normal” ou “anômala”.

Segunda Etapa: Caso uma anomalia seja detectada, o sistema identifica o tipo específico de ataque que está ocorrendo.

Para treinar e testar o sistema, Mariani *et al*. (2024) utilizou em seu artigo o dataset SWaT, que simula o funcionamento de uma estação de tratamento de água. Foi aplicada a técnica SMOTE para balancear os dados, garantindo que o modelo de aprendizado de máquina não fosse enviesado por uma quantidade desproporcional de dados de operações normais. Dentre os vários algoritmos de aprendizado de máquina testados, o Random Forest se destacou. Sua principal vantagem foi a alta capacidade de identificar todos os incidentes de segurança sem gerar falsos negativos (alto recall), o que é fundamental em ambientes críticos onde falhar em detectar um ataque pode ter consequências graves. Nesse trabalho, concluiu-se que o sistema proposto é eficaz para classificar as operações de um ICS, identificando corretamente tanto o estado do sistema (normal ou sob ataque) quanto o tipo de ameaça.

2 Abordagens Híbridas

A principal motivação para os modelos híbridos é combinar diferentes algoritmos para melhorar o desempenho da solução. Para Souza (2018), a RNA é aplicada na generalização de padrões com bom desempenho em classificação, enquanto o KNN é preciso na classificação de instâncias limítrofes. A combinação proposta visava, portanto, criar um classificador mais robusto e preciso. Outros estudos seguiram caminhos semelhantes, combinando diferentes técnicas, como em abordagens de aprendizado semi-supervisionado que utilizam a lógica fuzzy para aprimorar a detecção (ALOLAIYAN *et al*., 2021).

Moreira *et al*. (2021) investigaram o uso de técnicas de *Ensemble Learning* para aprimorar os Sistemas de Detecção de Intrusão (IDS). O estudo otimizou a identificação de ataques de negação de serviço distribuído (DDoS), que visam tornar um serviço online indisponível ao sobrecarregá-lo com tráfego de múltiplas fontes. A pesquisa se concentrou na aplicação do método Stacking, uma abordagem de *Ensemble Learning* que combina múltiplos modelos de aprendizado de máquina para melhorar a performance preditiva. Neste

método, um “meta-modelo” aprende a melhor forma de combinar as previsões de outros modelos base. Os algoritmos de base utilizados foram o Support Vector Machine (SVM) e o KNN. O SVM é conhecido por sua eficácia em encontrar um plano que melhor separa diferentes classes de dados, enquanto o KNN classifica novos dados com base na similaridade com seus vizinhos mais próximos.

Em Bentes *et al*. (2021) há a análise do desempenho de dois algoritmos de aprendizado de máquina, a **Árvore de Decisão** e o **Naive Bayes**, para aprimorar Sistemas de Detecção de Intrusão (IDS). A pesquisa utilizou o conjunto de dados KDDCUP'99, que contém uma variedade de simulações de ataques em um ambiente de rede militar. O principal objetivo do estudo foi classificar as conexões de rede como “normais” ou como “intrusões”. Para isso, os pesquisadores realizaram simulações em duas etapas distintas: divisão dos dados em duas classes (normal e intrusão), expandindo a classificação para cinco categorias, uma para conexões normais e quatro para diferentes tipos de ataques. Os resultados mostraram que o algoritmo de Árvore de Decisão foi mais eficiente na classificação correta das conexões, mas o algoritmo Naive Bayes se destacou pela sua velocidade superior no processo de classificação. O estudo em questão concluiu que o Naive Bayes é o mais indicado para essa tarefa, tanto no cenário de duas quanto no de cinco classes.

MATERIAIS E MÉTODOS

Este estudo foi conduzido como uma pesquisa de natureza aplicada, com abordagem quantitativa e experimental na área de segurança da informação, em detecção de intrusão.

1 Ambiente Experimental e Dataset

Para o treinamento e teste dos modelos, foi utilizada a base de dados pública **NSL-KDD**. Este dataset é uma versão aprimorada do KDD'99, criada para resolver algumas de suas deficiências, como a presença de registros redundantes. Ele contém 41 características (features) por registro de tráfego e inclui diversos tipos de ataques, categorizados em DoS (*Denial of Service*), Probe, R2L (*Root to Local*) e U2R (*User to Root*). A escolha do NSL-KDD se justifica por ser um benchmark amplamente reconhecido na comunidade, permitindo a comparabilidade dos resultados com outros trabalhos da área (KAGGLE, 2025). As coletas de Souza foram realizadas em laboratório próprio, em 2018. Neste trabalho, os experimentos foram executados em uma máquina com as seguintes especificações: Processador Intel Core i7-10750H, 16 GB de RAM e GPU NVIDIA GeForce RTX 2060. O ambiente de software consistiu em Python 3.9, com as bibliotecas Scikit-learn (versão 1.1.1), Pandas (versão 1.4.2) e TensorFlow (versão 2.9.1).

2 Pré-processamento dos Dados

Os dados passaram por uma etapa de pré-processamento essencial. As características categóricas (como *protocol_type*, *service*, e *flag*) foram convertidas em formato numérico utilizando a técnica de *One-Hot Encoding*. Em seguida, todas as características numéricas foram normalizadas para o intervalo através do *Min-Max Scaler*, garantindo que nenhuma característica dominasse o processo de aprendizado devido à sua escala. O dataset foi dividido em 80% para treinamento e 20% para teste.

3 Arquitetura e Configuração dos Modelos

3.1 Rede Neural Artificial (RNA):

Foi implementada uma rede neural do tipo *Multi-Layer Perceptron* (MLP) utilizando a biblioteca Keras com TensorFlow. A arquitetura consistiu em uma camada de entrada, duas camadas ocultas com 64 e 32 neurônios respectivamente (utilizando a função de ativação ReLU), e uma camada de saída com função de ativação *Softmax* para classificação multiclasse. O modelo foi compilado com o otimizador *Adam*, função de perda *categorical_crossentropy* e treinado por 50 épocas com um *batch size* de 64.

3.2 K-Nearest Neighbors (KNN):

O modelo KNN foi implementado com a biblioteca Scikit-learn. O número de vizinhos (k) foi definido como 5, valor encontrado como ótimo após testes de validação cruzada. A métrica de distância utilizada foi a Euclidiana e o algoritmo 'auto' para busca de vizinhos.

3.3 Modelo Híbrido (RNA+KNN):

A hibridização foi implementada de forma sequencial. Primeiramente, o modelo RNA classifica uma instância de tráfego. As predições com confiança inferior a 95% foram reavaliadas pelo modelo KNN, que fornecia a classificação final. O limiar de 95% foi definido empiricamente após análise na curva ROC (*Receiver Operating Characteristic*) em um conjunto de validação, buscando otimizar o equilíbrio entre a carga computacional e o ganho de precisão.

3.4 Métricas de Avaliação

Para avaliar e comparar o desempenho dos modelos, foram utilizadas as seguintes métricas, cujas fórmulas são definidas com base nos valores da matriz de confusão (TP: Verdadeiro Positivo, TN: Verdadeiro Negativo, FP: Falso Positivo, FN: Falso Negativo):

Acurácia: Mede a proporção de predições corretas.

$$A = \frac{TP + TN}{TP + TN + FP + FN}$$

Precisão: Mede a proporção de positivos corretamente identificados.

$$P = \frac{TP}{TP + FP}$$

Recall (Sensibilidade): Mede a proporção de positivos reais que foram corretamente identificados. Fórmula:

$$S = \frac{TP}{TP + FN}$$

F1-Score: Média harmônica entre precisão e recall.

$$FS = 2 \times \frac{Precisa\ \ o \times Recall}{Precisa\ \ o + Recall}$$

Tempo de Processamento: Tempo em segundos para classificar o conjunto de teste.

Esses mesmos parâmetros foram coletados por Souza (2018), para fins de comparação.

RESULTADOS

Após a execução dos testes, os resultados de desempenho foram consolidados e comparados, conforme apresentado na Tabela 1.

Tabela 1: Comparativo de Desempenho dos Modelos de Detecção.

Métrica	RNA Isolada	KNN Isolado	Modelo Híbrido (RNA+KNN)
Acurácia	97,8%	96,5%	99,2%
Precisão	97,5%	96,8%	99,1%
Recall	98,1%	96,2%	99,3%
F1-Score	97,8%	96,5%	99,2%
Tempo de Teste (s)	15s	125s	28s

Para uma análise mais granular dos erros de classificação, a matriz de confusão do modelo híbrido foi desenvolvida e é apresentada na Tabela 2. A análise da matriz revela que a maioria dos erros remanescentes ocorre na classificação de ataques raros, como U2R e R2L, que possuem poucas amostras no dataset de treinamento, um desafio conhecido na área.

Tabela 2: Matriz de Confusão Detalhada do Modelo Híbrido (RNA+KNN).

	Previsto: Normal	Previsto: DoS	Previsto: Probe	Previsto: R2L/U2R
Verdadeiro: Normal	9650	15	45	5
Verdadeiro: DoS	20	7440	0	2
Verdadeiro: Probe	35	0	2395	10
Verdadeiro: R2L/U2R	40	1	8	2918

Os resultados demonstram claramente a superioridade do modelo híbrido em todas as métricas de eficácia. A acurácia de 99,2% indica uma capacidade de classificação geral extremamente alta. O F1-Score, também de 99,2%, reforça essa eficácia, mostrando um excelente equilíbrio entre a capacidade de não gerar falsos alarmes (precisão) e a de não deixar passar ataques reais (recall).

A principal vantagem da abordagem híbrida reside na sua sinergia. A RNA, com sua capacidade de generalização, lida eficientemente com a maioria do tráfego. No entanto, ao delegar as instâncias de baixa confiança ao KNN, o modelo se beneficia da análise de vizinhança mais detalhada deste último, corrigindo potenciais erros da RNA e aumentando a precisão geral, especialmente na redução de falsos positivos.

Em relação ao tempo de processamento, o modelo híbrido apresentou um custo computacional maior que o da RNA isolada, mas significativamente menor que o do KNN isolado. O KNN é computacionalmente caro, na fase de teste, pois precisa calcular distâncias para todos os pontos de treinamento. O modelo híbrido mitiga esse problema, já que apenas uma pequena fração dos dados é repassada ao KNN. Esse trade-off entre um pequeno aumento no tempo e um ganho substancial em precisão é altamente vantajoso em cenários de segurança.

INTERPRETABILIDADE DO MODELO

O modelo híbrido RNA+KNN tem a vantagem de ser mais simples de interpretar que modelos mais complexos, como CNNs e LSTMs. A RNA realiza a primeira classificação e o KNN reavalia apenas os casos com baixa confiança, permitindo identificar de quais amostras a decisão depende. Isso ajuda o analista a entender o motivo de cada detecção e aumenta a transparência do sistema.

Estudos recentes também apontam a interpretabilidade como um ponto central em sistemas de detecção de intrusão baseados em IA, destacando o uso de técnicas como *Explainable AI* (XAI) para tornar os modelos mais compreensíveis (MOHALE; OBAGBUWA, 2025).

DISCUSSÃO

A validade externa pode ser limitada pelo uso exclusivo do dataset NSL-KDD, que, embora padronizado, pode não representar perfeitamente as características do tráfego de rede contemporâneo. A validade interna é robusta, mas dependente dos hiperparâmetros específicos escolhidos para os modelos. Embora otimizados, diferentes configurações poderiam levar a resultados ligeiramente distintos.

A relevância do método híbrido proposto por Souza (2018) torna-se mais evidente quando comparado a outras abordagens que também buscaram combinar algoritmos, mas com resultados menos expressivos. Em alguns estudos que aplicaram, por exemplo, combinações paralelas ou métodos de votação simples, a melhoria de desempenho foi marginal, frequentemente acompanhada por um aumento significativo no custo computacional (BERTONI, 2021). O diferencial da proposta de Souza reside na sua abordagem sequencial e hierarquizada: a Rede Neural Artificial (RNA) atua como um classificador rápido e generalista, processando a grande maioria do tráfego com alta eficiência, enquanto o K-Nearest Neighbors (KNN) é acionado apenas para os casos de baixa confiança. Essa especialização de tarefas cria uma sinergia única, onde o KNN compensa a principal fraqueza da RNA – a dificuldade em classificar instâncias atípicas ou de fronteira – sem sobrecarregar o sistema, justificando por que essa combinação específica se mostra tão robusta.

A validação da presente pesquisa é reforçada pela consistência de seus achados com outras investigações que exploraram modelos híbridos para a detecção de intrusão. Estudos que combinaram Árvores de Decisão com algoritmos de agrupamento, ou que utilizaram técnicas de *ensemble learning* como o Stacking, também relataram uma superioridade notável em relação aos seus modelos constituintes isolados (DALARMELINA, 2023). Assim como no nosso estudo, esses trabalhos concluíram que a combinação inteligente de múltiplos classificadores permite superar as limitações individuais de cada técnica, resultando em sistemas mais precisos e com menor taxa de falsos positivos. Isso demonstra que os resultados obtidos não são um caso isolado, mas sim um reflexo de uma tendência consolidada na área de cibersegurança, que aponta para a hibridização de modelos como um caminho eficaz para a construção de Sistemas de Detecção de Intrusão (IDS) mais resilientes.

Apesar do desempenho superior do modelo RNA+KNN, é fundamental reconhecer que o cenário de ameaças e as técnicas de defesa evoluíram. Pesquisas mais recentes, por exemplo, têm demonstrado o potencial de arquiteturas de *deep learning*, como Redes Neurais Convolucionais (CNN) e Long Short-Term Memory (LSTM), para superar modelos de *machine learning* tradicionais (DA SILVA *et al*., 2025). Esses modelos avançados são capazes de aprender representações hierárquicas e temporais complexas dos dados de rede, mostrando-se especialmente eficazes na detecção de ataques distribuídos (DDoS) e ameaças do tipo *zero-day* em datasets modernos como o CIC-IDS2017 e o CIC-IDS2018. Portanto, embora o método híbrido RNA+KNN continue sendo uma solução altamente eficaz e relevante, esses novos estudos indicam pontos claros para melhoria, como a substituição da RNA por uma arquitetura mais avançada, o que poderia elevar ainda mais a precisão e a capacidade de generalização do modelo frente aos vetores de ataque contemporâneos.

Considerações Finais

Este estudo se propôs reaplicar a metodologia proposta por Souza (2018) em um dataset atualizado para que pudesse ser avaliado o desempenho no contexto tecnológico, ou seja, o funcionamento do método híbrido de detecção de intrusão com a aplicação de Redes Neurais Artificiais e KNN.

Os resultados confirmaram que o desempenho do método híbrido se manteve superior quando comparada às técnicas de RNA e KNN aplicadas isoladamente. Portanto, o estudo indicou que a solução combinada ainda é a mais indicada para detecção de intrusão.

O modelo pode ser usado em sistemas reais, integrado a gateways de rede ou ferramentas SIEM, como Snort e Suricata, analisando eventos em tempo real e reduzindo falsos positivos (XIANG et al., 2025).

Como limitações, reconhece-se que o estudo utilizou o dataset NSL-KDD, que, embora seja um padrão, não contempla os vetores de ataque mais recentes. Para trabalhos futuros, sugere-se a aplicação e adaptação deste modelo híbrido em datasets mais modernos, como o CIC-IDS2018, e a exploração de sua eficácia em ambientes específicos, como redes de IoT. Além disso, a substituição da RNA por arquiteturas de deep learning mais avançadas, como Redes Neurais Convolucionais (CNN) ou Long Short-Term Memory (LSTM), pode ser um caminho promissor para aprimorar ainda mais a detecção de ameaças complexas e sequenciais.

Além disso, propõe-se como trabalho futuro integrar o modelo híbrido a um pipeline Snort+SIEM para correlação em tempo real, avaliando o impacto na taxa de falsos positivos e no tempo de resposta em SOC - Centros de Operação de Segurança.

Referências

BENTES, Eliel Dos S.; DE FIGUEIREDO, Yann Fabricio Cardoso; DE CAMPOS, Lidio ML. Aplicação de algoritmos de aprendizado de máquina para detecção de intrusão. In: **Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos (SBRC)**. SBC, 2021. p. 209-216.

BERTONI, Mateus Alves. **Aplicação do método conjunto Stacking do classificador Floresta de Caminhos Ótimos para o problema de detecção de intrusão**. Universidade Estadual Paulista Júlio de Mesquita Filho-Campus de São José do Rio Preto. São José do Rio Preto, São Paulo, Brasil, 2021.

CANTONE, M.; MARROCCO, C.; BRIA, A. **Machine Learning in Network Intrusion Detection: A Cross-Dataset Generalization Study.** IEEE Access, v. 12, p. 144489–144508, 2024.

DALARMELINA, Nicole do Vale. **Uma abordagem Ensemble Learning para modelos de detecção de intrusão para redes industriais**. 2023. Tese de Doutorado. Universidade de São Paulo.

DA SILVA, A. M. de A.; REGO, P. A. L.; BONFIM, M. S. Avaliação e Mitigação de Ataques Adversários em Sistema de Detecção de Intrusão IoT. In: **Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais (SBSeg)**. SBC, 2025. p. 1003-1010.

GUEZZAZ, Azidine *et al*. A reliable network intrusion detection approach using decision tree with enhanced data quality. **Security and Communication Networks**, v. 2021, n. 1, p. 1230593, 2021.

LIMA, Matheus H. *et al*. Predição não-supervisionada de ataques DDoS por sinais precoces e one-class SVM. In: **Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais (SBSeg)**. SBC, 2023. p. 403-416.

MARIANI, Wagner Carlos *et al*. Detecção de Intrusão e Análise Cyberfísica em Redes Industriais. In: **Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais (SBSeg)**. SBC, 2024. p. 787-793.

MOHALE, V. Z.; OBAGBUWA, I. C. **Evaluating Machine Learning-Based IDS with Explainable AI: Enhancing Transparency and Interpretability.** Frontiers in Computer Science, v. 7, p. 1520741, 2025.

MOREIRA, Andricson Abeline *et al*. Técnicas de ensemble learning para sistema de detecção de intrusão no contexto da cibersegurança. **Revista de Segurança da Informação e Comunicação**, v. 10, n. 1, p. 1-15, 2021.

NOGUEIRA, Michele. Segurança na Conectividade: Protegendo Redes e Conexões. **Computação Brasil**, n. 52, p. 30-34, 2024.

NSL KDD *dataset*. Disponível em: <https://www.kaggle.com/datasets/hassan06/nslkdd>. Acesso em 18 Out 2025.

SOUZA, C. A. **Método híbrido de detecção de intrusão aplicando inteligência artificial**. Dissertação de Mestrado. Disponível em: https://tede.unioeste.br/handle/tede/3534. Universidade Estadual Oeste do Paraná – UNIOESTE, Foz do Iguaçu – PR. Acesso em 15 Ago. 2025.

XIANG, B.; ZHENG, R.; ZHANG, K.; LI, C.; ZHENG, J. **FFT-RDNet: A Time–Frequency-Domain-Based Intrusion Detection Model for IoT Security.** Sensors, v. 25, n. 15, p. 4584, 2025.