THIAGO JOSÉ LUCAS

# TRÁFEGO DESBALANCEADO EM REDES DE COMPUTADORES: OBSERVAÇÕES ACERCA DOS EFEITOS DO BALANCEAMENTO DE DADOS E SUA RELAÇÃO COM TÉCNICAS DE ENSEMBLE LEARNING APLICADOS A CIBERSEGURANÇA

Relatório de Pós-doutorado realizado na Universidade Estadual Paulista (UNESP), Campus de Bauru/SP.

Supervisor(a): Prof. Dr. Kelton Augusto Pontara da Costa

Bauru

2024

# 1 Introdução

A qualidade dos dados de treinamento no fluxo de aprendizagem de máquina é tão importante quanto a robustez dos algoritmos classificadores. O pré-processamento dos dados garante valores normalizados, discretizados e com o mínimo possível de ruídos. Um levantamento prévio, associado à Tese de Doutorado do proponente deste Projeto, constatou que o ajuste de proporcionalidade na distribuição das amostras é normalmente negligenciado na relação entre Ensemble Learning e Cibersegurança. Hipoteticamente, o dimensionamento mais adequado quanto à distribuição dos rótulos tende a aprimorar os Sistemas de Detecção de Intrusão criados, seja na redução dos erros de classificação ou na diminuição do custo computacional.

A área da aprendizagem de máquina tem se destacado como uma abordagem promissora para a resolução de problemas complexos e no desenvolvimento de sistemas inteligentes, com aplicações relevantes no contexto de cibersegurança. É sabido que a qualidade dos dados de treinamento desempenha um papel fundamental, sendo tão relevante quanto a robustez dos algoritmos classificadores utilizados. No entanto, um levantamento prévio por realizado por ocasião do desenvolvimento de uma abrangente pesquisa associado à Tese de Doutorado do proponente deste Projeto identificou uma lacuna na relação entre Ensemble Learning e Cibersegurança, especificamente no trinamento de Sistemas de Detecção de Intrusão: o ajuste de proporcionalidade na distribuição das amostras não é comumente explorado [1]. Essa proporção inadequada tende a comprometer a eficácia dos Sistemas de Detecção de Intrusão desenvolvidos, resultando potencialmente em mais erros de classificação e na entrega de um alto custo computacional.

Nesse contexto, em hipótese, um dimensionamento mais adequado da distribuição dos rótulos nos conjuntos de dados de Cibersegurança pode aprimorar significativamente os resultados obtidos pelos algoritmos de Ensemble Learning criando Sistemas de Detecção de Intrusão mais robustos.

Ao considerar uma distribuição proporcionalmente balanceada das amostras, espera-se reduzir os erros de classificação e otimizar o desempenho dos Sistemas de Detecção de Intrusão. Diante do cenário supracitado, justifica-se a necessidade de aprofundar os estudos sobre a aplicação de técnicas de Ensemble Learning em conjuntos de dados de Cibersegurança, com foco específico na distribuição proporcional dos rótulos. Desta forma, busca-se contribuir para o desenvolvimento da área e fornecer modelos de sistemas mais eficientes e confiáveis.

O Problema de Pesquisa principal foi: quais são as alterações em termos de redução de erros de classificação e otimização de custo computacional na execução de técnicas de Ensemble Learning em dados balanceados em comparação com a aplicação em dados desbalanceados no contexto específico de cibersegurança?

O Objetivo Geral deste relatório é documentar toda a produção científica produzida durante o período de execução do pós-doutorado. A temática específica foi explorada diretamente em uma das publicações realizadas e indiretamente em outras duas. Ademais, como resultados foram obtidos também particiações em bancas de avaliação e, principalmente, co-orientações de Mestrado.

# 2 Sistemas de Detecção de Intrusão

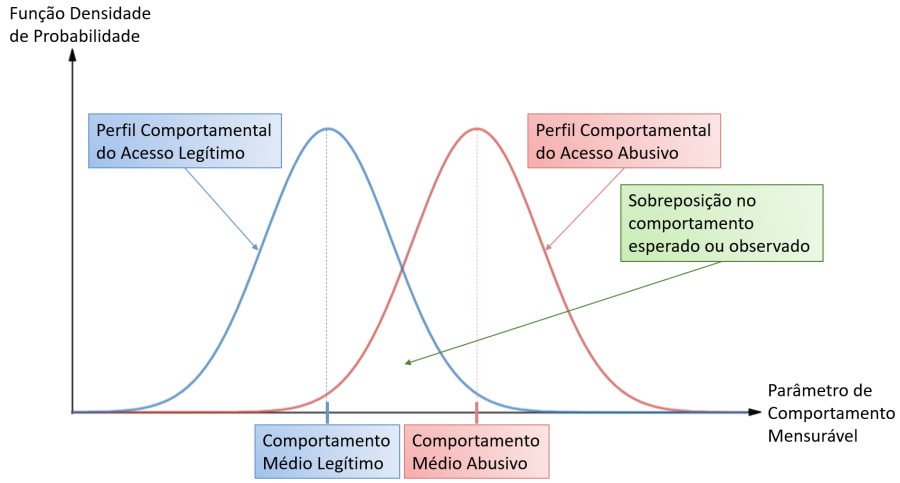
De acordo com [2], as ações relacionadas com foco na manutenção da integridade, acessibilidade ou confiabilidade de uma fonte de dados eletrônicos ou de uma rede de comunicação definem os objetivos de um IDS. Os autores fazem uma leitura histórica do surgimento e da evolução dos IDS atribuindo a James Anderson - quando da publicação do artigo "*Computer Security Threat Monitoring and Surveillance*", por [3], o primeiro relato de um IDS. Dois fatos marcantes na evolução dos IDS ocorreram em 1986 e posteriormente em 1993 quando publicações documentavam cientificamente modelos de detecção de intrusão baseados em análises estatísticas do tráfego de rede (ambos criados por Dorothy Denning e Peter Neumann em [4]).

Um IDS é um software desenvolvido para detectar ataques que tenham potencial para causar danos na rede de comunicação ou nos sistemas, sejam eles provenientes de um meio inseguro como a Internet ou da rede local [5]. Tais softwares executam contramedidas de segurança ao detectar alguma anomalia no tráfego de rede ou no comportamento dos hosts que possa caracterizar um ataque.

Os autores destacam que recentemente muitas abordagens têm sido aplicadas para se aumentar a taxa de detecção, de forma geral, envolvendo técnicas de *Machine Learning* (situações onde o detector aprende por meio de treinamento a detectar anomalias), *Rule Based* (caso onde o detector possui assinaturas características de ataques e apenas compara o tráfego real com as assinaturas de ataques já conhecidos) e/ou métodos estatísticos clássicos (emprego de cálculos de média, desvio padrão, mediana, dentre outros).

A aplicação de um modelo de detecção de intrusão somente é possível caso o comportamento dos usuários possa ser caracterizado em "legítimo" ou "abusivo" [6]. Contudo, em muitos cenários não existe um limite exato de comportamento, conforme a Figura 1 ilustra.

Figura 1: Funções Densidade de Probabilidade para Comportamentos Mensuráveis.




Fonte: Elaborado pelo Autor. Adaptado de [6].

As curvas gaussianas (Figura 1) ilustram, à esquerda, a distribuição normal de determinado comportamento mensurável que caracteriza usuários legítimos e, à direita, na mesma lógica, um perfil de comportamento abusivo. Entretanto, no caso exposto, existe uma sobreposição entre as duas distribuições normais que eleva o grau de dificuldade na classificação do comportamento. Técnicas mais robustas de classificação tendem a apresentar uma taxa de acurácia mais próxima da realidade com altos índices de *true-positives* (situação onde um acesso legítimo ou abusivo é classificado corretamente) enquanto técnicas menos apuradas tendem a aumentar as taxas de *false-negatives* (quando os rótulos são atribuídos de forma incorreta).

Os IDS possuem duas dimensões de classificação: pela Topologia de Rede e pela Abordagem dos Pacotes. A primeira dimensão, de acordo com [7], define se o detector trabalha analisando o fluxo de rede (topologicamente, neste caso, o IDS normalmente é colocado na rede de comunicação em forma de

*bridge*[1] ou recebendo uma cópia de todos os pacotes trafegados por meio de espelhamento[2] de uma porta da *switch*[3]) ou analisando o comportamento do sistema operacional, situação onde o detector trabalha observando medidas de processamento, espaço em disco, uso de memória ou auditando registros feitos nos logs do sistema. Já a segunda dimensão de classificação diz respeito a maneira como o detector analisa os dados. [8] afirmam que nesta categorização existem duas classes: detecção por assinatura ou detecção por anomalia. Os autores explicam que na detecção por assinatura o IDS possui uma base de dados de ataques já conhecidos e basicamente seu trabalho é comparar os pacotes que chegam até a rede com o seu banco de dados de forma a verificar similaridades. Na detecção por anomalia, entretanto, o sistema define um modelo de que seria o comportamento "normal" da rede ou do sistema fazendo com que pacotes que não se classifiquem como "normais" sejam rotulados como maliciosos.

# 3 Metodologia

Cada publicação realizada seguiu um método específico:

– A meta-análise produzida valeu-se da aplicação da Revisão Sistemática da Literatura, conforme [9];
– O modelo IDS baseado no pruning pela diversidade valeu-se do método Stacking [10] associado ao Disagreement Measure [11];
– O estudo publicado sobre as técnicas de reamostragem valeu-se de diversas técnicas de Oversampling [12], Undersampling [13] e Resampling [14].

Sugere-se ao leitor que obtenha acesso direto as publicações documentadas na Seção de Resultados para uma melhor compreensão dos métodos aplicados em cada um dos experimentos.

[1] situação topológica onde o dispositivo de rede é o único meio pelo qual o tráfego ocorre.
[2] técnica utilizada para se enviar cópias dos *frames* de outras portas para uma porta específica onde o IDS será conectado.
[3] dispositivo de interconexão de redes atuante na camada de Enlace do modelo de referência OSI.

# 4 Resultados

O presente Capítulo compila objetivamente os resultados obtidos durante a execução do pós-doutorado. Inicialmente são elencados os três trabalhos publicados, posteriormente as co-orientações de Mestrado e, por fim, as participações em bancas de avaliação de Mestrado e de Doutorado.

## 4.1 Produção Científica

Na sequência estão organizadas as produções científicas realizadas durante o período do pós-doutorado:

**Publicação 01 – "*A Comprehensive Survey on Ensemble Learning-Based Intrusion Detection Approaches in Computer Networks*"**

– Data do aceite: 24/10/2023
– Data da publicação: 30/10/2023
– Qualis CAPES: A1
– Periódico: IEEE Access
– Disponível em https://ieeexplore.ieee.org/abstract/document/10299619/

**Publicação 02 – "*Ensemble Diversity Pruning on Cybersecurity: Optimizing Intrusion Detection Systems*"**

– Data do aceite: 21/05/2024
– Data da apresentação: 09/07/2024
– Qualis CAPES: A3
– Conferência: IEEE *International Conference on Systems, Signals and Image Processing*
– *Conference Program*: https://www.cobcom.tugraz.at/

**Publicação 03 – "*Enhancing Cyberattack Detection in IoT Environments Through Advanced Resampling Techniques*"**

– Data do aceite: 21/05/2024
– Data da apresentação: 10/07/2024
– Qualis CAPES: A3

– Conferência: IEEE *International Conference on Systems, Signals and Image Processing*
– *Conference Program*: https://www.cobcom.tugraz.at/

## 4.2 Co-orientações de Mestrado

Na sequência estão organizadas as co-orientações de Mestrado realizadas durante o período do pós-doutorado:

**Co-orientação 01 – "Machine Learning para Identificação de Ataques de Intrusão Utilizando Métodos de Balanceamento de Dados"**

– Discente: Carlos Alexandre Carvalho Tojeiro
– Situação: Dissertação defendida.

**Co-orientação 02 – "Federated Transfer Learning para Detecção de Intrusão em Redes de Computadores"**

– Discente: Carlos de Jesus Reis
– Situação: Dissertação qualificada

## 4.3 Participações em Bancas

Na sequência estão organizadas as particiáções em bancas de avaliação realizadas durante o período do pós-doutorado:

**Banca 01 – "AIOPs - Utilizando uma Arquitetura Transformer em Time Series com Prometheus"**

– Tipo: Banca de Estudos Especiais (Mestrado)
– Discente: Weslley Rosalem
– Data: Julho/2023

**Banca 02 – "Machine Learning para Identificação de Ataques de Intrusão Utilizando Métodos de Balanceamento de Dados"**

– Tipo: Banca de Qualificação (Mestrado)
– Discente: Carlos Alexandre Carvalho Tojeiro
– Data: Agosto/2023

**Banca 03 – "AIOPs - Utilizando uma Arquitetura Transformer em Time Series com Prometheus"**

– Tipo: Banca de Qualificação (Mestrado)
– Discente: Weslley Rosalem
– Data: Dezembro/2023

**Banca 04 – "Sistemas Quânticos Inteligentes para Segurança de Dados"**

– Tipo: Banca de Estudos Especiais II (Doutorado)
– Discente: Ricardo Conde Camillo da Silva
– Data: Dezembro/2023

**Banca 05 – "Federated Transfer Learning para Detecção de Intrusão em Redes de Computadores"**

– Tipo: Banca de Qualificação (Mestrado)
– Discente: Carlos de Jesus Reis
– Data: Março/2024

**Banca 06 – "Arquiteturas de Deepfake em Cybersegurança"**

– Tipo: Banca de Qualificação (Mestrado)
– Discente: Fabricio Steinle Amoroso
– Data: Julho/2024

# 5 Considerações finais

A vivência com a pesquisa científica durante o período de execução do pós-doutorado foi de bastante importância para o aprimoramento geral do proponente, em especial pelas co-orientações dos alunos de Mestrado. As produções científicas demonstram resultados objetivos do tempo investido na pesquisa, bem como demonstram aceitabilidade dos métodos propostos, por conta da qualidade e seletividade dos congressos e dos periódicos. Este autor acredita que a aproximação com o trabalho do pesquisador fruto dos trabalhos realizados no período de execução do pós-doutorado foi fundamental para atingir não somente o objetivo proposto no projeto de pós-doutorado, mas para alcançar resultados que extrapolaram as espectativas iniciais.

# Referências


[1] Thiago José Lucas. About intrusion detection in computer networks and computational systems: a pruning proposal to reduce computational cost and gain performance using ensemble learning. 2023.

[2] Sinem Osken, Ecem Nur Yildirim, Gozde Karatas, and Levent Cuhaci. Intrusion detection systems with deep learning: A systematic mapping study. In *2019 Scientific Meeting on Electrical-Electronics & Biomedical Engineering and Computer Science (EBBT)*, pages 1–4. IEEE, 2019.

[3] James P Anderson. Computer security threat monitoring and surveillance. *Technical Report, James P. Anderson Company*, 1980.

[4] Dorothy E Denning. An intrusion-detection model. *IEEE Transactions on software engineering*, (2):222–232, 1987.

[5] Gozde Karatas and Ozgur Koray Sahingoz. Neural network based intrusion detection systems with different training functions. In *2018 6th International Symposium on Digital Forensic and Security (ISDFS)*, pages 1–6. IEEE, 2018.

[6] William Stallings. *Network security essentials: applications and standards*. Pearson, 2016.

[7] Mohamad Kaouk, Jean-Marie Flaus, Marie-Laure Potet, and Roland Groz. A review of intrusion detection systems for industrial control systems. In *2019 6th International Conference on Control, Decision and Information Technologies (CoDIT)*, pages 1699–1704. IEEE, 2019.

[8] Jing Ran, Yidong Ji, and Bihua Tang. A semi-supervised learning approach to ieee 802.11 network anomaly detection. In *2019 IEEE 89th Vehicular Technology Conference (VTC2019-Spring)*, pages 1–5. IEEE, 2019.

[9] Debajyoti Pati and Lesa N Lorusso. How to write a systematic review of the literature. *HERD: Health Environments Research & Design Journal*, 11(1):15–30, 2018.

[10] David H Wolpert. Stacked generalization. *Neural networks*, 5(2):241–259, 1992.

[11] Ludmila I Kuncheva and Christopher J Whitaker. Measures of diversity in classifier ensembles and their relationship with the ensemble accuracy. *Machine learning*, 51(2):181–207, 2003.

[12] Zhuoyuan Zheng, Yunpeng Cai, and Ye Li. Oversampling method for imbalanced classification. *Computing and Informatics*, 34(5):1017–1037, 2015.

[13] Mayuri S Shelke, Prashant R Deshmukh, and Vijaya K Shandilya. A review on imbalanced data handling using undersampling and oversampling technique. *Int. J. Recent Trends Eng. Res*, 3(4):444–449, 2017.

[14] Michael R Chernick. Resampling methods. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, 2(3):255–262, 2012.