Detecção On-line e Antecipada de Ataques à Rede usando Matrix Profile

Diego Abreu[1], **Antônio Abelém**[1]

[1] Universidade Federal do Pará - UFPA

Abstract. *In the digital age, the increasing sophistication and variety of cyber threats highlight the importance of strengthening cybersecurity to protect current networks. This study proposes an approach for the early detection of attacks, using the Matrix Profile (MP) technique to analyze network data streams as time series in an online manner. This method focuses on identifying anomalies in the network as early indicators of network attacks, addressing the limitations of existing Machine Learning systems that predominantly rely on offline training and struggle to recognize patterns of new or untrained attacks. Our proposal was evaluated in various attack scenarios, demonstrating superior performance metrics compared to traditional methods such as CUSUM, EWMA, and ARIMA.*

Resumo. *Na era digital, a crescente sofisticação e variedade de ameaças cibernéticas destacam a importância de fortalecer a cibersegurança para proteger as redes atuais. Este estudo propõe uma abordagem para a detecção antecipada de ataques, utilizando a técnica Matrix Profile (MP) para analisar de forma online fluxos de dados de rede como séries temporais. Este método concentra-se na identificação de anomalias na rede como indicadores de ataques de rede, abordando as limitações dos sistemas de Aprendizado de Máquina existentes que dependem predominantemente de treinamento offline e têm dificuldades em reconhecer padrões de ataques novos ou não treinados. Nossa proposta foi avaliada em diversos cenários de ataque, demonstrando métricas de desempenho superiores quando comparado com métodos tradicionais como CUSUM, EWMA e ARIMA.*

1. Introdução

A segurança da informação é uma preocupação crescente na era digital, onde a quantidade e a complexidade dos ataques cibernéticos aumentam continuamente. Neste cenário, a proteção de dados torna-se uma prioridade, não apenas para a segurança individual, mas também para a integridade e confiabilidade das operações na Internet. A relevância dos dados em nosso cotidiano e no ambiente de negócios eleva substancialmente as consequências de eventuais ataques, tornando a segurança cibernética um campo de constante evolução e desafio [He et al. 2023].

Métodos tradicionais de detecção de ataques, embora eficazes em vários contextos, estão se tornando insuficientes perante a sofisticação e a variedade das ameaças modernas [Ahmad et al. 2023]. Os agentes maliciosos estão continuamente aprimorando suas técnicas, apontando para a necessidade de métodos de detecção mais avançados e precisos. Neste contexto, a detecção antecipada de ataques (*early attack detection*), identifica a ação maliciosa logo nos primeiros estágios do ataque e é crucial para prevenir danos significativos à rede e seus usuários.

Nesse sentido, diversas abordagens de segurança têm sido propostas utilizando técnicas de Aprendizado de Máquina (AM), entretanto ainda enfrentam uma grande dificuldade devido à grande diversidade e complexidades dos dados gerados tanto pelo comportamento normal da rede quanto pela ação de agentes maliciosos [Ahmad et al. 2023]. Além disso, muitas dessas abordagens se baseiam em treinamento *off-line* de modelos que identificam o padrão de ataques previamente conhecidos, dificultando a identificação de ataques não treinados, como ataques novos ou não considerados no treino [Gomes et al. 2019]. Assim, muitas das técnicas propostas têm dificuldade de serem implementadas em ambientes de produção real [Jacobs et al. 2022].

Deste modo, este trabalho busca realizar a identificação antecipada de ataques utilizando a detecção de anomalias da rede como indicativo da ocorrência de ataques. Especificamente, nossa proposta consiste na implementação da técnica Matrix Profile (MP) [Yeh et al. 2016] para realizar a análise do fluxo de dados da rede como série temporal, identificando de forma *on-line* (por *stream* de dados) [Abreu and Abelém 2022, Gomes et al. 2019] as anomalias da rede que indicam o início de ataques. Ao longo deste estudo, é apresentada uma análise detalhada dessa técnica, explorando sua aplicabilidade, eficácia e os resultados obtidos na detecção de ataques à rede. Nossas principais contribuições consistem em:

- Desenvolvimento de um sistema de detecção antecipada de ataques utilizando o Matrix Profile.
- Análise detalhada das características mais relevantes para o Matrix Profile identificar tipos diferentes de ataques.
- Comparação do desempenho do sistema com outras técnicas do estado da arte.

O resto do trabalho está estruturado assim: Seção 2 detalha a detecção de anomalias utilizando o Matrix Profile. A Seção 3 revisa trabalhos relacionados, comparando a nossa proposta com o estado da arte. A proposta do estudo é detalhada na Seção 4, enfatizando a aplicação do Matrix Profile na detecção antecipada de ataques. A metodologia, incluindo as bases de dados e os parâmetros dos experimentos, é apresentada na Seção 5. As Seções 6 e 7, respectivamente, discutem os resultados obtidos e concluem o estudo, apontando para futuras direções de pesquisa.

2. Detecção de Anomalia com Matrix Profile

Séries temporais são conjuntos de observações coletadas sequencialmente ao longo do tempo, representando uma variedade de fenômenos através de padrões ou tendências dos dados [Zhou and Tang 2016]. A detecção de anomalias nessas séries envolve a identificação de padrões ou pontos de dados que se desviam significativamente do comportamento normal ou esperado, sendo essencial para antecipar atividades suspeitas ou irregulares, como potenciais ataques cibernéticos, antes que causem danos significativos [Ahmad et al. 2023].

As séries temporais são frequentemente ruidosas, contendo muitas flutuações aleatórias, o que pode dificultar a identificação de padrões ou tendências. Essas mudanças podem ser devido a diversos fatores, como alterações nas tendências, sazonalidade ou devido um novo comportamento dos dados. Nesse contexto, diversas técnicas têm sido propostas para entender os padrões das séries temporais e identificar corretamente as anomalias existentes. Nesse trabalho, além da técnica Matrix Profile, iremos utilizar em nosso

estudo de caso as técnicas CUSUM [Lu and Tong 2009], ARIMA [Yaacob et al. 2010] e EWMA [Zhou and Tang 2016], as quais são amplamente utilizadas no contexto de detecção de anomalias em séries temporais.

2.1. Funcionamento do Matrix Profile

O Matrix Profile busca identificar anomalias e tendências na série temporal através de junções de similaridade, comparando trechos da série temporal entre si [Yeh et al. 2016]. O método consiste em dois componentes principais: um perfil de distância e um índice de perfil. O perfil de distância é um vetor que contém as distâncias euclidianas z-normalizadas mínimas entre cada par de trechos. O índice de perfil, por outro lado, armazena o índice da sub-sequência mais próxima correspondente a cada trecho. O Algoritmo 1 apresenta o cálculo do Matrix Profile. O cálculo do Matrix Profile segue um procedimento de janela deslizante. Dado um tamanho de janela m, o processo é o seguinte:

1. Calcula-se as distâncias euclidianas z-normalizadas de cada subsequência de tamanho m com todas as outras subsequências da série temporal.
2. Aplica-se uma zona de exclusão para evitar correspondências triviais, como um segmento correspondendo a si mesmo.
3. Atualiza-se o perfil de distância com os valores mínimos encontrados.
4. Registra-se o índice da primeira correspondência mais próxima para cada segmento.

Esses cálculos de distância ocorrem $n - m + 1$ vezes; onde n é o comprimento da série temporal (T) e m é o tamanho da janela. Como as sub-sequências são extraídas da própria série temporal, uma zona de exclusão é necessária para prevenir correspondências triviais. Por exemplo, um trecho correspondendo a si mesmo ou muito próximo a si é considerado uma correspondência trivial. A zona de exclusão corresponde a metade do tamanho da janela (m) antes e depois do índice atual da janela. Os valores desses índices não são considerados ao calcular a distância mínima e o índice da correspondência mais próxima.

O resultado do Matrix Profile é um gráfico que pode ser utilizado para encontrar *Motifs* e *Discords*. *Motif* é um padrão repetido em uma série temporal e um *Discord* é uma anomalia. O Matrix Profile armazena as distâncias no espaço euclidiano, significando que uma distância próxima de 0 é mais similar a outra subsequência na série temporal, e uma distância distante de 0, é diferente de qualquer outra subsequência. A extração das menores distâncias fornece os *Motifs* e as maiores distâncias fornecem os *Discords*.

2.2. Matrix Profile On-line

O Matrix Profile pode ser utilizado de forma *on-line* através do algoritmo STAMPI [Gharghabi et al. 2017], apresentado no Algoritmo 2. O STAMPI não precisa considerar a disponibilidade completa da série temporal, e utiliza os dados de forma incremental para gerar o Matrix Profile. Essa abordagem é fundamental para lidar com dados em *stream*, extraindo os *Motifs* e *Discords* da série temporal de forma eficaz.

O STAMPI atualiza o perfil matricial à medida que novos dados são recebidos, sem a necessidade de recalcular todo o perfil a partir do zero. Isso é feito acompanhando

Algorithm 1 Cálculo do Matrix Profile

Entrada: Série Temporal T, Tamanho da Janela m
Saída: Matrix Profile (MP), Índice de Perfil (PI)
Inicialize MP com valores infinitos
Inicialize PI com zeros
for cada índice i em T **do**
    for cada índice j em T **do**
        if $|i - j| > \frac{m}{2}$ **then**
            Calcule a distância D entre $T[i : i + m]$ e $T[j : j + m]$
            if $D < MP[i]$ **then**
                $MP[i] \leftarrow D$
                $PI[i] \leftarrow j$
            end if
        end if
    end for
end for

os valores extremos (mínimos e máximos) do perfil matricial em crescimento. Um novo par de *Motifs* é reportado quando um novo valor mínimo é detectado, e um novo *Discord* é identificado ao observar um novo valor máximo.

Algorithm 2 Algoritmo STAMPI para Matrix Profile Online

Entrada: Série Temporal Original TA, Novo Ponto de Dados t, Perfil Matricial PAA, Índice do Perfil Matricial IAA
Saída: Perfil Matricial Atualizado PAA_{new}, Índice do Perfil Matricial Atualizado IAA_{new}
$TA_{\text{new}} \leftarrow [TA, t]$
$S \leftarrow$ última subsequência em TA_{new}, $idx \leftarrow$ índice de S em TA_{new}
$D \leftarrow$ similaridade(S, TA)
$PAA, IAA \leftarrow$ MenorValorCorrespondente(PAA, IAA, D, idx)
$pAA_{\text{last}}, iAA_{\text{last}} \leftarrow$ EncontrarMenorValor(D)
$PAA_{\text{new}} \leftarrow [PAA, pAA_{\text{last}}]$, $IAA_{\text{new}} \leftarrow [IAA, iAA_{\text{last}}]$
return $PAA_{\text{new}}, IAA_{\text{new}}$

2.3. Matrix Profile Multidimensional

O Matrix Profile também pode ser utilizado na versão multidimensional, que considera várias séries temporais como entrada ao mesmo tempo. O Algoritmo mSTAMP [Yeh et al. 2017] calcula o perfil matricial de *k* séries temporais, que podem ser resultado do monitoramento de *features* diferentes, em busca de *Motifs* que indiquem a presença de anomalias.

O mSTAMP, apresentado no Algoritmo 3, recebe como entrada a série temporal T e um comprimento de interesse m para as subsequências a serem analisadas. O perfil de matriz resultante P tem dimensões $d \times (n - m + 1)$, onde cada coluna representa o perfil de uma subsequência particular ao longo das várias dimensões de T. No início, o algoritmo inicializa P como uma matriz de infinitos, representando as distâncias iniciais

Algorithm 3 Algoritmo mSTAMP

Entrada: Série temporal $T \in \mathbb{R}^{d \times n}$, comprimento de subsequência de interesse $m \in \mathbb{Z}$
Saída: Conjunto de perfil de matriz k-dimensional $P \in \mathbb{R}^{d \times (n-m+1)}$
$P \leftarrow$ tamanho $d \times (n - m + 1)$
$idxs \leftarrow$ inteiros de 1 a $(n - m + 1)$
for cada idx **em** $idxs$ **do**
    $D \leftarrow$ tamanho $d \times (n - m + 1)$ matriz zero
    for $i \leftarrow 1$ **até** d **do**
        $Q \leftarrow T[i, idx : idx + m - 1]$
        $D[i, :] \leftarrow$ perfilDistancia$(Q, T[i, :])$
    end for
    $D \leftarrow$ ordenarColunaAscendente(D)
    $D' \leftarrow$ comprimento $(n - m + 1)$
    for $i \leftarrow 1$ **até** d **do**
        $D' \leftarrow D' + D[i, :]$
        $D'' \leftarrow D'/i$
        $P[i, :] \leftarrow$ MenorValorCorrespondente$(P[i, :], D'')$
    end for
end for
retorna P

como indefinidamente grandes, e prepara um conjunto de índices que representam todas as possíveis subsequências de interesse. Para cada índice, é construído uma matriz D que armazena os perfis de distância de todas as dimensões de T. Isso é feito extraindo a subsequência Q da série temporal T e calculando o perfil de distância de Q em relação a toda a série temporal para cada dimensão i. Após a ordenação ascendente das colunas de D, o algoritmo atualiza P com o mínimo elemento entre o perfil atual e as distâncias acumuladas divididas pelo índice da dimensão. Este processo é repetido para todos os índices, acumulando as informações de distância e refinando o perfil de matriz. O algoritmo retorna P, que encapsula as informações sobre padrões regulares e anomalias em todas as dimensões da série temporal analisada.

A versão multidimensional do Matrix Profile pode ser utilizada quando a anomalia de rede não é detectada utilizando apenas uma dimensão, ou apenas uma *feature*. Nesse caso, a adição de outras dimensões ajuda a detectar variações multidimensionais, que podem indicar a ocorrência da anomalia. No contexto do nosso trabalho, iremos explorar também o MP Multidimensional e comparar o desempenho com o MP de uma dimensão, que considera apenas uma *feature* na sua análise.

3. Trabalhos Relacionados

A proteção efetiva das redes contra ataques maliciosos ainda é um grande desafio, com diversas pesquisas nesse contexto. O estado da arte abrange uma série de técnicas de AM propostas para detectar a ocorrência de ação maliciosa [Ahmad et al. 2023], seja através de classificadores que diferenciam os dados de ataque do comportamento considerado normal da rede [Nascimento et al. 2023], seja com técnicas de agrupamento, que buscam

Tabela 1. Comparação entre Nossa Proposta e Trabalhos Relacionados.

	On-line	Detecção Antecipada	MP	Múltiplos Ataques
Nossa Proposta	✓	✓	✓	✓
[Elbez et al. 2023]	x	✓	x	x
[De Neira et al. 2023]	x	✓	x	x
[Anton et al. 2019]	x	x	✓	x
[Alzahrani et al. 2022]	x	x	✓	x
[Alotaibi and Lisitsa 2021]	x	x	✓	x

identificar perfis de ataque em meio ao conjunto de dados normais [Abreu et al. 2020]. Essas técnicas são aplicadas, em um ambiente de produção, principalmente no contexto de análise de dados suspeitos de serem de ataques, geralmente realizado durante ou depois da ocorrência do ataque [Kim et al. 2022]. De outro modo, nossa proposta tem como foco a detecção antecipada de ataques, identificando o ataque logo no início, que é fundamental para interromper ameaças emergentes antes que elas se concretizem. A Tabela 1 apresenta os principais pontos de comparação da proposta com os trabalhos relacionados.

Como a Tabela 1 destaca, algumas pesquisas recentes também têm focado no desafio da detecção antecipada de ataques. Em Elbez et al. (2023) [Elbez et al. 2023] são investigados ataques de *poisoning* (envenenamento) em redes de subestações que podem resultar em ameaças como ataques de *Denial of Service* (DoS) ou ataques de *flooding* (inundação), aplicando uma técnica própria baseada no ARIMA para análise da série temporal. Em De Neira et al. (2023) [De Neira et al. 2023], é adotada uma abordagem não supervisionada, onde são criadas *features* baseadas em curtose (*kurtosis*), assimetria (*skewness*) e coeficiente de variação a partir de dados de rede, como IPs de origem e destino. Esses indicadores são depois utilizados para classificar os dados com o algoritmo *k-means*, permitindo a detecção antecipada de ataques. Contudo, essa metodologia depende da coleta de dados em lote [Gomes et al. 2019], o que significa que as *features* são geradas a partir de um conjunto de dados previamente adquiridos, dispondo de todo o espaço de dados para análise. Em contrapartida, a nossa proposta analisa os dados de forma *on-line*, por meio de dados em *stream* [Gomes et al. 2019], processando as informações à medida que chegam ao sistema de detecção. Isso torna o método adequado para a aplicação na detecção de ataques em tempo real, sem a necessidade de treinamento ou análise prévia dos dados de ataques.

Recentemente, outras pesquisas também aplicaram a técnica de Matrix Profile no contexto de segurança de redes. Em Anton et al. (2019) [Anton et al. 2019], o Matrix Profile foi integrado com redes neurais recorrentes do tipo Long Short-Term Memory (LSTM) para ataques em sistemas industriais, levando em consideração *features* como volume, pressão e temperatura. Já Alzahrani et al. (2022) [Alzahrani et al. 2022] aplicou o MP na detecção de ataques DDoS em dispositivos de Internet das Coisas (IoT), utilizando métricas como uso da CPU, voltagem e consumo de memória para identificar anomalias. Esta aplicação provou ser eficaz ao indicar a presença de atividades maliciosas na rede quase no exato momento de seu início. Além disso, Alotaibi e Lisitsa (2021) [Alotaibi and Lisitsa 2021] também utilizaram o Matrix Profile para detecção de ataques do tipo *Distributed Denial of Service* (DDoS). Usando a base CIC-IDS-2019, eles geraram

o MP utilizando diferentes configurações de ataques e *features*, e analisaram a eficácia do MP em detectar todo o período de duração do ataque, utilizando os *Motifs* (padrões recorrentes do MP) como indicador do sistema de detecção, obtendo acurácia média de 75% para os melhores casos. De outro modo, nossa proposta utiliza o MP para detectar o início da ocorrência de ataques, utilizando os *Discords* para indicar as anomalias da rede.

Assim, observa-se que a proposta em questão é a única entre os trabalhos relacionados que utiliza o Matrix Profile de forma *on-line* para a detecção antecipada de diversos ataques de rede. O objetivo é alcançar a detecção dos ataques de maneira mais precisa, conforme será detalhado na próxima seção.

4. Sistema Proposto: Detecção Antecipada de Ataques utilizando Matrix Profile

A detecção antecipada de ataques, ou *early detection*, é um conceito importante na segurança cibernética que envolve a identificação de eventos anômalos, como ataques à rede, no início de sua ocorrência, permitindo ações corretivas rápidas para minimizar potenciais danos. Esta abordagem é desafiadora, uma vez que requer a identificação de padrões suspeitos antes que se manifestem completamente. Para abordar a detecção antecipada de ataques, é considerada a seguinte modelagem de ameaça (*Threat Model*):

- **Adversários**: Os adversários podem ser atacantes externos ou internos, com diferentes níveis de conhecimento e sofisticação. Eles podem utilizar um ou múltiplos dispositivos para realizar os ataques.
- **Objetivos dos Adversários**: Os adversários buscam comprometer a integridade e a disponibilidade do sistema de rede. Eles podem realizar ataques como exploração de vulnerabilidades, injeção de malware ou tentativas de negação de serviço.
- **Amplitude de Ataques**: São considerados uma ampla gama de ataques à rede. Isso inclui ataques que possam ser já conhecidos pelo sistema de detecção ou desconhecidos.
- **Objetivo do Detector**: O objetivo do sistema é identificar atividades anormais no tráfego de dados antes que causem impactos significativos. Isso significa que a detecção deve ocorrer em estágios iniciais, quando os padrões anômalos são recentes.

A modelagem do problema pode ser definida da seguinte forma: seja T uma série temporal representando o tráfego de dados em uma rede, o objetivo é identificar pontos em T que indiquem atividades anormais, sugerindo a ocorrência de um ataque. Utilizamos o Matrix Profile MP de T, buscando valores em MP que indiquem padrões atípicos na série temporal, no caso os *discords* do MP. Ao identificar essas anomalias, podemos tomar medidas proativas para investigar e mitigar potenciais ataques cibernéticos antes que causem danos à rede. O funcionamento da proposta é ilustrado na Figura 1 e pode ser detalhado da seguinte forma:

1. **Monitoramento da rede:** A coleta de dados da rede é feita em tempo real por meio de um fluxo contínuo de informações.
2. **Extração das características da rede:** Após a coleta dos dados, é necessário extrair características (*features*) relevantes que descrevam o comportamento da rede.

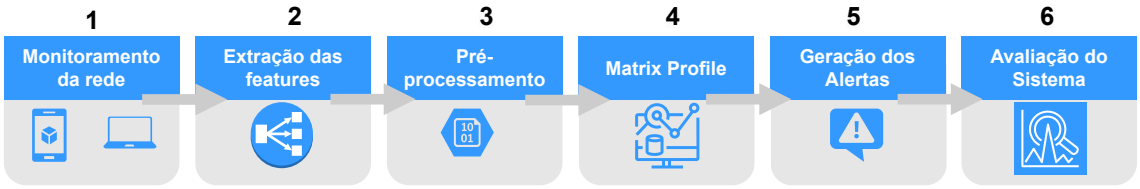


Figura 1. Funcionamento da Detecção Antecipada de Ataques Baseada em Matrix Profile.

3. **Pré-processamento:** Para garantir que os dados estejam em um formato adequado para análise é realizado o pré-processamento dos dados.
4. **Geração do Matrix Profile:** Nesta etapa, a técnica do Matrix Profile é aplicada, destacando os *discords* da série temporal original.
5. **Geração de alertas de ataques:** Para a detecção antecipada do ataque, quando um *discord* é encontrado, o sistema gera um alerta de ataque. Os alertas gerados são enviados para os responsáveis pela segurança cibernética, permitindo uma resposta para investigação e mitigação de possíveis ameaças.
6. **Avaliação do Sistema**: Após a realização da detecção do ataque, é feita a coleta das métricas necessárias para se realizar a avaliação do sistema.

A abordagem de detecção antecipada de ataques baseada em Matrix Profile busca proteger sistemas de rede contra ameaças cibernéticas, uma vez que permite identificar comportamentos suspeitos antes que eles causem danos significativos.

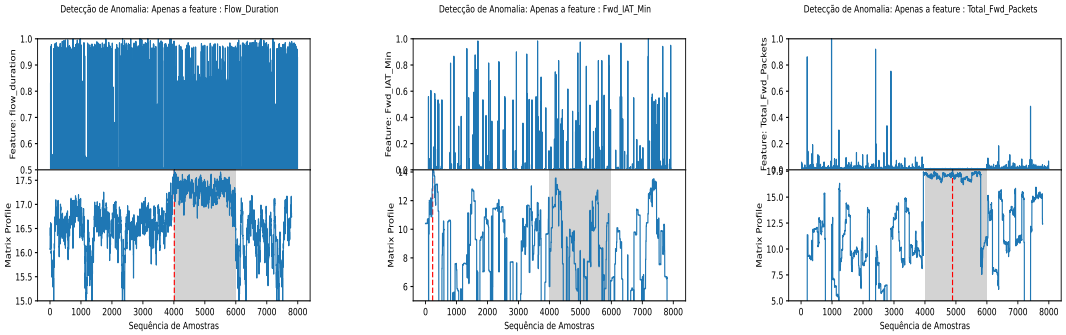
5. Estudo de Caso

5.1. Configuração dos Experimentos

Para avaliar a proposta, foi utilizado a base de dados CIC-IDS-17 [Sharafaldin et al. 2018], que contém dados de tráfego de rede, abrangendo tanto comportamento normal, quanto diferentes tipos de ataques. Essa base é amplamente utilizada no contexto de detecção e classificação de ameaças cibernéticas [Kim et al. 2022]. O CIC-IDS-17 contém 2,830,743 instâncias e 84 características (*features*) de rede. Para esse estudo de caso, são utilizados os ataques DDoS, DoS, análise de porta (Portscan), FTP-Patator (FTP) e força bruta (Brute). Os dados da base CIC-IDS-17 foram utilizados como entrada para o sistema proposto, sendo processados como um fluxo contínuo de *stream* de dados em uma série temporal. O Matrix profile, em sua versão *on-line*, foi utilizado para realizar detecção antecipada dos ataques da base CIC-IDS-17, tanto na versão de uma dimensão, como na versão multidimensional. As técnicas CUSUM, EWMA, ARIMA, também foram utilizadas e serão comparadas ao MP na detecção antecipada dos ataques.

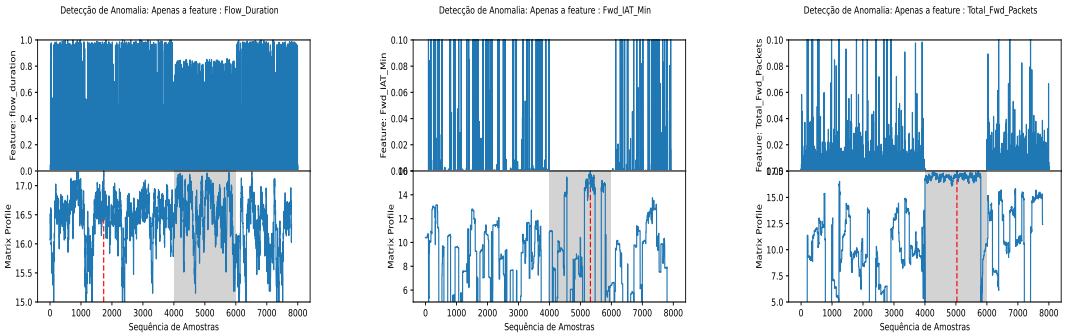
5.2. Visualização da Detecção Antecipada dos Ataques

Este estudo avaliou o uso do Matrix Profile na detecção de ataques cibernéticos de forma antecipada, utilizando séries temporais geradas por diferentes *features* e em diferentes cenários de ataques. As Figuras 2 e 3 ilustram o desempenho do Matrix Profile para a detecção de ataques DoS e DDoS, respectivamente. Cada subfigura apresenta a série temporal de uma *feature* específica na parte superior e o Matrix Profile correspondente na



(a) (b) (c)

Figura 2. Visualização da Detecção antecipada do ataque DoS.



(a) (b) (c)

Figura 3. Visualização da Detecção antecipada do ataque DDoS.

parte inferior. A área sombreada em cinza indica o período do ataque, enquanto a linha vermelha pontilhada identifica o ponto de detecção do ataque pelo sistema proposto.

Na Figura 2, observa-se que para o ataque DoS, a *feature flow_duration* (Figura 2a) permitiu uma detecção de anomalia muito próxima do início real do ataque. No entanto, a *feature fwd_iat_min* (Figura 2b) sinalizou uma anomalia bem antes do ataque começar, o que poderia levar a um número elevado de falsos positivos. Em contraste, a *feature total_fwd_packets* (Figura 2c) identificou uma anomalia após o início do ataque, resultando em potenciais falsos negativos. Para o ataque DDoS ilustrado na Figura 3, os resultados variaram significativamente. A *feature flow_duration*, que foi eficaz na detecção do ataque DoS, não foi capaz de detectar o ataque DDoS com a mesma antecedência. Isso indica que cada tipo de ataque pode ter uma ou mais *features* específicas que são mais adequadas para a detecção eficaz. Portanto, uma análise das *features* mais relevantes é essencial para otimizar o desempenho do sistema de detecção de anomalias

Na Figura 4, apresentamos a visualização da detecção de anomalias usando o Matrix Profile multidimensional. Foi utilizado as características *flow_duration*, *total_fwd_packets* e *fwd_iat_min* com os dados do ataque DoS. Os gráficos em amarelo representam o Matrix Profile, formado sequencialmente utilizando apenas uma característica, duas características e, por último, as três características em conjunto. Os triângulos indicam a região identificada como um ataque para cada um dos gráficos. No primeiro

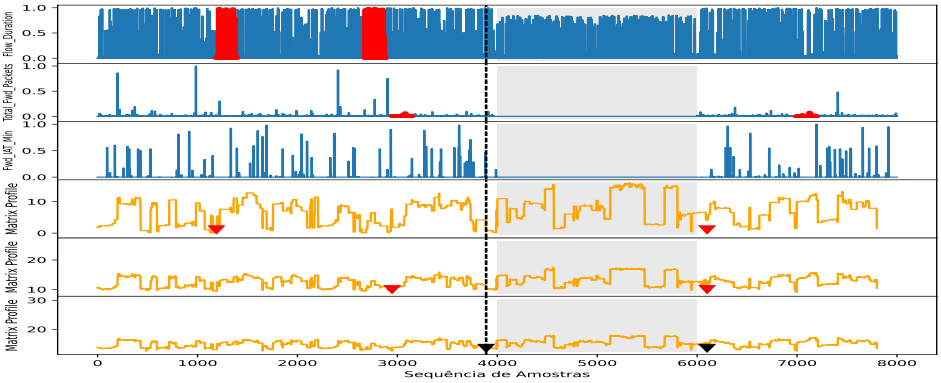


Figura 4. Matrix Profile Multidimensional: utilizando 3 *features*.

gráfico do Matrix Profile, essa região está distante da região em que os ataques realmente ocorreram (sombreada em cinza). À medida que adicionamos mais características, o Matrix Profile multidimensional melhora a identificação dos ataques, tornando-se mais preciso. Assim, o Matrix Profile multidimensional pode ser utilizado para melhorar a identificação dos ataques.

5.3. Análise das Características

A eficácia da detecção de ataques através do Matrix Profile depende significativamente da seleção e do comportamento das *features* de séries temporais utilizadas. As Tabelas 2 e 3 apresentam o ranking das *features* que tiveram melhor resultado na detecção de cada ataque. A partir dos resultados obtidos e apresentados nas Tabelas 2 e 3, é possível realizar uma análise das *features* que mais contribuem para a detecção eficiente de diferentes tipos de ataques, como DoS, DDoS e BoT, assim como Brute, FTP e Portscan.

Tabela 2. As cinco (5) melhores *features* para os ataques: DoS, DDoS, and BoT.

Rank	DoS	DDoS	BoT
1°	Flow_Duration	Bwd_IAT_Total	Bwd_IAT_Min
2°	Fwd_IAT_Total	Fwd_IAT_Mean	Active_Mean
3°	Fwd_Packet_Length_Mean	Active_Mean	Packet_Length_Variance
4°	Avg_Fwd_Segment_Size	Active_Min	Bwd_IAT_Total
5°	Fwd_Header_Length	Active_Max	Active_Mean

Tabela 3. As cinco (5) melhores *features* para os ataques: Brute, FTP, and Portscan.

Rank	Brute	FTP	Portscan
1°	Flow_IAT_Std	Total_Length_of_Fwd_Pkt	Flow_Duration
2°	Init_Win_bytes_backward	Subflow_Fwd_Bytes	Total_Fwd_Pkt
3°	Packet_Length_Variance	Flow_IAT_Max	Subflow_Fwd_Pkts
4°	Bwd_Packets/s	Average_Packet_Size	Avg_Fwd_Segment_Size
5°	Fwd_IAT_Max	Fwd_IAT_Max	Fwd_Pkt_Length_Mean

Para ataques DoS, a *feature Flow_Duration* mostrou-se a mais relevante, indicando que a duração do fluxo é um indicador crítico deste tipo de ataque. Isso é corroborado pelos resultados visualizados na Figura 2, onde *Flow_Duration* permitiu uma detecção precisa e próxima ao evento real. Já para ataques DDoS, *Bwd_IAT_Total* foi a *feature* de maior destaque, sugerindo que o tempo total entre pacotes enviados no sentido inverso possui um papel significativo na identificação deste tipo de ataque.

No contexto de ataques BoT, *Bwd_IAT_Min* foi identificada como a mais relevante. Isto implica que o intervalo mínimo entre pacotes é uma métrica importante para capturar a natureza deste ataque. A *feature Flow_IAT_Std*, que mede a variação no tempo entre fluxos, foi a principal *feature* para ataques de Brute Force, enquanto *Total_Length_of_Fwd_Packts* foi mais relevante para ataques via FTP. Em ataques de Portscan, *Flow_Duration* e *Total_Fwd_Packets* foram identificadas como as mais relevantes. indicando que diferentes tipos de ataques exigem estratégias distintas de monitoramento de *feature*.

6. Resultados

6.1. Qual o desempenho do Matrix Profile com apenas uma *feature*?

A eficácia do sistema de detecção de anomalias proposto foi avaliada utilizando o Matrix Profile como ferramenta de análise para diferentes tipos de ataques à rede. As métricas de desempenho acurácia, precisão, taxa de verdadeiros positivos (*True Positive Rate* - TPR), taxa de falsos alarmes (*False Alarm Rate* - FAR) e F1 Score, foram coletadas e são apresentadas na Tabela 3, refletindo o desempenho do sistema ao utilizar apenas a melhor *feature* identificada para cada tipo de ataque.

Os resultados indicam acurácia e precisão relevantes para vários tipos de ataques, particularmente DDoS e FTP, onde o sistema alcançou um F1 Score de 99,28% e 99,97%, respectivamente. O TPR para ataques Brute foi também significativo, indicando que o sistema foi capaz de detectar todos os ataques deste tipo. A taxa de falsos alarmes manteve-se em 0% para a maioria dos ataques, com exceção do DDoS, onde atingiu 1,43%, indicando um baixo número de falsos positivos.

A análise de desempenho utilizando as cinco melhores *features* para cada tipo de ataque, apresentada na Tabela 5, revela que o desempenho tende a diminuir à medida que *features* de menor ranking são utilizadas para gerar o Matrix Profile. No entanto, o F1 Score permanece alto para as principais *features*, indicando que uma seleção cuidadosa de *features* relevantes pode manter a eficácia do sistema.

Tabela 4. Métricas de avaliação por tipo de ataque com apenas a melhor *feature*.

Ataque	Acurácia (%)	Precisão (%)	TPR (%)	FAR (%)	F1 Score (%)
DoS	99.83	100.00	99.30	0.00	99.65
DDoS	100.00	98.57	100.00	1.43	99.28
BoT	99.94	100.00	99.75	0.00	99.87
Brute	98.63	94.79	100.00	5.21	97.32
FTP	99.99	100.00	99.95	0.00	99.97
PortScan	97.41	100.00	89.65	0.00	94.54

Tabela 5. F1 Score (%) por tipo de ataque, utilizando apenas uma das 5 melhores *features*.

Rank	DoS	DDoS	BoT	Brute	FTP	PortScan
1°	99.65	99.28	99.87	97.32	99.97	94.54
2°	99.65	98.57	99.70	96.34	99.97	86.26
3°	99.30	95.24	89.29	90.26	99.95	86.26
4°	99.30	95.15	82.63	82.90	99.95	85.93
5°	98.94	95.12	81.80	80.38	99.90	78.46

6.2. Qual o desempenho do Matrix comparado com outras técnicas?

A Tabela 6 compara o desempenho do Matrix Profile utilizando as melhores *features* individuais (MP.Rank 1) e combinadas no MP multidimensional (MP.multi) com as três (3f), cinco (5f) ou dez (10f) melhores *features*. Observa-se na Tabela 6 que o uso de um perfil multidimensional melhora os resultados, destacando-se o MP multidimensional com cinco *features* (MP.multi 5f) para a detecção de ataques DDoS e PortScan. Isso reforça a vantagem de utilizar múltiplas *features* em conjunto para melhorar a capacidade de detecção do sistema.

Em contraste, técnicas tradicionais como CUSUM, EWMA e ARIMA apresentaram desempenho inferior quando comparadas com o uso do Matrix Profile. Especificamente, a técnica CUSUM mostrou-se menos precisa, com uma redução no F1 Score em todos os tipos de ataques, o que pode ser atribuído à sua sensibilidade a variações mais sutis nas séries temporais. Estes resultados demonstram a superioridade do Matrix Profile sobre outras técnicas na detecção de ataques às redes, destacando seu potencial como uma ferramenta confiável e robusta na identificação precoce de ameaças cibernéticas em diversos cenários.

Tabela 6. F1 Score (%) por Tipo de Ataque com o Matrix Profile em diferentes configurações e comparação com outras técnicas.

Método	DoS	DDoS	BoT	Brute	FTP	PortScan
MP. (Rank 1)	99.65	99.28	99.87	97.32	99.97	94.54
MP.multi (**3f**)	99.77	99.38	99.93	98.61	98.50	95.01
MP.multi (**5f**)	99.87	99.35	99.80	99.33	98.91	96.61
MP.multi (**10f**)	99.23	99.78	99.73	97.62	99.45	95.19
CUSUM	98.81	95.90	95.23	76.89	76.91	70.47
EWMA	95.24	86.73	98.94	70.34	68.73	82.29
ARIMA	88.33	94.71	91.57	51.19	65.64	78.01

7. Conclusão e Trabalhos Futuros

Neste trabalho é proposto o Matrix Profile para realizar a detecção antecipada e de forma *on-line* de ataques à rede. Os resultados obtidos demonstram a eficácia do MP, tanto na análise com apenas uma *feature* quanto na configuração multidimensional. A capacidade do MP de detectar anomalias em tempo real e com alta precisão, mesmo com uma única

feature, representa um avanço significativo em relação aos sistemas existentes. A análise revelou que, apesar de um desempenho ligeiramente reduzido ao incluir *features* de menor ranking, o sistema mantém sua eficácia, ressaltando a importância de uma seleção cuidadosa de *features*. Além disso, a comparação com outras técnicas evidenciou a superioridade do MP na identificação antecipada de ameaças cibernéticas, tornando-o uma ferramenta valiosa para reforçar a segurança da rede.

Para trabalhos futuros, sugere-se a integração do sistema proposto com outras soluções de segurança cibernética, visando criar um ecossistema de defesa mais robusto e abrangente. Além disso, é importante testar e validar o sistema em um ambiente de produção real para avaliar sua eficiência e escalabilidade em cenários dinâmicos e diversificados. Investigações adicionais podem explorar a adaptação do MP para reconhecer padrões emergentes de ataques, bem como sua combinação com técnicas avançadas de aprendizado de máquina para melhorar a precisão da detecção de ameaças.

Agradecimentos

Este trabalho foi parcialmente financiado pelo Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq) e pela Fundação de Amparo à Pesquisa do Estado de São Paulo (FAPESP), projeto 2023/00673-7, projeto 2020/04031-1 e projeto 2018/23097-3.

Referências

Abreu, D. and Abelém, A. (2022). Ominacs: Online ml-based iot network attack detection and classification system. In *2022 IEEE Latin-American Conference on Communications (LATINCOM)*, pages 1–6. IEEE.

Abreu, D. M., Carvalho, I. F., Abelém, A. J. G., Menasché, D. S., Leão, R. M. M., and Silva, E. S. (2020). Seleção de características por clusterização para melhorar a detecção de ataques de rede. In *Anais do XXXVIII Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos*, pages 295–308. SBC.

Ahmad, R., Alsmadi, I., Alhamdani, W., and Tawalbeh, L. (2023). Zero-day attack detection: a systematic literature review. *Artificial Intelligence Review*, pages 1–79.

Alotaibi, F. and Lisitsa, A. (2021). Matrix profile for ddos attacks detection. In *2021 16th Conference on Computer Science and Intelligence Systems (FedCSIS)*, pages 357–361. IEEE.

Alzahrani, M. A., Alzahrani, A. M., and Siddiqui, M. S. (2022). Detecting ddos attacks in iot-based networks using matrix profile. *Applied Sciences*, 12(16):8294.

Anton, S. D. D., Hafner, A., and Schotten, H. D. (2019). Devil in the detail: Attack scenarios in industrial applications. In *2019 IEEE Security and Privacy Workshops (SPW)*, pages 169–174. IEEE.

De Neira, A. B., Borges, L. F., de Araújo, A. M., and Nogueira, M. (2023). Engenharia de sinais precoces de alerta para a predição de ataques ddos. In *Anais do XXVIII Workshop de Gerência e Operação de Redes e Serviços*, pages 139–152. SBC.

Elbez, G., Nahrstedt, K., and Hagenmeyer, V. (2023). Early attack detection for securing goose network traffic. *IEEE Transactions on Smart Grid*.

Gharghabi, S., Ding, Y., Yeh, C.-C. M., Kamgar, K., Ulanova, L., and Keogh, E. (2017). Matrix profile viii: Domain agnostic online semantic segmentation at superhuman performance levels. In *2017 IEEE International Conference on Data Mining (ICDM)*, pages 117–126.

Gomes, H. M., Read, J., Bifet, A., Barddal, J. P., and Gama, J. (2019). Machine learning for streaming data: state of the art, challenges, and opportunities. *ACM SIGKDD Explorations Newsletter*, 21(2):6–22.

He, K., Kim, D. D., and Asghar, M. R. (2023). Adversarial machine learning for network intrusion detection systems: a comprehensive survey. *IEEE Communications Surveys & Tutorials*.

Jacobs, A. S., Beltiukov, R., Willinger, W., Ferreira, R. A., Gupta, A., and Granville, L. Z. (2022). Ai/ml for network security: The emperor has no clothes. In *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security*, pages 1537–1551.

Kim, S., Park, K.-J., and Lu, C. (2022). A survey on network security for cyber–physical systems: From threats to resilient design. *IEEE Communications Surveys & Tutorials*, 24(3):1534–1573.

Lu, W. and Tong, H. (2009). Detecting network anomalies using cusum and em clustering. In *Advances in Computation and Intelligence: 4th International Symposium, ISICA 2009 Huangshi, China, Ocotober 23-25, 2009 Proceedings 4*, pages 297–308. Springer.

Nascimento, A., Abreu, D., Riker, A., and Abelém, A. (2023). Aid-sdn: Advanced intelligent defense for sdn using p4 and machine learning. In *2023 IEEE Latin-American Conference on Communications (LATINCOM)*, pages 1–6. IEEE.

Sharafaldin, I., Lashkari, A. H., and Ghorbani, A. A. (2018). Toward generating a new intrusion detection dataset and intrusion traffic characterization. *ICISSp*, 1:108–116.

Yaacob, A. H., Tan, I. K., Chien, S. F., and Tan, H. K. (2010). Arima based network anomaly detection. In *2010 Second International Conference on Communication Software and Networks*, pages 205–209. IEEE.

Yeh, C.-C. M., Kavantzas, N., and Keogh, E. (2017). Matrix profile vi: Meaningful multidimensional motif discovery. In *2017 IEEE international conference on data mining (ICDM)*, pages 565–574. IEEE.

Yeh, C.-C. M., Zhu, Y., Ulanova, L., Begum, N., Ding, Y., Dau, H. A., Silva, D. F., Mueen, A., and Keogh, E. (2016). Matrix profile i: all pairs similarity joins for time series: a unifying view that includes motifs, discords and shapelets. In *2016 IEEE 16th international conference on data mining (ICDM)*, pages 1317–1322. Ieee.

Zhou, Z.-G. and Tang, P. (2016). Improving time series anomaly detection based on exponentially weighted moving average (ewma) of season-trend model residuals. In *2016 IEEE International Geoscience and Remote Sensing Symposium (IGARSS)*, pages 3414–3417. IEEE.