Uma Arquitetura de IDS para IoT Baseada em Aprendizado Federado com Seleção de Atributos via PFI

Daniel W. S. Alves[1], **Joahannes Costa**[2], **Denis Lima do Rosário**[3], **Eduardo Cerqueira**[3], **Rodrigo Righi**[4], **Roger Immich**[1],

[1] Universidade Federal do Rio Grande do Norte (UFRN)
[2]Universidade Federal de Sao Paulo (UNIFESP)
[3]Universidade Federal do Pará (UFPA)
[4]Universidade do Vale do Rio dos Sinos (Unisinos)

dan.alves.w@gmail.com, joahannes.costa@unifesp.br, denis@ufpa.br, cerqueira@ufpa.br, rrrighi@unisinos.br, roger@imd.ufrn.br

Abstract. *Intrusion Detection Systems (IDS) in Internet of Things (IoT) environments face significant challenges due to device resource constraints, data privacy requirements, and communication overhead in distributed settings. In this context, Federated Learning has emerged as a promising paradigm, enabling collaborative model training without sharing raw data. This work presents a federated IDS architecture that integrates Permutation Feature Importance (PFI) into the training process to enable a Top-K feature selection mechanism, aiming to reduce the volume of transmitted updates. Although the complete federated architecture is defined, this study focuses on a controlled local evaluation of feature relevance, isolating the impact of PFI on attribute importance and dimensionality reduction. Experimental results using the UNSW-NB15 dataset demonstrate that significant reductions in feature dimensionality can be achieved while maintaining competitive accuracy and F1-score. Additionally, the analysis reveals a saturation point in feature contribution, indicating structural redundancy among attributes. These findings provide empirical support for the use of PFI-based feature selection as a key component in communication-efficient federated IDS, offering a solid foundation for future end-to-end federated implementations in resource-constrained IoT environments.*

Resumo. *Sistemas de Detecção de Intrusões (IDS) em ambientes de Internet das Coisas (IoT) enfrentam desafios significativos devido às restrições de recursos dos dispositivos, aos requisitos de privacidade dos dados e à sobrecarga de comunicação em cenários distribuídos. Nesse contexto, a Aprendizagem Federada (FL) tem emergido como um paradigma promissor, permitindo o treinamento colaborativo de modelos sem o compartilhamento de dados brutos. Este trabalho apresenta uma arquitetura de IDS federado que integra a técnica de Permutation Feature Importance (PFI) ao processo de treinamento, viabilizando um mecanismo de seleção de atributos Top-K com o objetivo de reduzir o volume de atualizações transmitidas. Embora a arquitetura federada completa seja definida, este estudo concentra-se em uma avaliação local controlada da relevância dos atributos, isolando o impacto do PFI na importância dos atributos e na redução de dimensionalidade, sem a implementação completa do processo federado. Resultados experimentais utilizando o conjunto de dados UNSW-NB15 demonstram que reduções significativas na dimensionalidade dos*

atributos podem ser alcançadas mantendo níveis competitivos de acurácia e F1-score. Além disso, a análise revela a existência de um ponto de saturação na contribuição dos atributos, indicando redundâncias estruturais entre os atributos. Esses resultados fornecem evidências empíricas de que a seleção de atributos baseada em PFI é um componente-chave para a eficiência de comunicação em IDS federados, estabelecendo uma base sólida para futuras implementações federadas completas em ambientes de IoT com restrições de recursos.

1. Introdução

A expansão da Internet das Coisas (IoT) tem transformado a forma como dispositivos, sistemas e usuários interagem em ambientes digitais [Barbosa et al. 2022, Greengard 2021]. Embora esse avanço traga benefícios significativos em termos de eficiência e inovação, ele também amplia a superfície de ataque das redes e intensifica os desafios relacionados à segurança cibernética [Santo et al. 2023, Fiorenza et al. 2021]. Esse cenário torna-se ainda mais crítico considerando que muitos dispositivos IoT operam com recursos limitados de processamento, memória e energia, o que dificulta a adoção de mecanismos de segurança robustos e os torna alvos potenciais de ataques [Pisani et al. 2020, Wei et al. 2016].

Nesse contexto, os Sistemas de Detecção de Intrusão (IDS) desempenham papel fundamental na identificação de atividades maliciosas por meio da análise do tráfego de rede e da detecção de comportamentos anômalos. Entretanto, arquiteturas tradicionais de IDS são majoritariamente centralizadas e dependem da transmissão contínua de dados para servidores de processamento. Em ambientes IoT, essa abordagem pode gerar elevado consumo de largura de banda, aumento do gasto energético e problemas de escalabilidade, comprometendo a eficiência operacional dos dispositivos envolvidos [Silva et al. 2023, Bittencourt et al. 2018].

Técnicas de Aprendizado de Máquina (ML) têm sido amplamente exploradas para aprimorar a detecção de intrusões, permitindo que modelos aprendam padrões complexos diretamente a partir dos dados de rede [Lieira et al. 2021, Liu and Lang 2019]. Contudo, abordagens tradicionais de ML dependem da centralização de grandes volumes de dados, o que levanta preocupações relacionadas à privacidade e ao custo de comunicação em ambientes distribuídos [Thakkar and Lohiya 2021, Chang et al. 2022]. Como alternativa, o Aprendizado Federado possibilita o treinamento colaborativo de modelos sem a necessidade de centralizar os dados originais, permitindo que cada participante realize o aprendizado localmente e compartilhe apenas atualizações de modelo [Li et al. 2020].

Apesar de seu potencial, a aplicação de ML federado em sistemas de detecção de intrusão para IoT ainda enfrenta desafios relevantes. Em particular, o volume de parâmetros transmitidos em cada rodada de treinamento pode gerar sobrecarga de comunicação e aumentar o consumo de recursos em dispositivos com capacidade limitada [Roy et al. 2023]. Além disso, estudos recentes indicam que grande parte das soluções existentes concentra-se na otimização de agregação de modelos ou na redução da latência de treinamento, dedicando pouca atenção à seleção de atributos relevantes e à interpretabilidade dos modelos.

Apesar dos avanços recentes, um aspecto ainda pouco explorado é o impacto da seleção de atributos no custo de comunicação. Em particular, técnicas de explicabili-

dade, como Permutation Feature Importance (PFI), são predominantemente utilizadas para interpretação de modelos, sendo raramente exploradas como mecanismo ativo de otimização do processo federado, especialmente no contexto da redução do volume de dados transmitidos entre clientes e servidor.

Diante dessa lacuna, este trabalho propõe uma arquitetura completa de IDS para ambientes IoT baseada em aprendizado federado, na qual um mecanismo de seleção de atributos guiado por PFI é integrado ao ciclo de treinamento. A proposta utiliza uma estratégia Top-K para selecionar e transmitir apenas os atributos mais relevantes durante as atualizações locais, com o objetivo de reduzir o custo de comunicação sem comprometer o desempenho do modelo.

Embora a arquitetura federada seja formalmente definida, esta etapa do trabalho concentra-se na análise controlada da relevância dos atributos em um cenário local, com o objetivo de isolar e compreender o comportamento do mecanismo de seleção baseado em PFI. Para isso, são conduzidos experimentos utilizando o conjunto de dados UNSW-NB15, avaliando diferentes classificadores supervisionados e investigando o impacto da redução de dimensionalidade no desempenho dos modelos.

Os resultados demonstram que a maior parte da capacidade preditiva está concentrada em um subconjunto reduzido de atributos, evidenciando a existência de redundância estrutural nos dados. Além disso, observa-se um ponto de saturação na contribuição dos atributos, a partir do qual a inclusão de novos atributos gera ganhos marginais. Esses resultados reforçam o potencial do uso de PFI como mecanismo para seleção eficiente de atributos, fornecendo subsídios para a redução do custo de comunicação em ambientes federados.

Assim, este trabalho contribui com: (i) a proposição de uma arquitetura de IDS federado com suporte à seleção de atributos baseada em PFI; (ii) uma análise empírica detalhada da relevância dos atributos em diferentes paradigmas de aprendizado; e (iii) evidências da viabilidade de estratégias Top-K para redução de dimensionalidade, estabelecendo uma base sólida para futuras implementações completas em cenários federados reais.

2. Trabalhos Relacionados

Diversos trabalhos investigam o uso de aprendizado federado em sistemas de detecção de intrusão para IoT, especialmente em cenários com dados não IID. Estudos recentes no contexto de IoMT, que consideram a heterogeneidade entre diferentes silos, demonstram que a distribuição não IID impacta negativamente o desempenho de modelos baseados em redes neurais profundas [Ali Kazmi et al. 2024]. Os resultados evidenciam degradações significativas em métricas como acurácia, precisão, recall e F1-score, além do aumento de falsos positivos e negativos, atribuídos ao desbalanceamento dos atributos relevantes entre os silos. Contudo, tais abordagens não exploram estratégias de redução de comunicação nem consideram a seleção dinâmica de atributos no processo de treinamento federado.

Uma abordagem relevante na literatura propõe o framework FedIoT, que integra aprendizado federado, explicabilidade e blockchain [El Houda et al. 2023]. Essa solução incorpora mecanismos de reputação para mitigar ataques adversariais e utiliza técnicas como SHAP e LIME para interpretar as decisões do modelo, alcançando elevados níveis

de acurácia e F1-score no conjunto UNSW-NB15. No entanto, a abordagem mantém a transmissão completa dos parâmetros durante o treinamento, sem considerar o impacto na largura de banda, e utiliza a explicabilidade apenas para interpretação, sem explorá-la como mecanismo para seleção de atributos ou redução do custo de comunicação.

No contexto de seleção de atributos, a redução de dimensionalidade pode ser alcançada sem perdas significativas de desempenho em sistemas de detecção de intrusão [Pham et al. 2023]. Os autores aplicam técnicas de ranqueamento e obtêm elevados níveis de acurácia com um número reduzido de atributos. Entretanto, a abordagem permanece centralizada, não considerando cenários de aprendizado federado. De forma semelhante, o método OFSM, foi proposta baseado em importância por permutação, para seleção de atributos em dispositivos IoT com recursos limitados [Kil et al. 2024]. Embora os resultados indiquem ganhos em desempenho e economia de memória, o estudo não considera ambientes federados nem avalia o impacto na comunicação entre dispositivos.

Por fim, abordagens como [Pei et al. 2023] e [Peng et al. 2022] exploram técnicas para lidar com limitações do aprendizado federado, incluindo transferência de conhecimento e mitigação de dados não IID. No entanto, essas soluções continuam baseadas na transmissão integral dos parâmetros do modelo e não incorporam mecanismos de seleção de atributos baseados em importância. O estudo de [Thevarajan et al. 2025] propõe um framework de aprendizado federado para detecção de anomalias em ambientes IoT, combinando 1D-CNN e autoencoders. A abordagem apresenta bons resultados em cenários não-IID e reduz o custo computacional por meio de quantização do modelo. No entanto, não explora estratégias de redução de comunicação baseadas na seleção de atributos, como o uso de PFI, aspecto abordado neste trabalho.

A Tabela 1 sumariza os trabalhos relacionados. Observa-se que, embora existam avanços relevantes em aprendizado federado e seleção de atributos, ainda há uma lacuna na integração dessas abordagens com foco na redução de comunicação. Este trabalho busca preencher essa lacuna ao incorporar o PFI ao ciclo federado, utilizando um mecanismo Top-K para selecionar atributos relevantes e reduzir o volume de dados transmitidos.

3. Arquitetura para IDS com aprendizado federado utilizando PFI

A arquitetura proposta tem como objetivo viabilizar a detecção de intrusões em ambientes IoT por meio de aprendizado federado com redução de comunicação baseada em PFI. O sistema é composto por um conjunto de componentes interdependentes que atuam ao longo do ciclo de aprendizado, desde o pré-processamento do tráfego até a agregação global dos modelos.

O desenho da arquitetura considera três aspectos centrais: a preservação da privacidade, mantendo os dados brutos na borda da rede; a redução da sobrecarga de comunicação em cenários de aprendizado federado; e a possibilidade de interpretação das decisões do modelo a partir da relevância dos atributos. Para atender a esses requisitos, a proposta integra o aprendizado federado a um mecanismo de seleção orientado por PFI, no qual cada *gateway* calcula a importância dos atributos após o treinamento local e transmite apenas uma atualização Top-K associada aos atributos mais influentes.

A Figura 1 apresenta a organização geral da arquitetura, estruturada em três ca-

Tabela 1. Comparação dos trabalhos relacionados

Ref.	**Contexto/Foco**	**Contribuição Principal**	**Limitação / Relação com este Trabalho**
[Ali Kazmi et al. 2024]	IDS federado em IoMT com dados não-IID	Avalia impacto da heterogeneidade de dados no desempenho de modelos FL	Não considera seleção de atributos nem estratégias de redução de comunicação
[El Houda et al. 2023]	Framework FedIoT com FL, blockchain e XAI	Integra explicabilidade (SHAP/LIME) e mecanismos de reputação	Mantém transmissão completa dos parâmetros e não usa explicabilidade para seleção de atributos
[Pham et al. 2023]	IDS baseado em ML com seleção de atributos	Demonstra redução de dimensionalidade sem perda significativa de desempenho	Abordagem centralizada, sem aprendizado federado
[Kil et al. 2024]	Seleção de atributos em IoT via importância por permutação (OFSM)	Melhora desempenho e uso de memória em dispositivos com recursos limitados	Não considera cenários federados nem impacto na comunicação
[Pei et al. 2023]	FL com transferência de conhecimento para detecção de malware	Propõe melhoria em cenários com dados não-IID	Não incorpora seleção de atributos e mantém transmissão completa de parâmetros
[Peng et al. 2022]	FL com troca de mapas de características para dados não-IID	Mitiga efeitos de heterogeneidade de dados	Não utiliza seleção de atributos baseada em importância
[Thevarajan et al. 2025]	FL para detecção de anomalias com 1D-CNN e autoencoders	Reduz custo computacional via quantização e lida com dados não-IID	Não explora seleção de atributos para redução de comunicação
Nossa proposta	IDS federado com seleção de atributos baseada em PFI	Integra PFI ao treinamento com estratégia Top-K para reduzir comunicação	Avaliação em ambiente local, sem implementação federada completa

madas. A primeira camada é composta pelos dispositivos IoT, responsáveis pela geração contínua de tráfego a partir de sensores, câmeras e demais equipamentos conectados. Esses dados são encaminhados para a camada de borda, onde ocorre o processamento local.

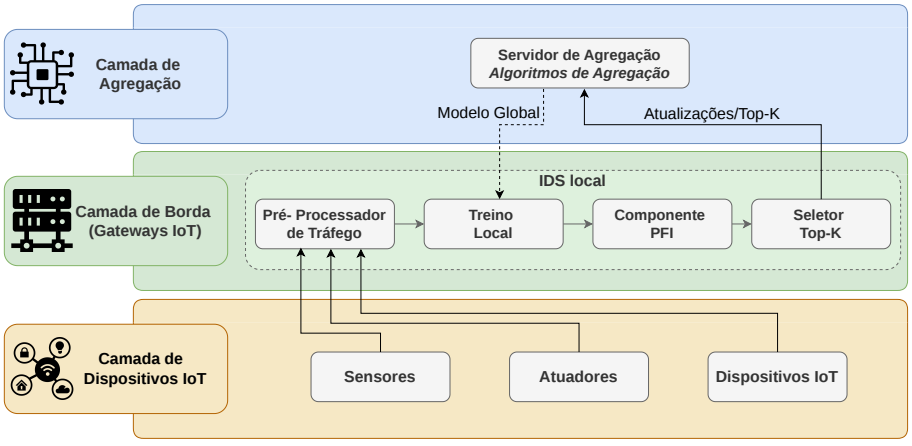

Figura 1. Arquitetura proposta para IDS em IoT com aprendizado federado e seleção de atributos baseada em PFI

Na camada intermediária, os *gateways* executam o pré-processamento do tráfego, incluindo normalização e extração de atributos relevantes para o treinamento. Em seguida, o IDS local realiza a detecção de intrusões e atualizações do modelo com base nos

dados recentes. Após essa etapa, o componente de PFI estima a relevância de cada atributo a partir da variação no desempenho do modelo, produzindo um ranqueamento dos atributos. Com base nesse ranqueamento, o seletor *Top-K* mantém apenas os atributos mais relevantes, gerando uma atualização compacta a ser enviada ao servidor.

Na camada superior, o servidor de agregação coordena o processo federado, recebendo as atualizações dos nós de borda, aplicando a política de agregação e redistribuindo o modelo global atualizado aos participantes. Esse processo ocorre de forma iterativa, permitindo a adaptação contínua do sistema ao longo do tempo.

Essa organização permite reduzir o volume de comunicação, preservar a privacidade dos dados e manter a capacidade de detecção do modelo, mesmo em ambientes com restrições de recursos. Além disso, a utilização do PFI contribui para a interpretabilidade das decisões do sistema, ao evidenciar quais atributos influenciam as atualizações do modelo.

O fluxo geral de comunicação e treinamento é representado na Figura 2. Nela são ilustrados, de forma sequencial, as etapas do ciclo federado de detecção. O processo inicia-se no passo (1), quando o servidor de agregação distribui o modelo global inicial aos gateways de borda. Em (2), o tráfego proveniente dos dispositivos IoT é capturado localmente e encaminhado ao pré-processador, responsável por normalizar os dados e extrair os atributos relevantes para o treinamento.

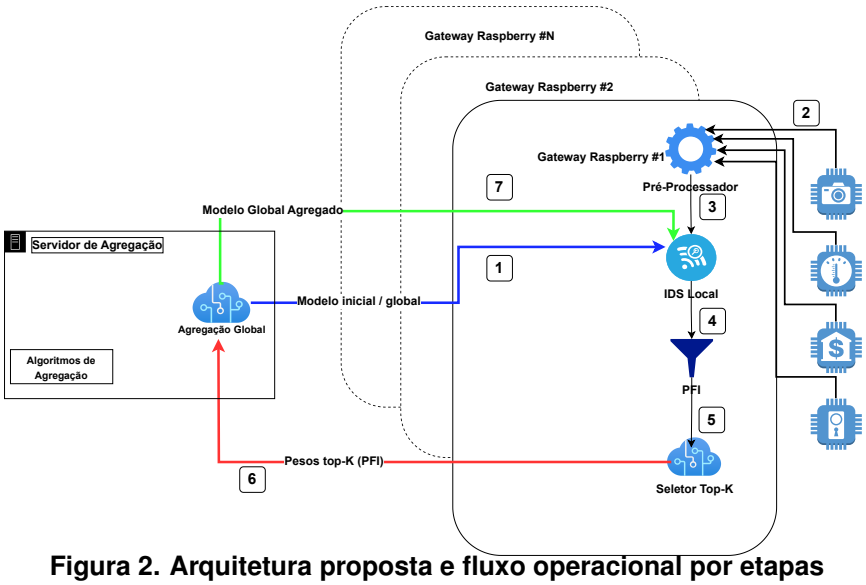

Figura 2. Arquitetura proposta e fluxo operacional por etapas

No passo (3), o IDS local realiza inferência sobre os fluxos coletados e executa pequenas iterações de ajuste do modelo com base nos dados recentes. Em seguida, no passo (4), o componente PFI calcula a importância de cada atributo, gerando um ranqueamento que indica o grau de contribuição de cada variável para o desempenho do modelo.

Com base nesse ranqueamento, o seletor Top-K atua no passo (5), retendo apenas os parâmetros associados aos atributos mais relevantes e empacotando uma atualização compacta. Essa atualização é então enviada ao servidor, que, no passo (6), aplica o algoritmo de agregação configurado como FedAvg, para combinar as contribuições dos clientes. Por fim, no passo (7), o modelo global atualizado é redistribuído aos gateways,

reiniciando o ciclo de aprendizado colaborativo.

Esse fluxo contínuo assegura que o IDS federado opere de forma adaptativa, mantendo a coerência entre as instâncias locais, reduzindo o tráfego de comunicação e preservando a privacidade dos dados coletados na borda.

4. Resultados da Análise da Relevância dos Atributos

Esta seção analisa o comportamento dos classificadores supervisionados aplicados ao conjunto de dados UNSW-NB15, considerando o impacto de cada atributo no desempenho das predições. O propósito central é compreender de que forma os modelos respondem às variações nos parâmetros de tráfego de rede e identificar quais características exercem maior influência na detecção de atividades anômalas. Essa análise preliminar fornece subsídios para a etapa subsequente da pesquisa, na qual o mecanismo de seleção Top-K guiado por PFI será integrado ao processo de aprendizado federado.

O conjunto UNSW-NB15 foi escolhido por representar um cenário realista de tráfego de rede, com registros de comunicações normais e maliciosas oriundas de múltiplas categorias de ataque. As amostras foram divididas em conjuntos de treino e teste na proporção de setenta e trinta por cento, respectivamente, mantendo-se o equilíbrio relativo entre as classes. As etapas de pré-processamento incluíram a remoção de atributos irrelevantes, como identificadores e endereços IP, a codificação de atributos categóricas e a normalização dos valores numéricos, de modo a evitar distorções de escala entre os atributos de entrada. Esse procedimento garantiu uniformidade na preparação dos dados e permitiu a comparação direta entre os diferentes classificadores avaliados.

Os modelos foram executados com parâmetros padrão da biblioteca Scikit-learn, assegurando reprodutibilidade por meio de semente fixa de aleatoriedade. Após o treinamento, aplicou-se o cálculo de importância por permutação, configurado com dez repetições e pontuação baseada na variação do F1-score. Essa métrica foi adotada por refletir o equilíbrio entre precisão e sensibilidade, característica particularmente relevante em contextos de detecção de intrusão, nos quais há predominância de classes negativas. A partir dos resultados do PFI, cada atributo foi ranqueado conforme a queda média de desempenho observada quando o seu valor foi permutado no conjunto de validação.

Foram empregados quatro classificadores com naturezas distintas: Random Forest, SVM Linear, AdaBoost e Regressão Logística. Essa seleção contempla abordagens baseadas em ensembles, boosting e modelos lineares, permitindo observar o comportamento do PFI em diferentes paradigmas de aprendizado. Além dessas análises, realizou-se um experimento adicional com o modelo de Regressão Logística, no qual foram avaliados subconjuntos progressivos de atributos selecionados pelo PFI. Esse estudo complementar, representado por um gráfico em formato de radar, teve como finalidade investigar o efeito da redução de dimensionalidade sobre as métricas de desempenho e identificar o ponto de equilíbrio entre custo computacional e acurácia.

Os resultados apresentados nas subseções seguintes correspondem aos quinze atributos mais relevantes identificadas por cada classificador, seguidos pela análise do comportamento do modelo sob diferentes valores de k. A comparação desses perfis permite avaliar a consistência dos atributos mais influentes e fornece evidências sobre a viabilidade do uso do PFI como critério de seleção adaptativa de atributos em cenários federados.

Dessa forma, esta etapa representa o elo entre os experimentos locais e as estratégias de redução de comunicação e preservação de desempenho que serão exploradas nas próximas seções.

4.1. Análise comparativa dos classificadores

Os resultados obtidos com os diferentes classificadores supervisionados evidenciam padrões distintos quanto à distribuição da importância dos atributos e ao desempenho na detecção de intrusões no conjunto UNSW-NB15. A análise conjunta, ilustrada nas Figuras 3 a 6, permite identificar tendências comuns entre os modelos, bem como características específicas associadas a cada paradigma de aprendizado.

De modo geral, observa-se que todos os classificadores concentram maior relevância em um subconjunto reduzido de atributos, ainda que com diferentes níveis de dispersão. Esse comportamento reforça a hipótese de que a contribuição marginal dos atributos menos relevantes é limitada, sustentando a viabilidade da aplicação de estratégias de seleção Top-K guiadas por PFI.

A Random Forest, apresentada na Figura 3, exibiu uma distribuição mais equilibrada das importâncias, com múltiplos atributos contribuindo de forma significativa para o desempenho do modelo. Atributos como *ct_dst_src_ltm*, *service* e *sbytes* destacam-se entre as mais relevantes, indicando que o modelo explora tanto características de volume quanto padrões de tráfego. Essa distribuição mais homogênea sugere maior robustez e tolerância à redundância entre atributos.

Em contraste, o AdaBoost, ilustrado na Figura 4, exibiu forte concentração da importância em um único atributo, *sttl*, evidenciando um comportamento altamente seletivo. Embora essa característica possa favorecer a eficiência na redução de dimensionalidade, ela também indica maior sensibilidade a ruídos ou variações nesse atributo específico.

Por sua vez, os modelos lineares, como Regressão logística e SVM Linear, representados nas Figuras 5 e 6, respectivamente, apresentaram um perfil intermediário. Ambos distribuíram a importância entre múltiplos atributos, com maior ênfase nas primeiras posições. No caso da Regressão Logística Figura 5, atributos como *swin*, *dttl* e *dwin* destacaram-se, indicando uma combinação de características relacionadas a janelas de comunicação, duração e protocolos. O SVM Linear Figura 6, por sua vez, concentrou maior relevância em atributos como *proto*, *state* e *dttl*, mantendo uma distribuição mais concentrada nos primeiros atributos.

A Tabela 1 complementa essa análise ao apresentar as métricas de desempenho dos classificadores. A Random Forest obteve os melhores resultados globais, com aproximadamente 95% de acurácia e 96% de F1-score, seguida pelo AdaBoost, que também apresentou desempenho competitivo. Os modelos SVM Linear e Regressão Logística mantiveram resultados consistentes, próximos a 90% de acurácia.

De forma geral, os resultados indicam que, apesar das diferenças nos mecanismos de aprendizado, os modelos convergem para um padrão comum: a maior parte da capacidade preditiva está concentrada em um conjunto reduzido de atributos.

De modo comparativo, observa-se que os quatro modelos apresentam padrões distintos de dependência entre atributos e desempenho, refletindo diferentes mecanismos de aprendizado e sensibilidade ao conjunto de dados. O AdaBoost mostrou o comportamento

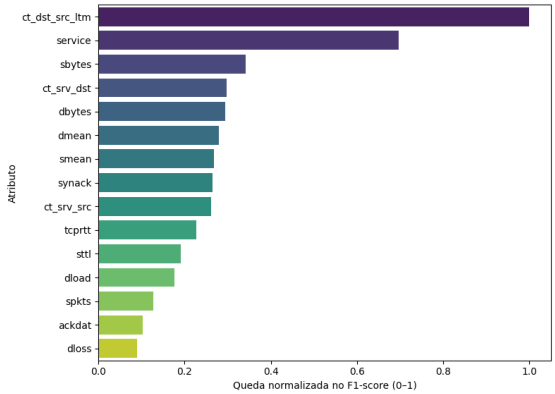

Figura 3. Random Forest

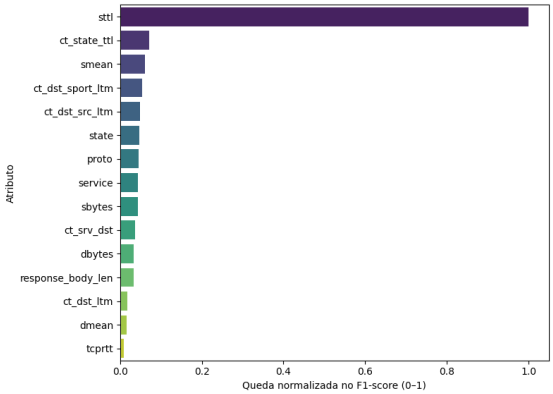

Figura 4. AdaBoost

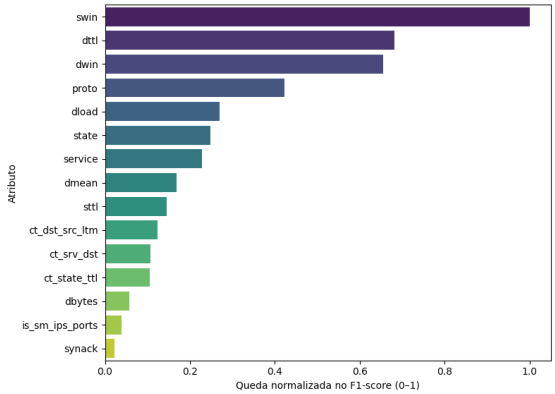

Figura 5. Logistic Regression

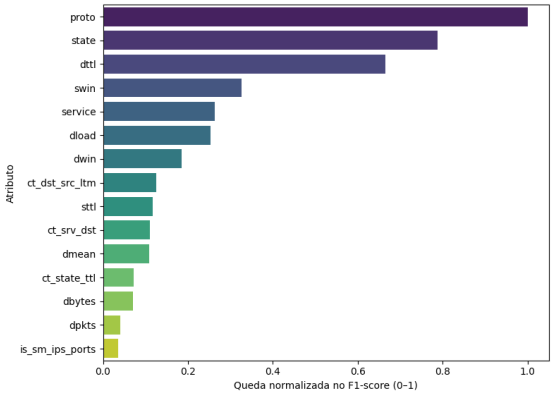

Figura 6. SVM Linear

Tabela 2. Métricas de desempenho por classificador

Modelo	Accuracy	F1-Score	Precision	Recall
Random Forest	0.9514	0.9619	0.9601	0.9637
SVM Linear	0.9030	0.9277	0.8856	0.9740
AdaBoost	0.9214	0.9385	0.9389	0.9380
Logistic Regression	0.9035	0.9276	0.8910	0.9674

mais seletivo, concentrando quase toda a relevância em um único atributo, *sttl*, o que evidencia alta capacidade de discriminação, porém menor robustez diante de ruídos ou perda de informação. A Random Forest, em contrapartida, exibiu uma distribuição mais estável e diversificada, indicando que o modelo combina múltiplos atributos de tráfego e volume para compor suas decisões, característica típica de ensembles com maior tolerância a variações. O SVM Linear e a Regressão Logística apresentaram perfis intermediários: ambos distribuem importância entre vários descritores, mas com ênfase moderada nas primeiras posições, sugerindo um balanceamento entre especialização e generalização. Em conjunto, esses resultados indicam que, apesar das diferenças internas, todos os modelos convergem para um ponto comum: a redução de dimensionalidade via PFI é viável, pois a contribuição marginal dos atributos de menor relevância é reduzida. Assim, a adoção de um mecanismo de seleção Top-K torna-se justificável não apenas como estratégia de eficiência de comunicação no aprendizado federado, mas também como meio de preservar a interpretabilidade e a consistência do sistema de detecção.

4.2. Experimento com Subconjuntos Top-K guiados por PFI

Este experimento investiga o impacto da redução de dimensionalidade por meio do PFI. Parte-se do ranqueamento obtido no *baseline* e avaliam-se as métricas de desempenho conforme $k \in \{5, 10, 20, 30, 50\}$. O procedimento consiste na seleção progressiva dos atributos mais relevantes, de acordo com o ranqueamento gerado, seguido do retreinamento do modelo. Neste estudo, utiliza-se o modelo de Regressão Logística.

Os resultados representados na Figura 7 mostram a variação das principais métricas de desempenho conforme o número de atributos selecionados pelo PFI. Observa-se que, à medida que o valor de k aumenta, há uma tendência de estabilização das métricas, indicando um ponto de saturação em torno de $k = 20$ a $k = 30$, no qual o acréscimo de novos atributos passa a gerar ganhos marginais. Para valores muito baixos de k, como $k = 5$, as métricas sofrem queda acentuada, evidenciando a perda de informação relevante. Já em configurações mais amplas ($k = 50$), o desempenho tende a se manter estável, o que sugere que a inclusão de atributos adicionais pouco contribui para a melhoria do modelo, mas aumenta o custo de comunicação. De forma geral, o comportamento observado reforça a hipótese de que a filtragem baseada em PFI pode reduzir a dimensionalidade mantendo níveis adequados de *accuracy*, *precision* e *recall*, equilibrando eficiência e desempenho em cenários federados.

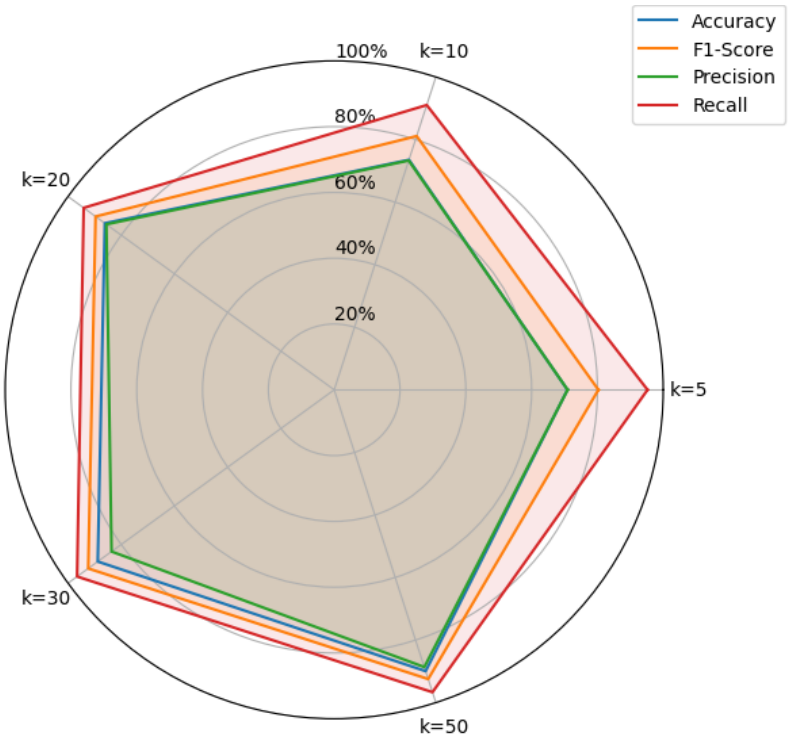

Figura 7. Variação de métricas (%) por *Top-*k de atributos (UNSW-NB15)

4.3. Discussão sobre a Seleção de Atributos em Ambientes IoT

Os experimentos realizados permitiram observar o comportamento de diferentes classificadores aplicados ao mesmo conjunto de dados e à mesma metodologia de cálculo de PFI. De modo geral, o *Random Forest* apresentou resultados consistentes, equilibrando as métricas de Precisão e *Recall* e mantendo boa estabilidade. O *AdaBoost* teve desempenho

próximo, mostrando que combinações de classificadores simples podem gerar modelos competitivos. O *SVM Linear* destacou-se pela maior taxa de *Recall*, indicando maior capacidade de identificar eventos suspeitos, ainda que com leve redução na *Precision*. Já a *Logistic Regression* manteve resultados intermediários, com comportamento estável e boa interpretabilidade.

Nos testes com subconjuntos Top-K guiados por PFI, observou-se que o desempenho tende a se estabilizar a partir de aproximadamente $k = 30$. Isso indica que parte relevante da capacidade preditiva está concentrada em um conjunto menor de atributos, especialmente aqueles relacionados a tempo e tipo de serviço. Essa constatação sugere que é possível reduzir o número de atributos utilizados sem causar perdas significativas nas métricas de avaliação. O gráfico em formato de radar auxilia na visualização desse comportamento, evidenciando que os valores de acurácia e *F1-Score* variam pouco entre $k = 20$ e $k = 50$.

A Figura 8 apresenta curvas de importância acumulada baseada em PFI, evidenciando padrões distintos na distribuição da relevância dos atributos entre os classificadores. O modelo Random Forest apresenta uma distribuição mais homogênea, na qual a importância está diluída entre um número maior de atributos. A análise dos atributos (k) é importante para quantificar o ponto de saturação da contribuição dos atributos, permitindo avaliar até que ponto a inclusão de novos atributos agrega ganho efetivo ao modelo. Para o Random Forest, os valores obtidos foram k80 = 9, k90 = 11 e k95 = 13. Esse comportamento indica que o modelo depende de um conjunto mais amplo de atributos para manter seu desempenho. Em contraste, o AdaBoost demonstra forte concentração de importância nos primeiros atributos, alcançando 80% da importância acumulada com apenas 6 atributos, 90% com 9 atributos e 95% com 11 atributos, o que revela alta seletividade e dependência de um subconjunto reduzido de features. Os modelos lineares, Logistic Regression e SVM, apresentam comportamento intermediário, com k80 = 7, k90 = 10 e k95 = 12, indicando um equilíbrio entre concentração e distribuição da importância. Esses resultados reforçam a hipótese de que a seleção baseada em PFI é uma abordagem eficaz para otimizar a eficiência e a escalabilidade de sistemas de detecção de intrusão em ambientes IoT.

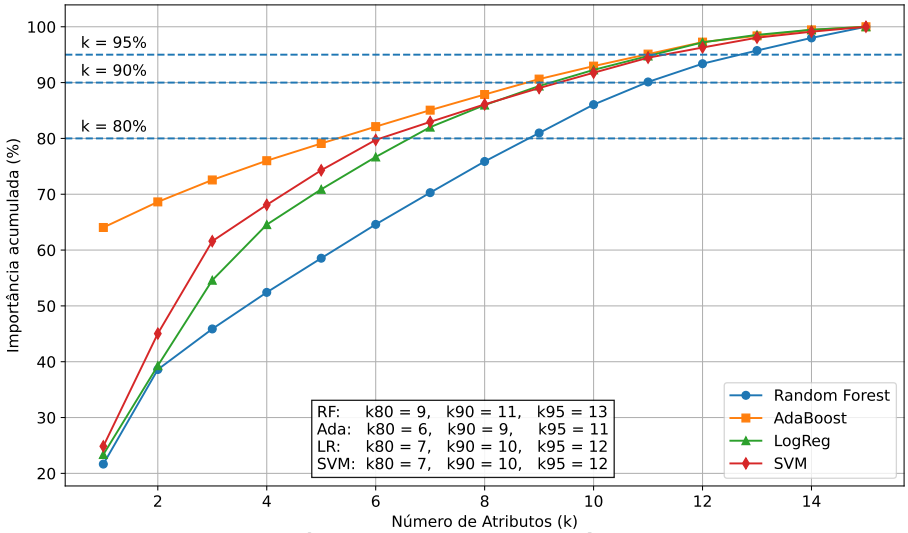

Figura 8. Importância acumulada vs Número de atributos

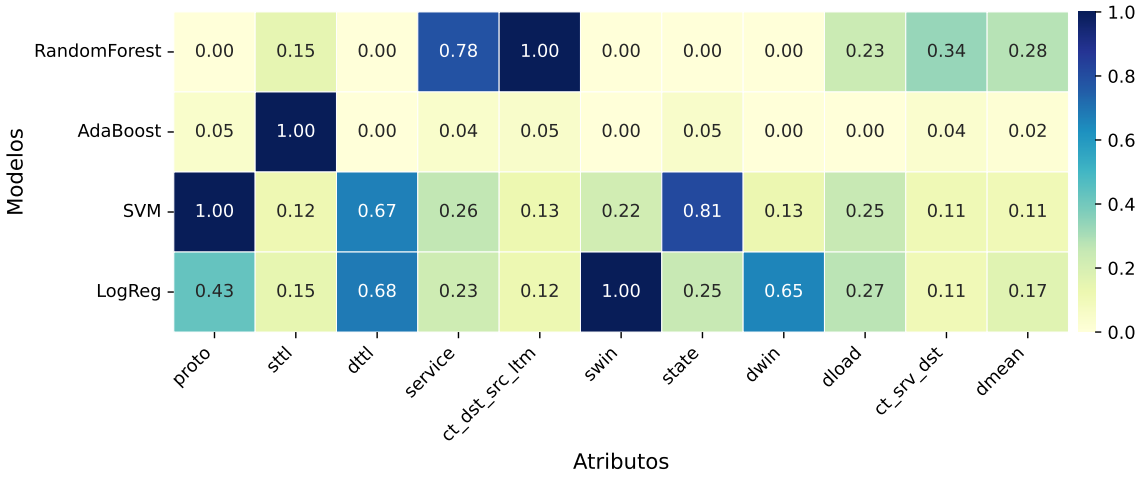

Figura 9. Comparação entre modelos e principais atributos

A Figura 9 apresenta o mapa de calor destacando a importância de atributos baseados em PFI. Permitindo, assim, uma análise comparativa da relevância dos atributos entre diferentes classificadores, evidenciando padrões de concordância e divergência no processo de aprendizagem. Observa-se que determinados atributos, como sttl, service, ct_dst_src_ltm, ct_srv_dst, dmean, e dload, apresentam relevância consistente pelo menos 3 modelos, indicando maior capacidade discriminativa e sugerindo que tais atributos capturam características fundamentais do comportamento do tráfego de rede. Por outro lado, alguns modelos exibem dependência mais concentrada em atributos específicos, como o AdaBoost, que atribui importância dominante a sttl, enquanto modelos lineares, como SVM e Regressão Logística, destacam atributos relacionados a estados de conexão e parâmetros de controle, como proto, state, dttl, swin e dwin. O Random Forest, por sua vez, apresenta uma distribuição concentrada em ct_dst_src_ltm e service e mais equilibrada entre diversos outros atributos, refletindo sua capacidade de explorar múltiplas relações não lineares. A ausência de determinados atributos em alguns modelos, representada por valores zeros, reforça a heterogeneidade dos mecanismos de aprendizado e evidencia que diferentes algoritmos capturam aspectos distintos do mesmo conjunto de dados. De forma geral, apesar das diferenças estruturais entre os modelos, existe um núcleo comum de atributos altamente relevantes, o que sustenta a viabilidade de estratégias de seleção de atributos baseadas em PFI, como o Top-K, visando reduzir a dimensionalidade sem comprometer significativamente o desempenho dos sistemas de detecção de intrusão em ambientes IoT.

De um modo geral, os experimentos concentraram-se na análise local dos classificadores, sem aplicação de mecanismos de agregação ou comunicação entre modelos. Essa escolha permitiu observar de forma isolada o impacto do PFI sobre o desempenho dos algoritmos, garantindo uma avaliação mais controlada. Essa análise preliminar também contribui para compreender o comportamento de cada modelo antes de futuras integrações em cenários distribuídos.

Adicionalmente, o PFI mostrou-se útil não apenas para interpretar a importância de cada atributo, mas também como ferramenta prática para reduzir a quantidade de dados processados. Essa característica pode contribuir para a eficiência do sistema, reduzindo o consumo de recursos e facilitando a aplicação em contextos de IoT, que normalmente apresentam restrições de processamento e energia. Em síntese, os resultados indicam

que a combinação entre aprendizado supervisionado e seleção de atributos via PFI Top-K constitui uma abordagem promissora para sistemas de detecção de intrusão. Embora os experimentos tenham sido realizados em ambiente local, as observações obtidas contribuem para orientar as próximas etapas, especialmente no contexto de integração com aprendizado federado.

5. Conclusão

Este trabalho apresentou uma arquitetura de detecção de intrusão para ambientes IoT baseada em aprendizado federado com seleção de atributos guiada por *Permutation Feature Importance* (PFI). A proposta integra a análise de importância ao ciclo de treinamento, permitindo a seleção local de atributos por meio de um mecanismo *Top-k*. Os resultados mostram que a capacidade preditiva está concentrada em um subconjunto reduzido de atributos, possibilitando a redução de dimensionalidade sem perdas significativas de desempenho. Observa-se ainda um ponto de saturação a partir de determinados valores de k, indicando um equilíbrio entre eficiência e desempenho. O uso do PFI mostrou-se eficaz não apenas para interpretação, mas também como mecanismo prático para reduzir o volume de dados processados e potencialmente transmitidos, aspecto relevante em ambientes IoT com restrições de recursos. Nesse sentido, a abordagem pode ser aplicada em cenários reais, como infraestruturas críticas, cidades inteligentes, sistemas de saúde e redes industriais. Como limitação, os experimentos foram realizados em ambiente controlado, sem a execução completa do ciclo federado. Ainda assim, os resultados fornecem evidências consistentes sobre a viabilidade da abordagem. Como trabalho futuro, pretende-se implementar e avaliar o sistema em um ambiente federado real, considerando consumo de recursos e desempenho em diferentes cenários.

Agradecimentos

O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) - Código de Financiamento 001. Foram utilizadas ferramentas de inteligência artificial como apoio na revisão textual deste trabalho.

Referências

Ali Kazmi, S. H., Hassan, R., Qamar, F., Nisar, K., and Dahnil, D. P. (2024). Threat intelligence in iomts with federated learning using non-iid data: An experimental analysis. In *2024 IEEE 7th International Symposium on Telecommunication Technologies (ISTT)*.

Barbosa, L., Dalmazo, B. L., Cordeiro, W., Immich, R., Abelém, A., and Riker, A. (2022). Deconn: Combining minimum and neutral energy consumption strategies in iot networks. In *IFIP Wireless and Mobile Networking Conference (WMNC)*.

Bittencourt, L., Immich, R., Sakellariou, R., Fonseca, N., Madeira, E., Curado, M., Villas, L., DaSilva, L., Lee, C., and Rana, O. (2018). The internet of things, fog and cloud continuum: Integration and challenges. *Internet of Things*, 3-4:134 – 155.

Chang, V., Golightly, L., Modesti, P., Xu, Q. A., Doan, L. M. T., Hall, K., Boddu, S., and Kobusińska, A. (2022). A survey on intrusion detection systems for fog and cloud computing. *Future Internet*, 14(3):89.

El Houda, Z. A., Moudoud, H., Brik, B., and Khoukhi, L. (2023). Securing federated learning through blockchain and explainable ai for robust intrusion detection in iot networks. In *IEEE Conference on Computer Communications Workshops*.

Fiorenza, M., Kreutz, D., Mansilha, R., Macedo, D., Feitosa, E., and Immich, R. (2021). Representação e aplicação de políticas de segurança em firewalls de redes híbridas. In *Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos*. SBC.

Greengard, S. (2021). *The internet of things*. MIT press.

Kil, Y.-S., Lee, Y.-J., Jeon, S.-E., Oh, Y.-S., and Lee, I.-G. (2024). Optimization of privacy-utility trade-off for efficient feature selection of secure internet of things. *IEEE Access*, 12:142582–142591.

Li, T., Sahu, A. K., Zaheer, M., Sanjabi, M., Talwalkar, A., and Smith, V. (2020). Federated optimization in heterogeneous networks. *Proceedings of Machine learning and systems*, 2:429–450.

Lieira, D. D., Quessada, M. S., Cristiani, A. L., Immich, R., and Meneguette, R. I. (2021). Triad: Whale optimization algorithm for 5g-iot resource allocation decision in edge computing. In *Iberian Conference on Information Systems and Technologies (CISTI)*.

Liu, H. and Lang, B. (2019). Machine learning and deep learning methods for intrusion detection systems: A survey. *applied sciences*, 9(20):4396.

Pei, X., Deng, X., Tian, S., Zhang, L., and Xue, K. (2023). A knowledge transfer-based semi-supervised federated learning for iot malware detection. *IEEE Transactions on Dependable and Secure Computing*, 20(3):2127–2143.

Peng, B., Chi, M., and Liu, C. (2022). Non-IID federated learning via random exchange of local feature maps for textile IIoT secure computing. *Science China Information Sciences*, 65(7):170302.

Pham, V. T., Nguyen, H. L., Le, H.-C., and Nguyen, M. T. (2023). Machine learning-based intrusion detection system for ddos attack in the internet of things. In *2023 International Conference on System Science and Engineering (ICSSE)*.

Pisani, F., de Oliveira, F., Gama, E. S., Immich, R., Bittencourt, L. F., and Borin, E. (2020). Fog computing on constrained devices: Paving the way for the future iot. *Advances in Edge Computing: Massive Parallel Processing and Applications*, 35:22.

Roy, S., Li, J., and Bai, Y. (2023). Federated learning-based intrusion detection system for iot environments with locally adapted model. In *IEEE 10th International Conference on Cyber Security and Cloud Computing (CSCloud)*. IEEE.

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*.

Silva, D., Fontes, R., Neto, A., Silva, G., and Immich, R. (2023). Esquema de autenticação e acordo de chaves para internet das coisas. In *Workshop de Gerência e Operação de Redes e Serviços*, Porto Alegre, RS, Brasil. SBC.

Thakkar, A. and Lohiya, R. (2021). A review on machine learning and deep learning perspectives of ids for iot: Recent updates, security issues, and challenges. *Archives of computational methods in engineering*, 28(4).

Thevarajan, J., Ravi, V., Kirushanth, S., Ganesalingam, V., Ahmadon, M. A., and Bt Che Lah, N. S. (2025). Federated learning for detecting anomalies in iot-driven smart home systems. In *Inter. Conference on Advancements in Computing (ICAC)*.

Wei, W., Yang, A. T., Shi, W., and Sha, K. (2016). Security in internet of things: Opportunities and challenges. In *2016 International Conference on Identification, Information and Knowledge in the Internet of Things (IIKI)*, pages 512–518. IEEE.