

Para Além das Médias Móveis: Uma Abordagem com Integral de Choquet para Detecção de Anomalias

Denner Ayres¹, Romulo de Moraes¹, Giancarlo Lucca¹,
André Riker², Roger Immich³, Bruno L. Dalmazo¹

¹ Federal University of Rio Grande (FURG) – Brazil

² Federal University of Para (UFPA) – Brazil

³ Federal University of Rio Grande do Norte (UFRN) – Brazil

{dennerayres, demoraes.romulo, giancarlo.lucca, dalmazo}@furg.br
roger@imd.ufrn.br, ariker@ufpa.br

Abstract. *This work presents a methodology for anomaly detection in networks, combining the Poisson Moving Average (PMA) and the Choquet Integral with Power Measures. The proposed approach aims to improve accuracy in scenarios with low historical dependence by adjusting the parameter q according to data dynamics. Using the CIC-IDS2017 dataset, the results showed a 5.31% reduction in MAE, a 6.78% increase in precision, and a 0.17% improvement in accuracy compared to PMA, highlighting the effectiveness of the hybrid model for attack prediction.*

Keywords: *Anomaly Detection; Choquet Integral; Power Measures.*

Resumo. *Este trabalho apresenta uma metodologia para detecção de anomalias em redes, combinando a Média Móvel de Poisson (PMA) e a Integral de Choquet com Medidas de Potência. A proposta busca aprimorar a precisão em cenários com baixa dependência histórica, ajustando o parâmetro q conforme a dinâmica dos dados. Utilizando o conjunto de dados CIC-IDS2017, os resultados mostraram uma redução de 5,31% no MAE, aumento de 6,78% na precisão e melhora de 0,17% na acurácia em relação ao PMA, evidenciando a eficácia do modelo híbrido para predição de ataques.*

Palavras-chave: *Detecção de Anomalias; Integral de Choquet; Medidas de Potência.*

1. Introdução

As redes de computadores são essenciais para serviços financeiros, sistemas hospitalares e diversas atividades da sociedade, tornando sua segurança fundamental [Dalmazo et al. 2017]. Com o crescimento dos dispositivos conectados e do volume de dados transmitidos, o monitoramento do tráfego tornou-se cada vez mais necessário [Zeufack et al. 2021].

Nesse cenário, ataques cibernéticos podem provocar alterações nos padrões de tráfego, permitindo sua identificação por métodos de detecção de anomalias [Santo et al. 2023]. Essas técnicas utilizam desde modelos estatísticos até abordagens de aprendizado de máquina para identificar comportamentos suspeitos e contribuir para a segurança das redes.

Este trabalho investiga a detecção de anomalias em tráfego de redes utilizando a Média Móvel de Poisson (PMA) e a Integral de Choquet parametrizada por Medidas de Potência. A proposta explora diferentes funções para adaptar o parâmetro q às características locais dos dados em janelas deslizantes, buscando reduzir o erro de predição e melhorar a acurácia e a precisão na detecção de ataques.

A principal contribuição consiste na avaliação de uma abordagem de agregação fuzzy com parametrização dinâmica, comparando seu desempenho com o PMA e analisando o impacto de diferentes tamanhos de janela, sem necessidade de treinamento prévio.

O artigo está organizado da seguinte forma: a Seção 2 apresenta os trabalhos relacionados; a Seção 3 descreve a metodologia; a Seção 4 apresenta os resultados; e a Seção 5 reúne as conclusões e os trabalhos futuros.

2. Trabalhos Relacionados

Esta seção revisa estudos sobre detecção de anomalias em redes, com foco nas Integrais de Choquet [Amorim et al. 2023]. Métodos baseados em densidade apresentam bons resultados, mas possuem limitações com dados incompletos ou incertos, motivando o uso de lógica fuzzy e teoria rough [Yuan et al. 2023]. Outros estudos compararam algoritmos de detecção de anomalias em diferentes séries temporais [Zeufack et al. 2021].

As médias móveis apresentam bons resultados em cenários de baixa dependência histórica [Dalmazo et al. 2018], enquanto a agregação fuzzy permite explorar relações não lineares entre os dados. Estudos anteriores aplicaram a Integral de Choquet na detecção de anomalias em redes [Ayres et al. 2024]. Ayres et al. [Ayres et al. 2026] investigaram sua parametrização por Medidas de Potência, avaliando funções e tamanhos de janela para reduzir erros de predição e analisar acurácia e precisão. Neste trabalho, são investigadas as funções AUTO, DIFF, CVAR e SKEW para adaptar o parâmetro q às características do tráfego.

3. Detecção de Anomalias com Medidas de Potência

Esta seção apresenta a metodologia para detecção de anomalias em tráfego de redes, combinando a Média Móvel de Poisson (PMA) e a Integral de Choquet parametrizada por Medidas de Potência. A abordagem utiliza janelas deslizantes para analisar o comportamento do tráfego e avaliar o impacto do tamanho das janelas no erro de predição, na acurácia e na precisão. O fluxo da metodologia é apresentado na Figura 1a.

3.1. Modelo PMA

A Média Móvel de Poisson (PMA) utiliza a distribuição de Poisson para ponderar observações em janelas deslizantes, atualizadas a cada novo valor, sem necessidade de treinamento prévio [Dalmazo et al. 2017]. O parâmetro λ está relacionado ao tamanho da janela e à distribuição dos pesos.

Estudos anteriores identificaram menores erros do PMA em comparação às médias móveis SMA, WMA e EMA em cenários de baixa dependência histórica [Dalmazo et al. 2017]. Assim, o PMA é adotado como referência para avaliar a Integral de Choquet com Medidas de Potência.

3.2. Medidas Fuzzy

As medidas fuzzy [Murofushi et al. 1994] representam a importância de elementos e seus subconjuntos, permitindo modelar relações não independentes ou uniformes entre os dados.

Para um conjunto $N = \{1, \dots, n\}$, uma função $m : 2^N \rightarrow [0, 1]$ é uma medida fuzzy se satisfizer: **(m1)** monotonicidade, em que $X \subseteq Y$ implica $m(X) \leq m(Y)$; e **(m2)** condições de contorno, com $m(\emptyset) = 0$ e $m(N) = 1$.

Neste estudo, utiliza-se a Medida de Potência (*Power Measure*) [Barrenechea et al. 2013], definida por $m(A) = (|A|/n)^q$, com $A \subseteq N$ e $q > 0$. O parâmetro q controla a importância dos subconjuntos conforme sua cardinalidade [Lucca et al. 2019], sendo determinado dinamicamente a partir das características dos dados em cada janela deslizante.

3.3. Modelo Choquet

A Integral de Choquet é uma função de agregação que considera a ordenação dos valores e a importância de seus subconjuntos por meio de uma medida fuzzy [Grabisch and Labreuche 2010], permitindo representar relações não aditivas entre os elementos.

Para um vetor $x = (x_1, \dots, x_n)$, a Integral de Choquet é definida por $C_m(x) = \sum_{i=1}^n (x_{(i)} - x_{(i-1)}) m(A_{(i)})$, em que $x_{(1)} \leq \dots \leq x_{(n)}$, $x_{(0)} = 0$ e $A_{(i)} = \{(i), \dots, (n)\}$ representa o subconjunto dos valores ordenados.

Neste trabalho, a Integral de Choquet é aplicada às observações de cada janela deslizante e parametrizada pela Medida de Potência. O parâmetro q é definido a partir das características da janela, adaptando a agregação ao comportamento local do tráfego. As funções utilizadas nessa parametrização são avaliadas na Seção 4.

3.4. Dataset

O conjunto de dados utilizado foi o CIC-IDS2017¹, disponibilizado pelo *Canadian Institute for Cybersecurity*. O conjunto contém tráfego benigno e malicioso capturado em ambiente controlado durante cinco dias úteis, totalizando aproximadamente 51,1 GB de dados utilizados neste estudo.

O pré-processamento foi realizado com a ferramenta TCP-Stats, que extraiu estatísticas como pacotes por segundo, total de pacotes e registros temporais. Com auxílio da biblioteca Pandas, os dados foram organizados e unificados em um arquivo CSV ordenado cronologicamente, formando a série temporal utilizada pelos modelos.

Como o PMA e as abordagens baseadas na Integral de Choquet não exigem treinamento prévio, os dados não foram divididos em conjuntos de treinamento e teste. As previsões foram realizadas sequencialmente a partir das observações de cada janela deslizante.

3.5. Modelo Conceitual

As funções AUTO, DIFF, CVAR e SKEW, apresentadas na Tabela 1, representam, respectivamente, a relação entre observações consecutivas, a variação absoluta, a dispersão

¹<https://www.unb.ca/cic/datasets/ids-2017.html>

Tabela 1. Funções utilizadas para determinar q

ID	Funções
(a)	$T_{AUTO}(v) = \frac{1}{n-1} \sum_{i=1}^{n-1} v_i v_{i+1}$
(b)	$T_{DIFF}(v) = \frac{1}{n} \sum_{i=1}^{n-1} v_{i+1} - v_i $
(c)	$T_{CVAR}(v) = \frac{\sigma(v)}{\bar{v}}$
(d)	$T_{SKEW}(v) = \frac{\frac{1}{n} \sum_{i=1}^n (v_i - \bar{v})^3}{\sigma(v)^3}$

relativa e a assimetria dos dados. Seus resultados são utilizados para definir o parâmetro q .

Conforme a Figura 1a, os dados são organizados em janelas deslizantes, nas quais são aplicados o PMA e a Integral de Choquet parametrizada pelas funções da Tabela 1. O erro de predição é avaliado para diferentes tamanhos de janela, e a configuração selecionada é utilizada na detecção de ataques.

3.6. Comparação com Modelos Contemporâneos

Métodos de aprendizado de máquina e profundo, como redes LSTM, são utilizados na análise de séries temporais e detecção de anomalias. Embora modelem relações temporais complexas, exigem treinamento e maior custo computacional. Em contrapartida, o PMA e a Integral de Choquet realizam predições em janelas deslizantes, sem treinamento prévio. Análises de complexidade [Dalmazo et al. 2026] indicam custos de $O(n)$ para o PMA, $O(n^2)$ para a implementação considerada da Integral de Choquet e $O(E \cdot n \cdot w \cdot h^2)$ para o treinamento de uma LSTM. Assim, a agregação fuzzy representa uma alternativa sem treinamento, cuja comparação experimental com modelos contemporâneos permanece como trabalho futuro.

4. Avaliação do Modelo

Esta seção apresenta e discute os resultados obtidos com as diferentes configurações avaliadas. A análise considera inicialmente o erro de predição e, posteriormente, o desempenho na detecção de ataques por meio das métricas de acurácia e precisão.

4.1. Erros de Predição

O desempenho foi avaliado pelo Erro Médio Absoluto (MAE), considerando diferentes tamanhos de janela para o PMA e a Integral de Choquet parametrizada pelas funções AUTO, DIFF, CVAR e SKEW. Conforme a Figura 1b, o erro varia conforme a função e o tamanho da janela, com a CVAR apresentando o menor erro nas configurações de melhor desempenho, sendo selecionada para a detecção de ataques.

4.2. Detecção de Ataques

Os rótulos do CIC-IDS2017 foram utilizados como *ground truth* para comparar as classificações do método e calcular as métricas de acurácia e precisão.

O *threshold* foi definido conforme Dalmazo *et al.* [Dalmazo et al. 2017], considerando a variação entre as médias de janelas consecutivas, calculada por $r = \left| \frac{\bar{x}_t}{\bar{x}_{t-1}} - \frac{\bar{x}_{t-1}}{\bar{x}_t} \right|$. Quando $r > (1 + \alpha)$, com $\alpha = 0,05$, a variação indica uma possível anomalia. Esse critério foi aplicado ao PMA, à Integral de Choquet e à sua versão parametrizada por CVAR, considerando diferentes tamanhos de janela.

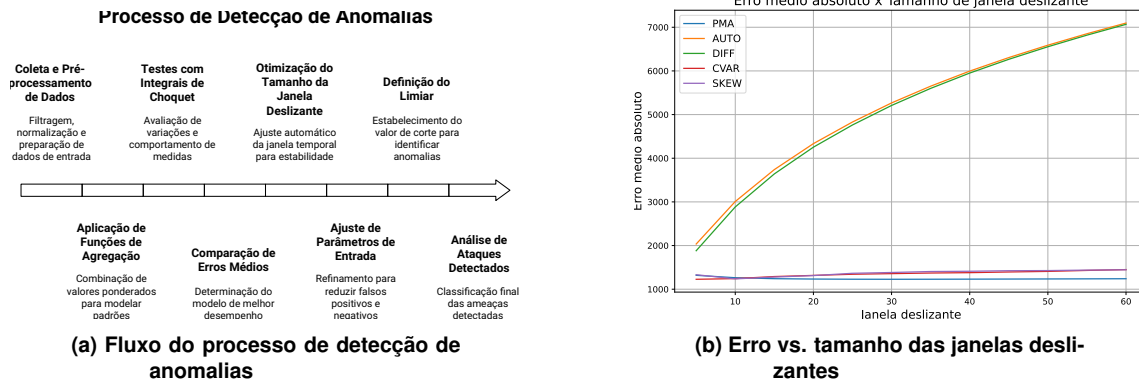


Figura 1. Fluxo da metodologia e análise do erro de predição

Conforme as Figuras 2a e 2b, a parametrização com CVAR apresentou variações de acurácia e precisão conforme o tamanho da janela. O melhor desempenho conjunto ocorreu com janela de tamanho 7, utilizada na comparação com o PMA.

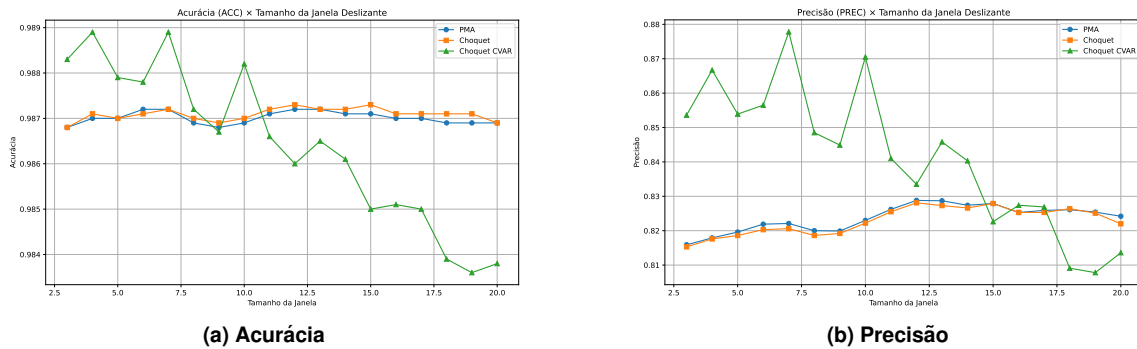


Figura 2. Acurácia e precisão em função do tamanho da janela deslizante

5. Considerações Finais

Este trabalho investigou a detecção de anomalias em tráfego de redes utilizando a Média Móvel de Poisson (PMA) e a Integral de Choquet parametrizada por Medidas de Potência. Foram avaliadas diferentes funções para definir o parâmetro q a partir dos dados das janelas deslizantes. Entre elas, a CVAR apresentou o melhor desempenho, sendo utilizada na etapa de detecção de ataques.

O melhor resultado ocorreu com janela de tamanho 7, apresentando redução de 5,31% no MAE, aumento de 6,78% na precisão e melhora de 0,17% na acurácia em relação ao PMA. Esses resultados indicam que a parametrização da Integral de Choquet com base nas características locais dos dados pode melhorar a predição e a detecção de anomalias.

Entretanto, o estudo apresenta limitações, como o uso exclusivo do CIC-IDS2017, a ausência de comparações com métodos contemporâneos de aprendizado de máquina e profundo e a falta de testes de significância estatística. Assim, os resultados demonstram o potencial da abordagem no cenário avaliado, sem estabelecer sua superioridade geral.

Como trabalhos futuros, pretende-se avaliar outros conjuntos de dados, incorporar novas métricas, comparar a abordagem com modelos de aprendizado de máquina e profundo e realizar análises estatísticas. Também serão investigadas medidas fuzzy alternativas e estratégias de otimização dinâmica dos parâmetros e das janelas deslizantes.

Referências

- Amorim, M., Dimuro, G., Borges, E., Dalmazo, B. L., Marco-Detchart, C., Lucca, G., and Bustince, H. (2023). Systematic review of aggregation functions applied to image edge detection. *Axioms*, 12(4).
- Ayres, D., Quevedo, A., Dimuro, G., Lucca, G., and Dalmazo, B. L. (2026). Reducing mean absolute error in attack predictions with power-parametrized choquet integrals. *Internet Technology Letters*, 9(5):e70368.
- Ayres, D., Quevedo, A., Lucca, G., Dimuro, G., and Dalmazo, B. (2024). Comparando médias móveis com integral de choquet para detectar anomalias no tráfego de redes. In *Anais Estendidos do XXIV Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais*, pages 353–357, Porto Alegre, RS, Brasil. SBC.
- Barrenechea, E., Bustince, H., Fernandez, J., Paternain, D., and Sanz, J. A. (2013). Using the Choquet integral in the fuzzy reasoning method of fuzzy rule-based classification systems. *Axioms*, 2(2):208–223.
- Dalmazo, B. L., Ayres, D. G., Lucca, G., Bedregal, B., Bustince, H., and Dimuro, G. P. (2026). Predicting network traffic: Leveraging temporal capacities in fuzzy integrals to capture temporal interrelationships among data. *IEEE Transactions on Fuzzy Systems*, pages 1–11.
- Dalmazo, B. L., Vilela, J. P., and Curado, M. (2017). Performance analysis of network traffic predictors in the cloud. *Journal of Network and Systems Management*, 25:290–320.
- Dalmazo, B. L., Vilela, J. P., and Curado, M. (2018). Triple-similarity mechanism for alarm management in the cloud. *Computers & Security*, 78:33–42.
- Grabisch, M. and Labreuche, C. (2010). A decade of application of the choquet and sugeno integrals in multi-criteria decision aid. *Annals of Operations Research*, 175(1):247–286.
- Lucca, G., Sanz, J. A., Dimuro, G. P., Borges, E. N., Santos, H., and Bustince, H. (2019). Analyzing the performance of different fuzzy measures with generalizations of the choquet integral in classification problems. In *2019 IEEE International Conference on Fuzzy Systems (FUZZ-IEEE)*, pages 1–6.
- Murofushi, T., Sugeno, M., and Machida, M. (1994). Non-monotonic fuzzy measures and the Choquet integral. *Fuzzy Sets and Systems*, 64(1):73 – 86.
- Santo, Y., Immich, R., Dalmazo, B. L., and Riker, A. (2023). Fault detection on the edge and adaptive communication for state of alert in industrial internet of things. *Sensors*, 23(7).
- Yuan, Z., Chen, B., Liu, J., Chen, H., Peng, D., and Li, P. (2023). Anomaly detection based on weighted fuzzy-rough density. *Applied Soft Computing*, 134:109995.
- Zeufack, V., Kim, D., Seo, D., and Lee, A. (2021). An unsupervised anomaly detection framework for detecting anomalies in real time through network system’s log files analysis. *High-Confidence Computing*, 1(2):100030.