

UNIVERSIDADE FEDERAL DE JUIZ DE FORA
INSTITUTO DE CIÊNCIAS EXATAS
PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO

Michael Vitor Zancanella Barboza

Aprendizado de Máquina para Detecção de Ataques Mirai em Redes IoT 5G

Juiz de Fora

2026

Michael Vitor Zancanella Barboza

Aprendizado de Máquina para Detecção de Ataques Mirai em Redes IoT 5G

Dissertação apresentada ao PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO da Universidade Federal de Juiz de Fora como requisito parcial à obtenção do título de Mestre em Ciência da Computação.

Orientador: Dr. Edelberto Franco Silva

Juiz de Fora

2026

Ficha catalográfica elaborada através do Modelo Latex do CDC da UFJF
com os dados fornecidos pelo(a) autor(a)

Zancanella, Michael Vitor Barboza.

Aprendizado de Máquina para Detecção de Ataques Mirai em Redes
IoT 5G / Michael Vitor Zancanella Barboza. – 2026.
93 f. : il.

Orientador: Edelberto Franco Silva

Dissertação (Mestrado) – Universidade Federal de Juiz de Fora, INSTITUTO DE CIÊNCIAS EXATAS. PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO, 2026.

1. Internet das coisas. 2. 5G. 3. Detecção de intrusões. 4. Mirai 5. Aprendizado de máquina I. Franco Silva, Edelberto, orient. II. Título.

Michael Vitor Zancanella Barboza

Aprendizado de Máquina para Detecção de Ataques Mirai em Redes IoT 5G

Dissertação apresentada ao Programa de Pós-graduação em Ciência da Computação da Universidade Federal de Juiz de Fora como requisito parcial à obtenção do título de Mestre em Ciência da Computação. Área de concentração: Ciência da Computação.

Aprovada em 02 de outubro de 2026.

BANCA EXAMINADORA

Prof. Dr. Edelberto Franco Silva - Orientador

Universidade Federal de Juiz de Fora

Prof. Dr. Alex Borges Vieira

Universidade Federal de Juiz de Fora

Prof. Dr. Lourenço Alves Pereira Júnior

Instituto Tecnológico de Aeronáutica

Juiz de Fora, 07/10/2026.



Documento assinado eletronicamente por **Lourenço Alves Pereira Júnior, Usuário Externo**, em 07/10/2026, às 13:53, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do [Decreto nº 10.543, de 13 de novembro de 2020](#).



Documento assinado eletronicamente por **Edelberto Franco Silva, Professor(a)**, em 09/10/2026, às 14:51, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do [Decreto nº 10.543, de 13 de novembro de 2020](#).



Documento assinado eletronicamente por **Alex Borges Vieira, Coordenador(a)**, em 09/10/2026, às 16:16, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do [Decreto nº 10.543, de 13 de novembro de 2020](#).



A autenticidade deste documento pode ser conferida no Portal do SEI-Ufjf (www2.ufjf.br/SEI) através do ícone Conferência de Documentos, informando o código verificador **3273696** e o código CRC **0B7EDCB4**.

Dedico este trabalho à minha mãe, pai (*in memoriam*)
minha esposa e minha filha, pelo apoio incondicional
durante todo o curso de mestrado.

AGRADECIMENTOS

Agradeço primeiramente à Deus, por guiar meu caminho e por me cercar de pessoas incríveis que me dão a força necessária para persistir em meus objetivos.

Aos meus amados pais, Marcos (*in memoriam*) e Maria Goretti, dedico esta conquista. O amor incondicional de vocês e o exemplo de dedicação me moldaram e me deram as oportunidades de que precisei. A cada passo desta jornada, senti a presença e o apoio de vocês.

À minha querida esposa, Cássia, minha parceira incansável, que com seu amor e compreensão tornou esta jornada mais leve.

À minha filha, Antonella, que com sua alegria e inocência é minha maior inspiração.

Meus sinceros agradecimentos ao professor Edelberto Franco, por me orientar com tamanha sabedoria, dedicação e profissionalismo. Foi uma honra aprender com você.

Aos meus amigos, que foram um incentivo constante, meu muito obrigado por fazerem parte dessa caminhada.

À Universidade Federal de Juiz de Fora e ao Programa de Pós-Graduação em Ciência da Computação, sou grato pela chance de crescimento e pela excelente estrutura que impulsionaram minha formação.

“Cibercriminosos estão sempre procurando por alguma falha de segurança. E, por isso, não podemos esquecer os dispositivos portáteis, por exemplo, os aparelhos que fazem parte da Internet das Coisas (IoT).” (Almiani et. al, 2021)

RESUMO

A massificação da Internet das Coisas (IoT) impõe desafios que redes móveis legadas não suportam. Para superá-los, o 5G adota uma arquitetura baseada em serviços. Contudo, devido a restrições de custo e *hardware*, dispositivos terminais são frequentemente vulneráveis, tornando-se alvos ideais para recrutamento em *botnets* massivas, como o *malware* Mirai, para orquestrar ataques de Negação de Serviço Distribuída (DDoS). Ao empregarem ofuscação e encapsulamento (*GRE-ETH* e *GRE-IP*), esses ataques trafegam mascarados nos túneis da operadora (GTP-U), contornando filtros tradicionais. Para bloquear tais anomalias, este trabalho propõe um Sistema de Detecção de Intrusões (IDS) proativo. Inspirada na *Network Data Analytics Function* (NWDAF), a solução implementa uma Função Lógica de Análise (AnLF) como microsserviço descentralizado na camada de Névoa (*Fog Computing*). Contornando o ponto cego do encapsulamento celular, o sistema avalia fluxos (*flow-based*) extraídos na interface de saída da Função de Plano de Usuário (UPF/N6), processando tráfego IP isento do ruído do GTP-U. O treinamento baseou-se no *dataset* CICIoT2023, adotando-se o algoritmo *LightGBM* pela sua leveza e interpretabilidade. A validação empírica ocorreu em um *testbed* 5G (Open5GS e UERANSIM) submetido a um emulador estocástico, calibrado via Inteligência Artificial Explicável (SHAP) e minimização da Distância de Wasserstein (W_1). Em ambiente *offline*, o modelo atingiu F1-Macro de 0,97. Nas condições dinâmicas do *testbed*, o sistema manteve Acurácia de 88,00% e Precisão perfeita (1,00) para o tráfego legítimo, assegurando 100% de contenção das ameaças encapsuladas (0,0% de evasão). Ademais, a Adaptação de Domínio Não-Supervisionada validou a generalização cruzada em topologias inéditas (*dataset Bot-IoT*). A arquitetura avança o estado da arte ao provar que a extração estatística pós-túnel resolve a severa degradação preditiva causada pelo encapsulamento celular (GTP-U) — limitação reportada na literatura para detecções no ingresso do núcleo (interface N3). Essa abordagem, aliada a modelos de *ensemble*, elimina o custo da Inspeção Profunda de Pacotes (DPI), viabilizando a contenção de ameaças em microssegundos (16,50 μs) e protegendo redes móveis de próxima geração.

Palavras-chave: Internet das Coisas. 5G. Detecção de Intrusões. Interpretabilidade. Malware Mirai;

ABSTRACT

The massification of the Internet of Things (IoT) imposes challenges that legacy mobile networks cannot support. To overcome them, 5G adopts a service-based architecture. However, due to cost and *hardware* constraints, end devices are frequently vulnerable, making them ideal targets for recruitment into massive *botnets*, such as the Mirai *malware*, to orchestrate Distributed Denial of Service (DDoS) attacks. By employing obfuscation and encapsulation (*GRE-ETH* and *GRE-IP*), these attacks travel disguised within the operator’s tunnels (GTP-U), bypassing traditional filters. To block such anomalies, this work proposes a proactive Intrusion Detection System (IDS). Inspired by the *Network Data Analytics Function* (NWDAF), the solution implements an Analytics Logical Function (AnLF) as a decentralized microservice at the *Fog Computing* layer. Bypassing the cellular encapsulation blind spot, the system evaluates *flow-based* traffic extracted at the egress interface of the User Plane Function (UPF/N6), processing pure IP traffic free from GTP-U noise. Training was based on the CICIoT2023 *dataset*, adopting the *LightGBM* algorithm for its lightness and interpretability. Empirical validation occurred in a 5G *testbed* (Open5GS and UERANSIM) subjected to a stochastic emulator, calibrated via eXplainable Artificial Intelligence (SHAP) and Wasserstein Distance (W_1) minimization. In an *offline* environment, the model achieved a Macro F1-Score of 0.97. Under the dynamic conditions of the *testbed*, the system maintained an 88.00% Accuracy and a perfect Precision (1.00) for legitimate traffic, ensuring 100% containment of encapsulated threats (0.0% evasion). Furthermore, Unsupervised Domain Adaptation validated the cross-generalization in novel topologies (*Bot-IoT dataset*). The architecture advances the state of the art by proving that post-tunnel statistical extraction resolves the severe predictive degradation caused by cellular encapsulation (GTP-U)—a limitation reported in the literature for detections at the core ingress (N3 interface). This approach, combined with *ensemble* models, eliminates the cost of Deep Packet Inspection (DPI), enabling threat containment in microseconds (16.50 μ s) and protecting next-generation mobile networks.

Keywords: Internet of Things. 5G. Intrusion detection. Explainable AI. Mirai malware.

LISTA DE ILUSTRAÇÕES

Figura 1 – Arquitetura de três camadas da IoT detalhando os domínios de percepção, rede e aplicação.	20
Figura 2 – Linha do tempo da evolução das gerações de redes móveis, evidenciando a transição de serviços focados em voz (1G/2G) para a hiperconectividade heterogênea do 5G.	21
Figura 3 – Evolução arquitetural: a transição do núcleo rígido (EPC) no 4G para a Arquitetura Baseada em Serviços (SBA) no 5G.	23
Figura 4 – Exemplo de fatiamento de rede no núcleo 5G, destacando o compartilhamento da AMF e o isolamento das instâncias de SMF e UPF por tipo de serviço. Fonte: Elaborado pelo autor, baseado em Afolabi <i>et al.</i> (8).	24
Figura 5 – Mecânica de encapsulamento GTP-U: o pacote original é envelopado pelos cabeçalhos da operadora na interface N3.	26
Figura 6 – Arquitetura de propagação e ataque da <i>botnet</i> Mirai.	30
Figura 7 – Fluxograma da Revisão Sistemática da Literatura (RSL).	37
Figura 8 – Comparativo topológico de extração de tráfego na UPF: Abordagem da literatura <i>vs</i> Modelo Proposto.	41
Figura 9 – Diagrama de blocos do <i>pipeline</i> de Aprendizado de Máquina baseado na NWDAF.	44
Figura 10 – Arquitetura do ambiente experimental: Integração UERANSIM, Open5GS (com separação CUPS entre Plano de Controle e Plano de Usuário) e Internet.	46
Figura 11 – Matriz de confusão do modelo Random Forest.	58
Figura 12 – Matriz de confusão do modelo LightGBM.	58
Figura 13 – Importância global de características via SHAP para o modelo LightGBM.	60
Figura 14 – Validação estocástica guiada por SHAP para a classe <i>BenignTraffic</i>	62
Figura 15 – Validação estocástica guiada por SHAP para a classe <i>Mirai-greeth_flood</i>	63
Figura 16 – Validação estocástica guiada por SHAP para a classe <i>Mirai-greip_flood</i>	63
Figura 17 – Validação estocástica guiada por SHAP para a classe <i>Mirai-udpplain</i>	64
Figura 18 – Matriz de confusão da classificação operacional do tráfego sob estresse volumétrico no <i>testbed</i> 5G.	67
Figura 19 – Matriz de correlação inicial de Pearson antes da redução de dimensionalidade.	88
Figura 20 – Matriz de correlação final com o subconjunto das 11 <i>features</i> preditivas.	89
Figura 21 – Validação estocástica guiada pelo SHAP: Tráfego Benigno (<i>BenignTraffic</i>).	90
Figura 22 – Validação estocástica guiada pelo SHAP: Inundação Mirai GRE-ETH.	91
Figura 23 – Validação estocástica guiada pelo SHAP: Inundação Mirai GRE-IP.	92
Figura 24 – Validação estocástica guiada pelo SHAP: Inundação Mirai UDP-Plain.	93

LISTA DE TABELAS

Tabela 1 – Cronologia do desenvolvimento e padronização do 5G pelo 3GPP. . . .	22
Tabela 2 – Síntese comparativa dos trabalhos relacionados sob a ótica dos requisitos operacionais 5G.	40
Tabela 3 – Distribuição de amostras das classes selecionadas (CICIoT2023). . . .	49
Tabela 4 – Vetor de atributos extraídos e selecionados para o treinamento dos modelos.	52
Tabela 5 – Espaço de busca de hiperparâmetros submetido ao <i>Grid Search</i> ($k = 3$). .	53
Tabela 6 – Melhores hiperparâmetros extraídos via GridSearchCV.	55
Tabela 7 – Comparativo de desempenho e custo computacional dos modelos finais.	56
Tabela 8 – Relatório de Classificação Detalhado para o Modelo LightGBM. . . .	57
Tabela 9 – Relatório de Classificação Detalhado para o Modelo Random Forest. .	57
Tabela 10 – Valores médios e importância SHAP (ϕ) das principais variáveis por classe.	59
Tabela 11 – Avaliação da fidelidade estocástica via Distância de Wasserstein Absoluta (W_1) baseada no SHAP.	61
Tabela 12 – Desempenho de Detecção Cruzada no Bot-IoT aplicando Adaptação de Domínio Cronológica Não-Supervisionada.	69
Tabela 13 – Comparativo de desempenho do modelo LightGBM em diferentes cenários de validação.	70
Tabela 14 – Conjunto final de 11 características preditivas e atributo alvo. . . .	81
Tabela 15 – Especificações das Máquinas Virtuais (VMs) no Oracle VM VirtualBox.	85
Tabela 16 – Versões das Ferramentas de Software Utilizadas.	85

LISTA DE ABREVIATURAS E SIGLAS

3GPP	Projeto de Parceria de 3ª Geração (<i>3rd Generation Partnership Project</i>)
5G	Quinta Geração de Redes Móveis (<i>Fifth Generation Mobile Networks</i>)
5GC	Núcleo da Rede 5G (<i>5G Core</i>)
AMF	Função de Gerenciamento de Acesso e Mobilidade (<i>Access and Mobility Management Function</i>)
AnLF	Função Lógica de Análise (<i>Analytics Logical Function</i>)
CNC	Comando e Controle (<i>Command and Control</i>)
CNN	Rede Neural Convolutacional (<i>Convolutional Neural Network</i>)
CSV	Valores Separados por Vírgula (<i>Comma-Separated Values</i>)
CUPS	Separação entre os Planos de Controle e de Usuário (<i>Control and User Plane Separation</i>)
DDoS	Negação de Serviço Distribuída (<i>Distributed Denial of Service</i>)
DPI	Inspeção Profunda de Pacotes (<i>Deep Packet Inspection</i>)
eMBB	Banda Larga Móvel Aprimorada (<i>Enhanced Mobile Broadband</i>)
EPC	Núcleo de Pacote Evoluído (<i>Evolved Packet Core</i>)
FPGA	Matriz de Portas Programável em Campo (<i>Field Programmable Gate Array</i>)
gNB	Estação Rádio-Base 5G (<i>next Generation Node B</i>)
GRE	Encapsulamento de Roteamento Genérico (<i>Generic Routing Encapsulation</i>)
GTP-U	Protocolo de Tunelamento GPRS para o Plano de Usuário (<i>GPRS Tunnelling Protocol for User Plane</i>)
HTTP	Protocolo de Transferência de Hipertexto (<i>Hypertext Transfer Protocol</i>)
IDS	Sistema de Detecção de Intrusões (<i>Intrusion Detection System</i>)
IoT	Internet das Coisas (<i>Internet of Things</i>)
IP	Protocolo de Internet (<i>Internet Protocol</i>)
LGBM	Máquina de Potenciamento de Gradiente Leve (<i>Light Gradient Boosting Machine</i>)
LSTM	Memória de Longo Curto Prazo (<i>Long Short-Term Memory</i>)
LTE	Evolução de Longo Prazo (<i>Long Term Evolution</i>)
MAC	Controle de Acesso ao Meio (<i>Media Access Control</i>)
ML	Aprendizado de Máquina (<i>Machine Learning</i>)
mMTC	Comunicação Massiva do Tipo Máquina (<i>Massive Machine Type Communications</i>)
MTLF	Função Lógica de Treinamento de Modelos (<i>Model Training Logical Function</i>)
NF	Função de Rede (<i>Network Function</i>)
NFV	Virtualização de Funções de Rede (<i>Network Functions Virtualization</i>)

NSSAI	Informação de Assistência à Seleção de Fatias de Rede (<i>Network Slice Selection Assistance Information</i>)
NWDAF	Função de Análise de Dados da Rede (<i>Network Data Analytics Function</i>)
PCAP	Captura de Pacotes (<i>Packet Capture</i>)
PCF	Função de Controle de Política (<i>Policy Control Function</i>)
RAN	Rede de Acesso por Rádio (<i>Radio Access Network</i>)
RF	Floresta Aleatória (<i>Random Forest</i>)
RTT	Tempo de Ida e Volta (<i>Round-Trip Time</i>)
SBA	Arquitetura Baseada em Serviços (<i>Service-Based Architecture</i>)
SBI	Interface Baseada em Serviços (<i>Service-Based Interface</i>)
SHAP	Explicações Aditivas de Shapley (<i>SHapley Additive exPlanations</i>)
SMF	Função de Gerenciamento de Sessão (<i>Session Management Function</i>)
S-NSSAI	Informação de Assistência à Seleção de Fatias de Rede Única (<i>Single-NSSAI</i>)
SST	Tipo de Serviço ou Fatia (<i>Slice/Service Type</i>)
TCP	Protocolo de Controle de Transmissão (<i>Transmission Control Protocol</i>)
TEID	Identificador de Ponto Final de Túnel (<i>Tunnel Endpoint Identifier</i>)
UDP	Protocolo de Datagrama de Usuário (<i>User Datagram Protocol</i>)
UE	Equipamento de Usuário (<i>User Equipment</i>)
UPF	Função de Plano de Usuário (<i>User Plane Function</i>)
URLLC	Comunicações Ultraconfiáveis e de Baixa Latência (<i>Ultra-Reliable and Low Latency Communications</i>)
XAI	Inteligência Artificial Explicável (<i>Explainable Artificial Intelligence</i>)

SUMÁRIO

1	Introdução	15
2	Fundamentação Teórica	19
2.1	A Internet das Coisas (IoT) e suas Restrições	19
2.2	A Evolução das Redes Móveis e o Ecossistema 5G	20
2.2.1	Contexto Histórico: Das Gerações Iniciais à Necessidade do 5G	21
2.2.2	O Núcleo da Rede (5GC) e a Mudança de Paradigma para a SBA	22
2.2.3	O Protocolo GTP-U e a Relevância Estratégica da UPF	25
2.3	Automação e Inteligência Nativa: A Função NWDAF	26
2.4	Paradigmas de Processamento: Da Nuvem à Névoa (<i>Cloud, Edge e Fog Computing</i>)	27
2.5	Botnets e o Cenário de Ameaças: Mirai e Ataques DDoS	28
2.6	Aprendizado de Máquina e Avaliação de Desempenho	31
2.6.1	Ciclo de Vida do Modelo	31
2.6.2	Métricas de Desempenho	32
2.7	Considerações Finais do Capítulo	33
3	Trabalhos Relacionados	35
3.1	Revisão Sistemática da Literatura	35
3.2	Análise dos Trabalhos Relacionados	38
3.3	Síntese Comparativa e Posicionamento do Trabalho	40
3.4	Síntese do Capítulo	42
4	Metodologia	44
4.1	Pipeline de Aprendizado de Máquina e Arquitetura NWDAF	44
4.2	Ambiente de Simulação 5G e Emulação de Tráfego	45
4.3	O Conjunto de Dados <i>CICIoT2023</i>	49
4.4	Implementação da Funcionalidade NWDAF	50
4.4.1	Preparação, Extração e Engenharia de Atributos	50
4.4.2	Detalhes de Implementação e Execução do Modelo	51
4.5	Síntese do Capítulo	54
5	Resultados e Discussão	55
5.1	Definição da Linha de Base e Hiperparâmetros Ótimos	55
5.2	Desempenho Comparativo e Custo Computacional	56
5.3	Análise de Interpretabilidade (XAI) com SHAP	59
5.4	Validação da Fidelidade Estatística do Tráfego Emulado	61
5.5	Aplicação da Proposta e Avaliação Topológica na Fatia 5G	65
5.5.1	Impacto do Encapsulamento GTP-U e a Latência Sistêmica da UPF	65
5.5.2	Avaliação Preditiva no Ambiente de Emulação 5G	66
5.6	Discussão, Implicações Práticas e Generalização	68

5.6.1	Validação de Generalização Cruzada (Dataset Bot-IoT)	68
5.6.2	Os Pilares da Viabilidade em Redes 5G	70
5.7	Síntese do Capítulo	71
6	CONCLUSÃO E TRABALHOS FUTUROS	72
6.1	Limitações e Delimitações	72
6.2	Trabalhos Futuros	73
	REFERÊNCIAS	75
	APÊNDICE A – Descrição das <i>features</i> selecionadas	81
	APÊNDICE B – Código-Fonte: Motor Estocástico de Geração de Tráfego (<code>synth_generator.py</code>)	82
	APÊNDICE C – Código-Fonte: Injetor e Escalonador de Alta Fidelidade (<code>inject.py</code>)	83
	APÊNDICE D – Código-Fonte: Servidor de Inferência (<code>app.py</code>)	84
	APÊNDICE E – Configuração Detalhada do Ambiente de Testes e Componentes 5G	85
	APÊNDICE F – Matrizes de Correlação Linear (Seleção de Atributos)	88
	APÊNDICE G – Validação Estocástica do Tráfego Sintético (XAI)	90

1 Introdução

A integração massiva de dispositivos da Internet das Coisas (*Internet of Things* - IoT) transformou a sociedade, conectando desde eletrodomésticos até infraestruturas de cidades inteligentes e indústrias (71, 65). No entanto, conectar bilhões de máquinas impôs um limite que as redes de telefonia móvel, como o 4G/LTE, não foram projetadas para suportar. Essas infraestruturas foram construídas com foco no tráfego humano (*Human-to-Human* - H2H), utilizando equipamentos físicos centralizados para fornecer banda larga móvel a *smartphones*. A tentativa de conectar milhões de sensores IoT simultaneamente nessas redes tradicionais gera um excesso de mensagens de tamanho reduzido, o que eleva drasticamente a carga de sinalização, causa congestionamentos graves e esgota os recursos do núcleo do sistema (9).

Para resolver esse problema e acomodar a comunicação entre máquinas, a quinta geração de redes móveis (5G) foi criada com um pensamento totalmente diferente (12). Em vez de depender apenas de *hardwares* pesados, o 5G transformou os componentes da rede em programas de computador, um processo conhecido como “softwarização”. Segundo as diretrizes do consórcio 3GPP (*3rd Generation Partnership Project*) (4), essa nova arquitetura converte equipamentos físicos em módulos lógicos independentes. A grande vantagem dessa mudança é permitir o fatiamento da rede (*Network Slicing*). Na prática, isso significa que o 5G consegue criar várias redes virtuais isoladas usando a mesma infraestrutura física: uma “fatia” pode fornecer altíssima velocidade para celulares convencionais, enquanto outra é configurada especificamente para suportar o tráfego massivo de sensores da IoT, sem que uma interfira diretamente na outra. Além disso, operadoras podem utilizar essas tecnologias de compartilhamento para integrar infraestrutura com outras empresas, as chamadas operadoras virtuais móveis (MVNO - *Mobile Virtual Network Operator*).

Apesar dos avanços arquiteturais do 5G para suportar a comunicação massiva, o elo mais fraco dessa integração, em geral, reside na segurança dos próprios equipamentos IoT. Devido a rígidas restrições de custo e limitações de *hardware* (bateria e processamento), muitos desses sensores são fabricados e implantados com vulnerabilidades estruturais críticas. Como aponta a literatura (49), é comum o uso de credenciais de fábrica inalteráveis, a exposição de serviços de gerenciamento obsoletos e a incapacidade de suportar mecanismos robustos de atualização. Quando expostos à Internet, esses aparelhos desprotegidos tornam-se alvos e, ao serem infectados e controlados remotamente, formam uma rede zumbi (*botnet*). Um dos exemplos mais emblemáticos desse cenário é o *malware* Mirai (13, 43), um código malicioso especializado em sequestrar sensores residenciais e industriais.

Uma vez sequestrados pela *botnet*, esses dispositivos são utilizados como fontes para orquestrar ataques de Negação de Serviço Distribuída (DDoS — *Distributed Denial of Service*). Para ilustrar o impacto e a viabilidade operacional dessa ameaça, considere o cenário

de um campus universitário inteligente (*Smart Campus*) provido por uma rede 5G privada. Nesse ambiente, a rede conecta uma miríade de dispositivos heterogêneos — câmeras de segurança de alta resolução, catracas eletrônicas, sensores de laboratório e *smartphones* de alunos —, cujos fluxos são gerenciados por múltiplas *User Plane Functions* (UPFs) distribuídas geograficamente. Embora a motivação da defesa resida na vulnerabilidade intrínseca desses sensores IoT na borda, o que o sistema de monitoramento observa de fato no núcleo celular não são dispositivos isolados, mas sim o tráfego de transporte agregado que converge e deságua na interface N6 — o enlace crítico de roteamento que conecta as múltiplas UPFs à rede de dados externa. Neste ponto de convergência, se os sensores do campus forem cooptados por uma variante do Mirai, o problema central agrava-se: em vez de a infraestrutura 5G ser apenas a vítima local, a sua altíssima capacidade de transmissão e baixa latência transformam-na em um poderoso vetor de ataque. A rede móvel atua involuntariamente como um amplificador da ameaça, permitindo que os invasores projetem inundações volumétricas massivas contra alvos externos (como servidores na Internet), empregando desde inundações diretas (*UDP-Plain*) até evasões baseadas em protocolos encapsulados (*GRE-IP* e *GRE-ETH*) (13).

Nesse cenário, a interface N6 torna-se a última linha de defesa antes que a infraestrutura 5G projete o ataque para o exterior. Contudo, o encapsulamento dos pacotes funciona escondendo o tráfego malicioso dentro de outro pacote de rede, aparentemente legítimo. Para combater esses ataques, as arquiteturas de defesa convencionais baseadas em Inspeção Profunda de Pacotes (DPI) e redirecionamento para a Nuvem (*Cloud*) tornam-se ineficazes. A inspeção exaustiva pacote a pacote impõe um severo gargalo computacional (66). Além disso, no cenário de mitigação na Nuvem, o desvio da rota cria uma latência intolerável, permitindo que o volume massivo de tráfego atinja o alvo antes da aplicação da regra de bloqueio (56, 58).

Uma proteção eficaz exige que a segurança seja validada no exato ponto de estrangulamento. A inspeção direta na estação rádio-base (gNB), por exemplo, é inviável, visto que consome recursos de processamento que devem ser estritamente dedicados à modulação de radiofrequência e à gestão de mobilidade, além de lidar com tráfego ainda encapsulado pelo protocolo de rádio. Por outro lado, a interface N6 surge como o ponto estratégico ideal para monitoramento: o tráfego de transporte já percorreu o túnel GTP-U, foi agregado pela UPF e encontra-se pronto para roteamento externo. Mover a inteligência de detecção para a camada de Névoa (*Fog Computing*) adjacente à N6 permite neutralizar a ameaça de forma descentralizada, impedindo que a velocidade do 5G seja convertida em uma arma. Essa abordagem alinha-se ao conceito da *Network Data Analytics Function* (NWDAF), um módulo padronizado do 5G responsável por coletar e processar métricas de comportamento (3).

O problema central que norteia esta pesquisa, entretanto, reside em uma lacuna metodológica observada na transição de sistemas de segurança do laboratório para esse

ambiente operacional 5G: a grande assimetria estocástica entre as bases de dados estáticas utilizadas no treinamento de modelos e a dinâmica ofuscada do tráfego celular vivo. O encapsulamento em túneis da operadora causa uma limitação de observabilidade que impede os extratores convencionais de acessarem os mesmos metadados profundos que estavam disponíveis na fase de treinamento (41). Diante dessa barreira, a questão de pesquisa que motiva este trabalho é: “*Como projetar e validar um Sistema de Detecção de Intrusões (IDS) capaz de identificar inundações evasivas do malware Mirai em infraestruturas 5G com baixa latência, garantindo a paridade metodológica (schema parity) entre a extração de dados sintéticos e a captura restrita no tráfego celular?*”

O objetivo geral deste trabalho é desenvolver, otimizar e validar um IDS proativo, fundamentado em algoritmos de *ensemble* baseados em fluxos, projetado para operar na camada de Névoa da interface N6 na detecção do *malware* Mirai. A escolha pelos algoritmos *Random Forest* e *LightGBM* justifica-se por sua eficiência em mapear fronteiras de decisão não-lineares com baixo custo computacional na inferência, tornando-os ideais para ambientes com restrições de latência (21, 39).

Para alcançar este propósito, o trabalho propõe-se a instanciar um *testbed* 5G (Open5GS e UERANSIM), desenvolver um *pipeline* de extração com paridade de esquema, comparar o desempenho preditivo dos classificadores sobre o conjunto CICIoT2023, e aplicar a Inteligência Artificial Explicável (XAI) para auditar a lógica de decisão na Névoa. Avalia-se ainda a capacidade de generalização estrutural do sistema por meio da Adaptação de Domínio Não-Supervisionada.

Nesse contexto, as principais contribuições desta pesquisa distribuem-se em frentes arquiteturais, computacionais, experimentais e analíticas. O trabalho avança o estado da arte ao consolidar a extração de metadados na camada de Névoa (Interface N6), viabilizando a classificação baseada em fluxos sem a necessidade de DPI, o que atende aos orçamentos de latência da rede celular (55, 38). Experimentalmente, quantifica-se o fenômeno de *Data Shift* imposto pelas latências estocásticas das filas da UPF (31). Analiticamente, a aplicação do método SHAP, aliada à Distância de Wasserstein, garante a auditabilidade da identificação de ofuscação. Apesar das contribuições apresentadas, delimita-se no escopo analítico desta pesquisa a avaliação da paridade de esquema e do desempenho preditivo dos algoritmos. Nesse sentido, e em consonância com as limitações amplamente reconhecidas na literatura da área, registra-se a ausência de uma caracterização formal da carga de trabalho (*workload*) de tráfego. Devido à escassez de perfis de tráfego 5G reais e públicos, e à complexidade inerente de modelar toda a variabilidade e concorrência de um ambiente de produção, a injeção no *testbed* restringe-se a padrões estocásticos controlados. Trabalhos futuros devem englobar a validação do sistema sob cargas de trabalho formalmente caracterizadas, refletindo o tráfego de fundo (*background traffic*) e as flutuações de um ecossistema de larga escala.

Durante o desenvolvimento da pesquisa, o arcabouço arquitetural e a avaliação preliminar originaram o artigo *Machine Learning for Mirai Attack Detection in 5G-Enabled IoT Networks*, apresentado na *13th Wireless Days Conference (WD 2025)* (73). Um segundo artigo, *A Decentralized Fog-NWDAF Architecture for Mirai Attack Detection in 5G IoT Networks*, aceito no simpósio *WPMC*, consolida a validação de domínio e os testes sob estresse. Os códigos-fonte do ambiente encontram-se abertos em repositório público¹.

O restante deste documento está assim organizado: o Capítulo 2 fundamenta o referencial teórico (5G, NWDAF e IoT); o Capítulo 3 promove uma revisão sistemática e crítica do estado da arte; o Capítulo 4 detalha o percurso metodológico, a topologia do *testbed* e a otimização dos classificadores; o Capítulo 5 discute pormenorizadamente os resultados experimentais, a validação estatística e a interpretabilidade (XAI); e o Capítulo 6 sintetiza as conclusões, as limitações metodológicas e direciona trabalhos futuros.

¹ <https://github.com/MichaelZancanellaUFJF/ids-5g>

2 Fundamentação Teórica

Durante as últimas décadas, a Internet passou por uma profunda evolução. O que inicialmente foi concebido como uma simples rede de troca de dados entre servidores evoluiu para um sistema onipresente, onde praticamente qualquer objeto físico atua como um potencial nó de rede (25). Essa hiperconectividade tornou-se a espinha dorsal de infraestruturas modernas, impulsionando desde a automação da Indústria 4.0 até a gestão inteligente de centros urbanos e sistemas de saúde (71, 33).

Contudo, a velocidade com que essa adoção em massa ocorreu gerou um descompasso fundamental entre conectividade e segurança. A urgência do mercado em lançar dispositivos cada vez mais baratos e integrados fez com que os requisitos de segurança fossem frequentemente negligenciados na fase de projeto (*security by design*) (65). Como resultado, o ambiente digital expandiu sua superfície de ataque de forma exponencial. Diferente das redes corporativas tradicionais, que operam sob perímetros bem definidos e *firewalls* robustos, as redes modernas são altamente distribuídas e heterogêneas, diluindo as fronteiras clássicas de proteção (60).

Nesse cenário, a convergência entre trilhões de sensores e redes móveis de altíssima capacidade criou um paradoxo de segurança: ao mesmo tempo em que a rede possibilita inovações disruptivas, ela fornece a infraestrutura perfeita para que cibercriminosos orquestram ataques em escala global de forma rápida e volumétrica (75). Para compreender a magnitude dessa ameaça e a necessidade de sistemas de defesa distribuídos, é imprescindível analisar os elementos que compõem a base desse sistema: os próprios dispositivos conectados.

2.1 A Internet das Coisas (IoT) e suas Restrições

A Internet das Coisas (IoT - *Internet of Things*) consolida-se como o modelo tecnológico que estende a conectividade da rede global a objetos físicos do cotidiano, permitindo que estes colem e troquem dados de forma autônoma (71). Do ponto de vista arquitetônico, a literatura converge para um modelo de referência estruturado em três níveis interdependentes, conforme ilustrado na Figura 1, delineando a pilha tecnológica desde a captura física da informação até a sua utilização final (23).

O fluxo de funcionamento desse sistema inicia-se na base da estrutura, denominada camada de percepção. Formada essencialmente por sensores, atuadores e identificadores, essa etapa tem a responsabilidade primária de interagir com o ambiente físico para capturar dados brutos. Uma vez coletada, a informação é encaminhada para a camada de rede, que atua como a espinha dorsal de transporte e roteamento do ecossistema. Dependendo dos requisitos da aplicação, essa transmissão ocorre por meio de tecnologias heterogêneas, que variam desde protocolos de baixo consumo energético até conexões celulares de altíssima



Figura 1 – Arquitetura de três camadas da IoT detalhando os domínios de percepção, rede e aplicação.

Fonte: Elaborado pelo autor, adaptado de Chaabouni *et al.* (23).

capacidade, como o 5G, garantindo que os dados alcancem os *gateways* ou servidores na nuvem. Por fim, o ciclo se encerra na camada de aplicação, responsável por traduzir esses dados em serviços finais de valor agregado, viabilizando soluções como automação industrial avançada e o monitoramento em cidades inteligentes (23).

Embora essa topologia integrada permita a escalabilidade de bilhões de dispositivos, ela evidencia um gargalo crítico em sua camada mais elementar. A base da pirâmide da IoT é composta por *hardware* com limitações de processamento, memória e capacidade energética. Conforme aponta Neshenko *et al.* (49), essas restrições físicas inviabilizam a execução de rotinas de segurança tradicionais, tornando muitos desses dispositivos incapazes de suportar algoritmos criptográficos robustos ou de receber atualizações frequentes de *firmware*. A combinação letal entre essa fragilidade computacional intrínseca na camada de percepção e a alta disponibilidade de conexão fornecida pela camada de rede torna a infraestrutura IoT um vetor altamente atrativo. Como consequência, tais equipamentos tornam-se alvos para recrutamento em ataques cibernéticos em larga escala, atuando frequentemente como os nós primários em redes zumbis (*botnets*).

2.2 A Evolução das Redes Móveis e o Ecossistema 5G

Para compreender como a quinta geração de redes móveis (5G) revolucionou a conectividade da Internet das Coisas e, simultaneamente, introduziu novos paradigmas de segurança, é imprescindível analisar a sua trajetória evolutiva e as suas fundações

arquiteturais. Esta seção delinea o avanço das infraestruturas celulares, transitando do panorama histórico das gerações legadas para a consolidação da Arquitetura Baseada em Serviços (SBA). Na sequência, serão exploradas as inovações de virtualização e fatiamento de rede (*Network Slicing*), culminando na análise do protocolo de tunelamento GTP-U e na relevância tática da Função de Plano de Usuário (UPF) como o ponto focal para a interceptação de ameaças no núcleo móvel.

2.2.1 Contexto Histórico: Das Gerações Iniciais à Necessidade do 5G

A trajetória das redes móveis celulares é pautada por saltos tecnológicos a cada década, desenhados para responder às crescentes exigências da sociedade e do mercado, conforme ilustrado na Figura 2. As duas primeiras gerações (1G e 2G) focaram essencialmente na viabilização e massificação da voz e mensagens de texto (SMS), transacionando do meio analógico para o digital. Com o advento do 3G e, de forma mais consolidada, do 4G (LTE - *Long Term Evolution*), o foco deslocou-se para a comunicação de dados e o acesso ubíquo à Internet de banda larga móvel, impulsionando a era dos *smartphones* (63).



Figura 2 – Linha do tempo da evolução das gerações de redes móveis, evidenciando a transição de serviços focados em voz (1G/2G) para a hiperconectividade heterogênea do 5G.

Fonte: Elaborado pelo autor.

Contudo, a proliferação da Internet das Coisas (IoT) evidenciou as limitações estruturais da infraestrutura 4G. O núcleo dessa rede (*Evolved Packet Core* - EPC) foi projetado para lidar fundamentalmente com o tráfego humano, que se caracteriza por requisições de alto volume de dados (como *streaming*), mas com um número previsível e controlável de conexões ativas (9). Com a projeção de bilhões de sensores conectados operando de forma autônoma, a infraestrutura 4G depara-se com um estrangulamento crítico na sua capacidade de gerenciar o volume massivo de sinalizações. Esta limitação arquitetural inviabiliza o suporte à densidade extrema de dispositivos exigida pelo paradigma mMTC (*massive Machine-Type Communications*), essencial para a consolidação da Internet das Coisas (IoT) em larga escala (9).

Para suprir este vazio tecnológico e suportar a hiperconectividade, a definição das novas normas foi capitaneada pelo *3rd Generation Partnership Project* (3GPP). O 3GPP é um consórcio global formado pela união de diversas organizações regionais de padronização de telecomunicações — como o ETSI na Europa, o ATIS na América do

Norte e entidades equivalentes na Ásia. Criado originalmente no final da década de 1990 para ditar os rumos do 3G, o consórcio consolidou-se como a autoridade máxima mundial na especificação da arquitetura, protocolos e diretrizes de segurança para as redes celulares de banda larga. Mais do que uma mera evolução nas taxas de transferência da interface de rádio, as especificações do 3GPP para o 5G representam uma revolução holística na arquitetura da rede. Elas redefinem as fronteiras da comunicação móvel para acomodar cenários heterogêneos, desde a banda larga aprimorada (eMBB), passando por comunicações ultraconfiáveis e de baixa latência (URLLC), até a comunicação massiva entre máquinas (mMTC) (63, 48).

A consolidação dessas especificações, no entanto, não ocorreu de forma imediata, mas sim através de um cronograma de padronização contínuo e iterativo liderado pelo 3GPP, estruturado em pacotes técnicos denominados *Releases*. A Tabela 1 sumariza os principais marcos evolutivos do 5G. Observa-se que, enquanto as etapas iniciais priorizaram a entrega de banda larga, as versões subsequentes (*Releases* 16 e 17) foram cruciais para a introdução dos pilares desta dissertação: os aprimoramentos para a IoT Industrial e a integração nativa da inteligência de rede (NWDAF).

Tabela 1 – Cronologia do desenvolvimento e padronização do 5G pelo 3GPP.

Ano	Marco / <i>Release</i>	Principais Contribuições e Foco Tecnológico
2015	Visão IMT-2020	Definição dos requisitos globais (eMBB, URLLC, mMTC) pela UIT.
2017	<i>Release 15</i> (NSA)	Foco na banda larga (eMBB). Rádio 5G (NR) ancorado no núcleo 4G (EPC).
2018	<i>Release 15</i> (SA)	Especificação do núcleo 5G autêntico (5GC) e arquitetura baseada em microserviços (SBA).
2020	<i>Release 16</i>	Expansão para a indústria: aprimoramentos em URLLC, suporte à IoT Industrial e introdução oficial da função NWDAF.
2022	<i>Release 17</i>	Otimizações para dispositivos com restrição de recursos (IoT/RedCap) e melhorias estruturais de coleta de dados na NWDAF.
2024	<i>Release 18</i>	Início do ciclo <i>5G-Advanced</i> : integração profunda de <i>Machine Learning</i> em todas as camadas da rede.

Fonte: Elaborado pelo autor, com base no histórico do 3GPP e ITU-R.

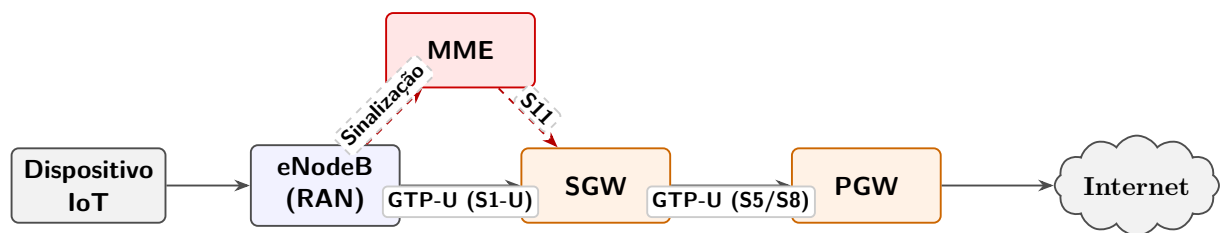
2.2.2 O Núcleo da Rede (5GC) e a Mudança de Paradigma para a SBA

A transição para a quinta geração de redes móveis (5G) estabelece uma ruptura definitiva com o modelo de *hardware* dedicado das gerações anteriores, introduzindo o

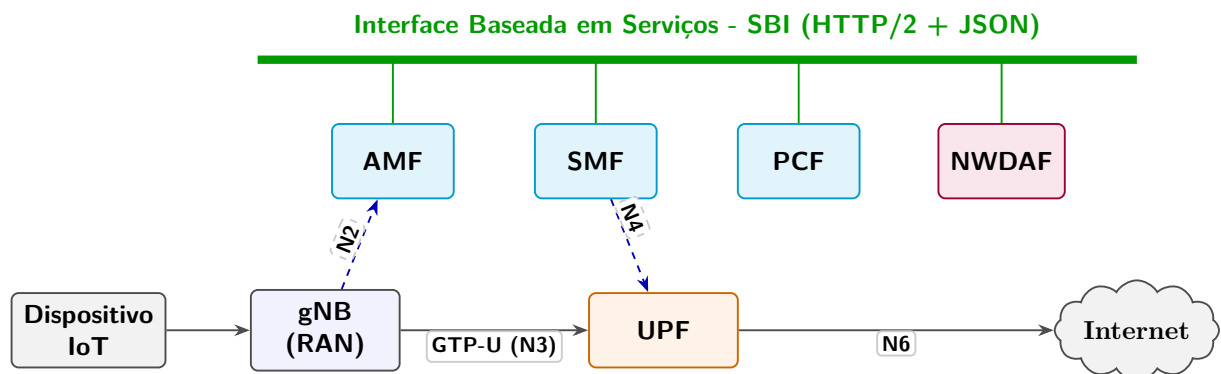
sistema 5G (*5G System* - 5GS). Enquanto o núcleo 4G (EPC) operava de forma monolítica e pouco escalável, o núcleo 5G (*5G Core* - 5GC) é fundamentado na Arquitetura Baseada em Serviços (*Service-Based Architecture* - SBA) (4). Nesta abordagem, as Funções de Rede (NFs) são concebidas como microsserviços independentes que expõem as suas capacidades através de Interfaces Baseadas em Serviços (SBI), utilizando protocolos abertos da *web* como HTTP/2 e serialização JSON para a comunicação no plano de controle.

Figura 3 – Evolução arquitetural: a transição do núcleo rígido (EPC) no 4G para a Arquitetura Baseada em Serviços (SBA) no 5G.

Arquitetura 4G: Evolved Packet Core - Monolítica



Arquitetura 5G: Service-Based Architecture e Slicing



Fonte: Elaborado pelo autor, adaptado de Nguyen *et al.* (52) e especificações do 3GPP (2, 4).

Essa *softwarização* é o que viabiliza a Separação entre o Plano de controle e o Plano de Usuário (CUPS - *Control and User Plane Separation*). Um dos pilares operacionais viabilizados por essa flexibilidade arquitetural é o Fatiamento de Rede (*Network Slicing*). Conforme o mapeamento exaustivo conduzido por Afolabi *et al.* (8), o fatiamento permite a criação de múltiplas redes lógicas independentes e isoladas a operarem simultaneamente sobre uma mesma infraestrutura física subjacente. Esse paradigma garante que serviços com requisitos de desempenho diametralmente opostos — como a massiva densidade de conexões da IoT e a altíssima vazão de vídeo sob demanda — coexistam sem interferência mútua.

Do ponto de vista arquitetural, uma das abordagens mais eficientes para otimizar os recursos do núcleo é o compartilhamento de funções do plano de controle, mantendo a segregação estrita no plano de usuário. A Figura 4 ilustra essa topologia: uma função central de controle, como a *Access and Mobility Management Function* (AMF), é compartilhada para gerir a sinalização e a mobilidade de todos os dispositivos. A partir desse ponto, o sistema instancia fatias dedicadas para serviços específicos, como as Comunicações Massivas do Tipo Máquina (mMTC). Nesse modelo, cada segmento aloca a sua própria *Session Management Function* (SMF) e as suas respectivas instâncias de Função de Plano de Usuário (UPF).

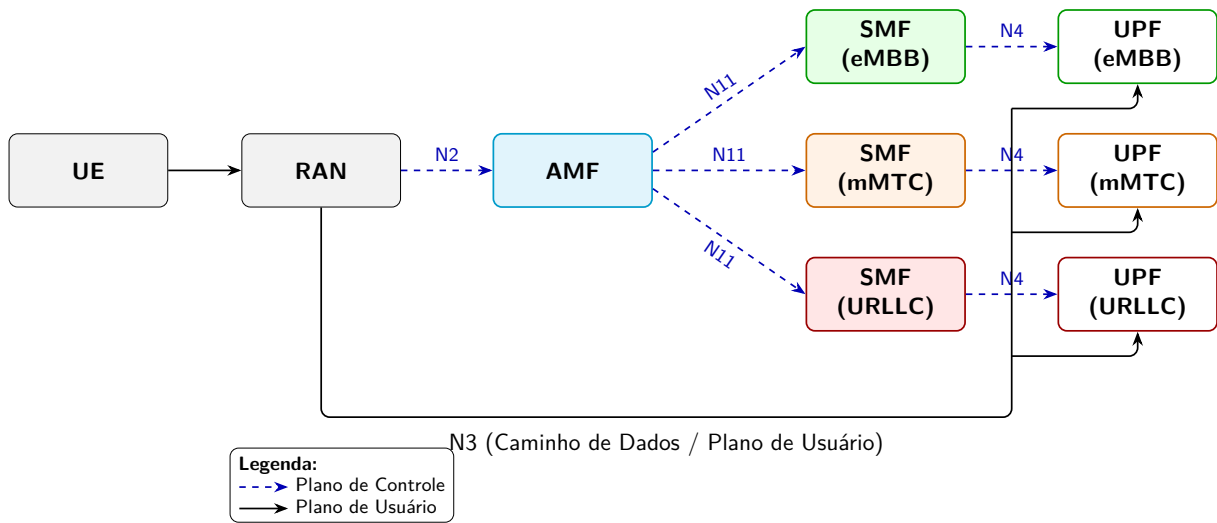


Figura 4 – Exemplo de fatiamento de rede no núcleo 5G, destacando o compartilhamento da AMF e o isolamento das instâncias de SMF e UPF por tipo de serviço. Fonte: Elaborado pelo autor, baseado em Afolabi *et al.* (8).

Para que o tráfego de um dispositivo seja roteado para a Função de Plano de Usuário (UPF) correta da sua respectiva fatia, o 3GPP estabeleceu um mecanismo de descoberta e seleção baseado na Informação de Assistência à Seleção de Fatias de Rede (*Network Slice Selection Assistance Information* - NSSAI) (8). O NSSAI é composto por identificadores únicos denominados S-NSSAI (*Single-NSSAI*), que definem o Tipo de Serviço ou Fatia (SST - *Slice/Service Type*) (8). Para garantir a interoperabilidade global, foram padronizados valores de SST: o SST=1 refere-se ao tráfego de banda larga humano (eMBB), o SST=2 é designado para serviços críticos de latência ultrabaixa (URLLC), e o SST=3 corresponde à conectividade massiva de Internet das Coisas (mMTC) (8).

O fluxo de seleção ocorre no momento em que o dispositivo IoT estabelece a conexão com a Rede de Acesso por Rádio (RAN). O equipamento transmite o seu respectivo identificador S-NSSAI (por exemplo, SST=3) nos parâmetros de sinalização. A estação rádio base (gNB) encaminha essa requisição para a *Access and Mobility Management Function* (AMF) compartilhada. Ao decodificar o identificador, a AMF aciona a *Session*

Management Function (SMF) dedicada exclusivamente àquela fatia específica. A SMF, por sua vez, estabelece a sessão de dados (*PDU Session*) e designa a UPF isolada que será responsável por processar o tráfego daquele dispositivo (8).

É esta rigorosa orquestração de sinalização que garante que o tráfego proveniente de sensores e dispositivos máquina-a-máquina (potenciais vetores de infecções *botnets*) seja canalizado obrigatoriamente para a UPF da fatia mMTC/URLLC, isolando as anomalias volumétricas do restante da infraestrutura celular.

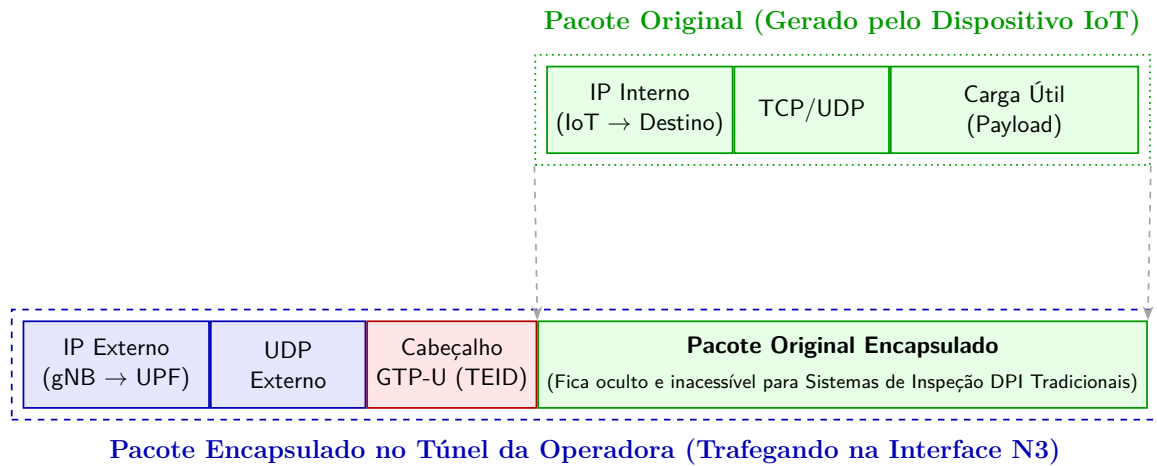
2.2.3 O Protocolo GTP-U e a Relevância Estratégica da UPF

Um elemento central para o roteamento e a segurança na arquitetura 5G é a mecânica do protocolo GTP-U (*GPRS Tunneling Protocol for User Plane*). Operando primariamente na interface N3 — que conecta a Rede de Acesso (gNB) à Função de Plano de Usuário (UPF) —, o GTP-U atua como uma camada de abstração topológica. Quando um dispositivo IoT transmite dados, o pacote IP original gerado pelo equipamento (contendo os endereços de origem e destino da aplicação) é encapsulado ao ingressar na rede celular. Este processo de “envelopamento” insere o datagrama original dentro de um novo pacote, adicionando cabeçalhos de roteamento externos (IP e UDP) e um cabeçalho específico do protocolo GTP, o qual carrega um Identificador de Ponto Final de Túnel (TEID - *Tunnel Endpoint Identifier*) (5).

É precisamente a mecânica deste túnel que viabiliza a mobilidade ininterrupta e o ancoramento de sessão (*Session Anchoring*) de forma transparente ao usuário. Como o dispositivo IoT preserva o seu endereço IP interno inalterado, as conexões ativas (como *sockets* TCP e fluxos de telemetria) não são derrubadas caso o equipamento se desloque fisicamente entre diferentes antenas. Durante um *handover*, o núcleo 5G apenas atualiza as coordenadas do túnel externo, enquanto a UPF atua como a âncora fixa que deságua o tráfego na rede externa (Internet) sempre a partir do mesmo ponto. Contudo, sob a ótica da cibersegurança, esse mesmo encapsulamento que garante a mobilidade cria um “ponto cego” estrutural: o tráfego viaja ofuscado através da interface N3, impedindo que Sistemas de Detecção de Intrusão inspecionem as verdadeiras assinaturas do fluxo antes que o pacote seja desencapsulado pela UPF.

A UPF atua como a fronteira definitiva entre o sistema celular e a Rede de Dados (DN) externa. É exclusivamente nesta Função de Rede que ocorre o processo de desencapsulamento, onde os cabeçalhos GTP da operadora são removidos, e o pacote original é roteado para a Internet (4). Sob a ótica de monitorização de rede e cibersegurança, essa característica estrutural estabelece a UPF como o ponto focal estratégico. Qualquer inspeção de tráfego realizada em nós anteriores à UPF estaria limitada à visualização de pacotes mascarados pelo túnel GTP, impossibilitando a análise profunda do *payload* e a identificação precisa de anomalias geradas pelo utilizador.

Figura 5 – Mecânica de encapsulamento GTP-U: o pacote original é envelopado pelos cabeçalhos da operadora na interface N3.



Fonte: Elaborado pelo autor com base na especificação 3GPP TS 29.281 (5).

Adicionalmente, embora o ecossistema 5G preveja mecanismos de inteligência e automação nativos no plano de controle — tema que será aprofundado na Seção 2.3 —, a literatura adverte que depender exclusivamente do núcleo central para mitigar ataques volumétricos intensivos, satura os enlaces de transporte (*backhaul*). Conforme evidenciado por Chouman *et al.* (24) e Pham *et al.* (58), essa centralização analítica introduz severos gargalos de sinalização nas Interfaces Baseadas em Serviços (SBI) e um atraso de propagação (*Round-Trip Time*) incompatível com os requisitos de fatias de missão crítica. A solução de segurança apresentada nesta dissertação inspira-se nos padrões analíticos do 5G, mas resolve essa limitação temporal ao deslocar o motor de detecção proativamente para o plano de usuário (junto à UPF). Ao operar sob o paradigma de processamento descentralizado em Névoa (*Fog*), o modelo garante a interceptação e mitigação da ameaça exata no momento em que ela é desencapsulada, bloqueando o ataque antes que ele utilize a alta capacidade da operadora para atingir a Internet ou o seu alvo final.

2.3 Automação e Inteligência Nativa: A Função NWDAF

Para gerenciar a complexidade intrínseca da Arquitetura Baseada em Serviços (SBA), o consórcio 3GPP introduziu a Função de Análise de Dados da Rede (*Network Data Analytics Function* – NWDAF) como o motor de inteligência analítica nativo do núcleo 5G (3). Conforme detalhado por Chouman, Manias e Shami (24), a NWDAF rompe com o modelo de monitoramento estritamente passivo ao estabelecer um arcabouço padronizado para a coleta autônoma de dados e o fornecimento de inferências estatísticas às demais Funções de Rede (NFs). Operando por meio de Interfaces Baseadas em Serviços (SBI), a NWDAF interage dinamicamente com o ecossistema celular para consumir telemetria

de funções — como AMF, SMF e UPF —, transformando dados brutos em *insights* operacionais acionáveis.

A implementação prática desta função é estruturada em um ciclo iterativo de processamento de dados. A primeira etapa consiste na subscrição e coleta, na qual a NWDAF utiliza serviços padronizados, como o *Nnf_EventExposure*, para solicitar estatísticas de tráfego às funções do núcleo. Em seguida, as informações brutas extraídas da rede são normalizadas e convertidas em vetores de características (*features*) compatíveis com modelos de Aprendizado de Máquina.

Para viabilizar a análise avançada, a arquitetura moderna da NWDAF promove o desacoplamento estratégico de suas capacidades em duas funções lógicas distintas. A primeira é a Unidade Lógica de Treinamento de Modelos (*Model Training Logical Function* – MTLF), responsável por orquestrar o treinamento algorítmico, frequentemente de forma *offline* ou em repositórios com alta capacidade computacional, gerando modelos preditivos consolidados. A segunda é a Unidade Lógica de Análise (*Analytics Logical Function* – AnLF), que atua como o motor de inferência em tempo real. A AnLF consome os modelos treinados pela MTLF e os aplica sobre a telemetria ao vivo da rede para identificar padrões, prever falhas ou detectar anomalias volumétricas instantaneamente.

Confirmada a detecção de um evento de interesse, o ciclo encerra-se com a notificação dos resultados para o plano de controle, fornecendo o embasamento automatizado necessário para que a rede aplique políticas de mitigação ou otimização. Contudo, Chouman et al. (24) alertam que a implantação estritamente centralizada dessa infraestrutura analítica impõe gargalos de latência e de consumo de *backhaul* ao lidar com volumes massivos de tráfego. É precisamente esta limitação inerente aos núcleos tradicionais que motiva a adoção de arquiteturas distribuídas, onde as capacidades de inferência da AnLF são deslocadas da nuvem central para camadas computacionais mais próximas à borda da rede.

2.4 Paradigmas de Processamento: Da Nuvem à Névoa (*Cloud, Edge e Fog Computing*)

A evolução da infraestrutura de processamento distribuído é marcada por transições arquiteturais que buscam equacionar o dilema constante entre capacidade computacional e latência. O paradigma seminal dessa evolução é a Computação em Nuvem (*Cloud Computing*), caracterizada pelo agrupamento centralizado de recursos elásticos e virtualizados, providos sob demanda em *data centers* de hiperescala (15). Embora ofereça capacidade de armazenamento em larga escala, a literatura contemporânea evidencia que o modelo estritamente baseado em nuvem impõe gargalos estruturais graves ao lidar com cenários de alta densidade de conexões. A centralização topológica do processamento introduz um estrangulamento crônico de largura de banda na rede de transporte (*backhaul*) e sobrecarga de sinalização no núcleo da rede, limitações que se contrapõem diretamente aos requisitos

de escalabilidade e suporte a milhões de acessos simultâneos preconizados pelo pilar de Comunicações Massivas do Tipo Máquina (mMTC) das redes 5G (58).

Em antítese à centralização da nuvem, emergiu o paradigma de Computação de Borda (*Edge Computing*). Como definido formalmente por Shi *et al.* (64), este modelo propõe o deslocamento da computação e do armazenamento para as extremidades lógicas da rede, executando tarefas diretamente nos dispositivos terminais ou a um salto de distância (*one-hop*). Contudo, no contexto da Internet das Coisas (IoT) massiva, essa abordagem colide com as severas restrições físicas de *hardware* desses componentes (*resource-constrained nodes*). Dispositivos típicos do ecossistema mMTC, como sensores e atuadores de baixo custo, carecem da densidade computacional, do suprimento energético constante e da memória volátil necessários para instanciar modelos analíticos robustos, tornando a execução local de rotinas avançadas de cibersegurança e detecção de intrusões totalmente impraticável (44).

Para preencher a lacuna semântica e operacional entre a saturação de tráfego na nuvem e a severa restrição de recursos nos nós terminais mMTC, a academia e a indústria consolidaram a Computação em Névoa (*Fog Computing*), conceito cunhado originalmente por Bonomi *et al.* (19). A viabilidade dessa arquitetura foi empiricamente validada por Thomé (67), que demonstrou que a alocação de serviços na camada de Névoa otimiza significativamente o tempo de resposta e a eficiência de processamento em cenários de alta demanda, comparativamente à centralização em nuvem. Essa capacidade de processamento descentralizado constitui um pré-requisito técnico para absorver e mitigar o tráfego massivo e simultâneo que caracteriza o ecossistema 5G-IoT.

Neste contexto, operando de forma intermediária, a névoa estende os serviços da nuvem para a periferia da rede, constituindo-se por nós dotados de recursos substanciais de processamento estrategicamente alocados na infraestrutura de roteamento — notadamente co-localizados com instâncias da Função de Plano de Usuário (UPF) no núcleo 5G (58). A relevância estratégica de posicionar a inteligência analítica mais próxima à origem do tráfego reside na capacidade de detectar anomalias em tempo real. Sob a perspectiva da segurança de redes, a descentralização do processamento transcendeu a otimização de infraestrutura, convertendo-se em um imperativo de segurança diante da sofisticação dos vetores de ataque. Para compreender a urgência de estabelecer uma defesa ágil e descentralizada na camada de Névoa, torna-se necessário escrutinar a dinâmica operacional da ameaça mais devastadora ao cenário mMTC atual, capaz de saturar os links de transporte e colapsar recursos centrais: as *botnets*.

2.5 Botnets e o Cenário de Ameaças: Mirai e Ataques DDoS

As *botnets* (redes zumbis) constituem, contemporaneamente, uma das ameaças críticas à estabilidade das redes de telecomunicações. Sob o ponto de vista arquitetural,

uma *botnet* é uma sobreposição de rede (*overlay network*) formada por milhares — ou até milhões — de nós computacionais previamente comprometidos (45). Estes equipamentos, operando de forma silente e à revelia de seus proprietários originais, são unificados sob o domínio de uma infraestrutura de Comando e Controle (C2). A letalidade dessa estrutura reside na sua capacidade de paralelização: ao sincronizar ações coordenadas, o cibercriminoso (*Botmaster*) converte um aglomerado de dispositivos inofensivos em um vetor de força bruta formidável, capaz de gerar tráfego malicioso em escala global (43).

No ecossistema da Internet das Coisas (IoT), as *botnets* encontraram um vetor de proliferação ideal. A massificação de sensores, câmeras e atuadores desenvolveu-se, historicamente, à margem de práticas rigorosas de segurança (*security by design*), resultando na implantação de *hardwares* com credenciais padronizadas de fábrica e ausência de rotinas de atualização (49). A convergência destas vulnerabilidades intrínsecas com a altíssima disponibilidade de banda e a baixa latência providas pelas redes 5G estabelece um cenário de risco assimétrico. Neste contexto, a infraestrutura de quinta geração atua involuntariamente como um catalisador de danos, viabilizando ataques de magnitude sem precedentes (75).

O paradigma definitivo dessa tipologia de ameaça em ambientes IoT é o *malware* Mirai, que subverteu a lógica tradicional das redes zumbis ao explorar massivamente esses sensores limitados para orquestrar ataques de Negação de Serviço Distribuída (DDoS) capazes de desferir inundações volumétricas devastadoras contra alvos externos, utilizando a infraestrutura de rede como um condúite invisível de alta velocidade (13).

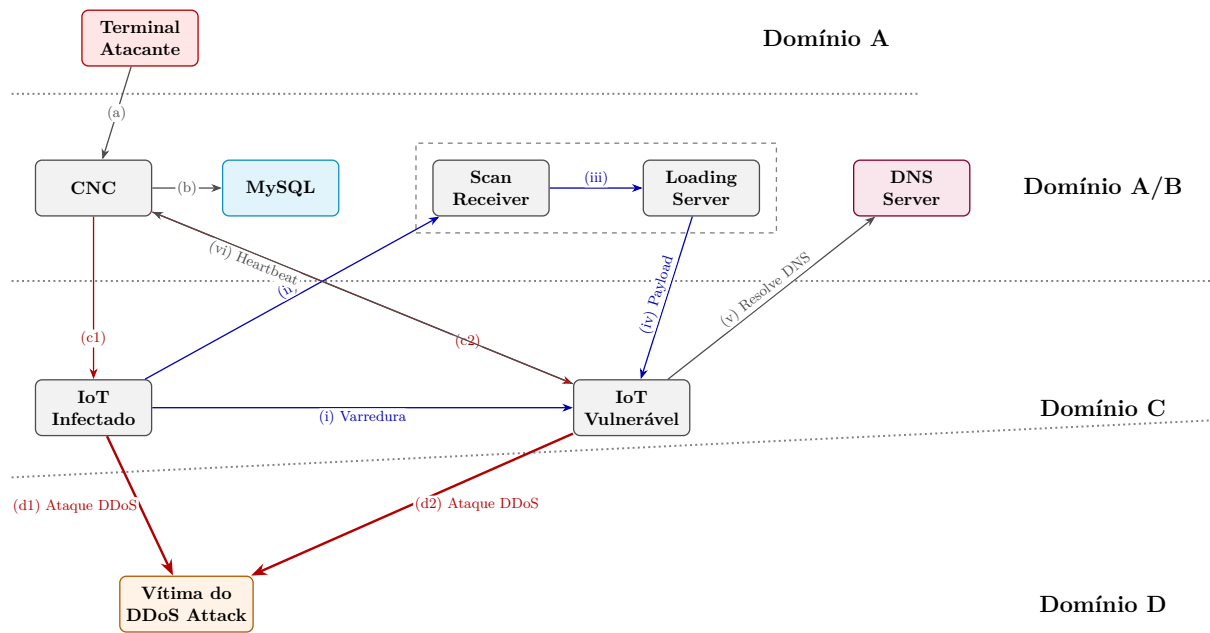
A topologia de propagação e ataque do *malware* Mirai fundamenta-se em um ciclo epidêmico e autônomo, estruturado em domínios operacionais distintos (A, A/B, C e D), conforme ilustra a Figura 6 e delineado por Zhang *et al.* (74). A dinâmica de expansão inicia-se de forma descentralizada no Domínio C (Usuários IoT), onde um dispositivo já infectado realiza varreduras assíncronas (*stateless scanning*) em busca de alvos expostos (i). Ao identificar um IoT vulnerável, o nó infectado reporta o achado ao *Scan Receiver* (ii), que, por sua vez, aciona o *Loading Server* (iii) na infraestrutura do atacante (Domínio A/B). Este servidor de carga é o responsável por injetar o *payload* malicioso no novo dispositivo alvo (iv) (13).

Uma vez concretizada a infecção, o recém-recrutado resolve o endereço da infraestrutura de controle através de consultas ao Servidor DNS (v) e estabelece uma comunicação de registro (*heartbeat*) diretamente com o servidor de Comando e Controle - CNC (vi). A partir deste ancoramento, a rede zumbi passa a operar de forma orquestrada: o atacante (Domínio A) interage com o CNC (a), que consulta as suas bases de dados MySQL (b) e subordina os dispositivos infectados (c1, c2). No estágio final da cadeia, a infraestrutura centralizada emite a ordem de execução, deflagrando rajadas ininterruptas de tráfego de todos os nós controlados (d1, d2) direcionadas à exaustão e negação de serviço da vítima

(Domínio D) (74).

Para maximizar a evasão e o dano estrutural, as variantes modernas do Mirai afastam-se de inundações triviais e empregam técnicas sofisticadas de ofuscação de tráfego. Além de vetores de alta volumetria como o *UDP-Plain*, o *malware* notabiliza-se pela subversão de protocolos de tunelamento legítimos, empregando inundações *GRE-IP* e *GRE-ETH* (13). Ao injetar cargas maliciosas dentro de cabeçalhos *Generic Routing Encapsulation* (GRE), o ataque mascara as assinaturas de transporte originais. Quando essa técnica é transposta para o ecossistema celular, o encapsulamento malicioso do GRE é obrigatoriamente envelopado de forma sobreposta pelo protocolo GTP-U ao ingressar na rede de acesso, gerando uma topologia de rede extremamente complexa caracterizada pelo duplo encapsulamento (GRE embutido em GTP-U).

Figura 6 – Arquitetura de propagação e ataque da *botnet* Mirai.



Fonte: Elaborado pelo autor com base em (74).

Esta sobreposição de cabeçalhos ofuscados impõe um obstáculo sistêmico para os mecanismos de defesa tradicionais. Conforme demonstrado por Sperotto *et al.* (66), sistemas baseados em Inspeção Profunda de Pacotes (DPI - *Deep Packet Inspection*) exigem a análise do conteúdo integral (*payload*) de cada datagrama, o que os torna computacionalmente ineficientes e incapazes de operar em tempo real (*line-rate*) em redes de altíssima velocidade. No atual ecossistema 5G, essa limitação é drasticamente agravada. Como discutido por Khan *et al.* (40), a densidade massiva de conexões e a complexidade introduzida pelos múltiplos encapsulamentos das operadoras exigem abordagens de monitoramento que sejam simultaneamente leves e reativas. O esforço computacional intensivo exigido do DPI para inspecionar iterativamente as camadas de

túneis GRE embutidos no protocolo GTP-U resulta em latência inaceitável para o núcleo, causando o rápido esgotamento dos recursos da própria ferramenta de segurança.

Diante da inviabilidade técnica da inspeção profunda contra inundações massivas e ofuscadas, a literatura consolida a adoção de defesas proativas fundamentadas na extração estatística de metadados de fluxos (*flow-based analysis*) (66). Ao focar na avaliação de atributos comportamentais — como variações de tamanho de pacote, duração de conexão e taxas de pacotes por segundo — logo após a terminação do túnel GTP-U, essa abordagem elimina a necessidade de descriptografar ou inspecionar o *payload*. Consequentemente, viabiliza-se a detecção em alta velocidade de anomalias volumétricas por meio de algoritmos avançados de Aprendizado de Máquina, integrando uma camada de segurança robusta que respeita rigorosamente as restrições de latência do 5G (40).

2.6 Aprendizado de Máquina e Avaliação de Desempenho

Para que a análise baseada em fluxos se converta em uma defesa efetiva, a rede necessita de um motor capaz de interpretar essas características comportamentais de forma rápida e autônoma. É para preencher essa lacuna analítica que o Aprendizado de Máquina (ML - *Machine Learning*) consolida-se como a ferramenta ideal. Sendo um ramo fundamental da Inteligência Artificial focado no desenvolvimento de algoritmos estatísticos, o ML capacita os sistemas computacionais a extraírem padrões complexos a partir de grandes volumes de dados, permitindo a generalização do conhecimento para amostras inéditas e a execução de tarefas sem a necessidade de programação explícita por regras estáticas (11).

No contexto das redes celulares de próxima geração e da mitigação de ameaças volumétricas como o Mirai, os modelos de ML assumem o papel de motores decisórios em Sistemas de Detecção de Intrusões (IDS) (61). Ao processar os metadados estatísticos extraídos na UPF, essas ferramentas conseguem distinguir matematicamente o tráfego legítimo das anomalias maliciosas. Para fundamentar a metodologia operacional proposta nesta dissertação, faz-se necessário definir a terminologia do ciclo de vida desses modelos e as métricas rigorosas empregadas na sua validação.

2.6.1 Ciclo de Vida do Modelo

A operacionalização de um modelo de Aprendizado de Máquina em ambientes de cibersegurança segue um ciclo de vida estruturado, essencialmente composto por quatro estágios interdependentes: experimentação, treinamento, teste e inferência. A delimitação destas fases é imperativa para assegurar a robustez metodológica e a estabilidade na implantação de sistemas de defesa (61).

A fase de experimentação consiste na exploração arquitetural, onde diferentes algoritmos e hiperparâmetros são avaliados para determinar a abordagem com maior

aderência à natureza estocástica do problema. Em cenários de detecção baseada em fluxos de rede, esta etapa frequentemente prioriza algoritmos de aprendizado por conjunto baseados em árvores de decisão — como o *Random Forest* (21, 17) e o *LightGBM* (39, 38) —, buscando o ponto ótimo entre o custo computacional exigido e a capacidade preditiva (23).

Subsequentemente, na fase de treinamento supervisionado, o algoritmo selecionado é alimentado com um conjunto de dados (*dataset*) previamente rotulado. Durante este processamento iterativo, o modelo ajusta os seus limiares internos para mapear as correlações intrínsecas entre os atributos de rede (*features*) e os seus respectivos rótulos (tráfego normal ou ataque *DDoS*). A representatividade estatística e a integridade geométrica deste conjunto de treinamento são determinantes absolutos para a resiliência do modelo final (11).

Após o treinamento, o algoritmo é submetido à fase de testes, cujo propósito é mensurar a sua capacidade de generalização. O modelo é exposto a um subconjunto de dados inéditos, e as suas predições automatizadas são confrontadas com os rótulos reais (*ground truth*). Esta validação empírica quantifica a confiabilidade do sistema e fornece os indicadores necessários para eventuais ajustes de hiperparâmetros. Por fim, ao atingir os limiares de desempenho estipulados, o modelo transita para a fase de inferência. Neste estágio de produção, o sistema é efetivamente implantado na infraestrutura operacional da rede, passando a classificar o tráfego contínuo e a fornecer os insumos analíticos necessários para a mitigação de ameaças.

2.6.2 Métricas de Desempenho

A avaliação rigorosa de um classificador binário em cibersegurança repousa sobre os axiomas da matriz de confusão, que categoriza o comportamento preditivo em quatro dimensões fundamentais (28). Considera-se Verdadeiro Positivo (VP) a correta identificação de uma amostra pertencente à classe alvo (neste escopo, um fluxo anômalo ou ataque); Verdadeiro Negativo (VN) denota a predição exata de uma amostra da classe de fundo (tráfego benigno humano ou máquina). Em contrapartida, as falhas classificatórias dividem-se em Falso Positivo (FP), quando um fluxo benigno é erroneamente penalizado como ameaça (gerando um alarme falso estrutural), e Falso Negativo (FN), cenário crítico no qual um vetor de ataque real passa despercebido pelos crivos de detecção.

Com base nestes fundamentos, derivam-se as métricas estatísticas de desempenho, garantindo uma interpretação padronizada da eficácia de mitigação do IDS (59).

A Exatidão (*Accuracy*) representa a proporção global de predições corretas em relação à totalidade de amostras analisadas. Embora ofereça uma perspectiva macroscópica, trata-se de uma métrica frequentemente ilusória em ambientes de rede altamente desbalanceados, onde o tráfego benigno suplanta o tráfego malicioso em ordens de grandeza.

Sua formulação matemática é expressa por:

$$Accuracy = \frac{VP + VN}{VP + VN + FP + FN} \quad (2.1)$$

Para focalizar o rigor na classe de interesse, aplica-se a Precisão (*Precision*). Esta métrica quantifica a confiabilidade intrínseca dos alertas gerados pelo sistema de defesa, definindo a razão entre os ataques verdadeiramente identificados e a soma de todos os fluxos classificados pelo modelo como ameaça. Um alto índice de precisão assegura que ações de bloqueio não prejudicarão usuários legítimos. É calculada pela equação:

$$Precision = \frac{VP}{VP + FP} \quad (2.2)$$

De maneira complementar, a Revocação (*Recall* ou Sensibilidade) mensura a exaustividade do modelo em detectar os eventos maliciosos efetivamente presentes no ecossistema de rede. Ela estabelece a proporção de ataques reais que foram corretamente interceptados, evidenciando a blindagem do sistema contra ameaças furtivas (falsos negativos). Sua definição é obtida mediante a relação:

$$Recall = \frac{VP}{VP + FN} \quad (2.3)$$

Diante da natural relação de compromisso (*trade-off*) existente entre Precisão e Revocação, o *F1-Score* impõe-se como o avaliador definitivo da coesão estatística do modelo (59). Formulado como a média harmônica entre estas duas grandezas, o *F1-Score* converge para o seu valor ótimo de 1 exclusivamente quando o classificador demonstra excelência balanceada em ambas as frentes, penalizando de forma severa discrepâncias acentuadas entre alarmes falsos e evasões. A métrica é consolidada pela equação:

$$F1 = 2 \times \frac{Precision \times Recall}{Precision + Recall} \quad (2.4)$$

2.7 Considerações Finais do Capítulo

Este capítulo consolidou o alicerce teórico fundamental para a compreensão da problemática e da solução investigadas nesta dissertação. Inicialmente, delineou-se a evolução arquitetural das redes móveis, contrastando a rigidez do núcleo monolítico do 4G (EPC) com a flexibilidade orientada a serviços da infraestrutura 5G (SBA). Em paralelo, discutiu-se a transição dos paradigmas de processamento, evidenciando como a Computação em Névoa (*Fog Computing*) resolve o dilema entre a alta latência da nuvem e as restrições de *hardware* da borda.

Sob a ótica da cibersegurança, o texto desconstruiu o cenário atual de ameaças, demonstrando como as vulnerabilidades intrínsecas da Internet das Coisas (IoT) são exploradas para a orquestração de *botnets* epidêmicas, como o Mirai. Restou evidenciado

que a sobreposição de túneis ofuscados (duplo encapsulamento) inviabiliza os sistemas tradicionais de Inspeção Profunda de Pacotes (DPI) nos núcleos celulares modernos. Diante dessa limitação arquitetural, o capítulo estabeleceu os preceitos do Aprendizado de Máquina (*Machine Learning*) como a alternativa viável, formalizando o ciclo de vida dos modelos estatísticos — destacando a aplicabilidade de algoritmos baseados em árvores de decisão, a exemplo do *Random Forest* e *LightGBM* — além das métricas matemáticas essenciais para a avaliação rigorosa de Sistemas de Detecção de Intrusões (IDS) baseados em fluxos.

Este arcabouço conceitual provê o contexto técnico indispensável para as etapas subsequentes do trabalho: a análise crítica do estado da arte e dos trabalhos correlatos (Capítulo 3), a fundamentação da arquitetura e da metodologia experimental propostas (Capítulo 4) e, por fim, a apresentação e discussão dos resultados obtidos (Capítulo 5).

3 Trabalhos Relacionados

Este capítulo fornece uma visão geral da revisão da literatura conduzida antes da fase experimental desta pesquisa. A Seção 3.1 define a revisão da literatura e delineia a metodologia empregada durante o processo de busca. Os achados da revisão sistemática foram utilizados para selecionar os trabalhos mais relevantes, os quais são discutidos detalhadamente na Seção 3.2. Os principais pontos dos trabalhos revisados são sumarizados e criticamente comparados na Seção 3.3, onde também é apresentado o posicionamento da solução proposta frente às lacunas identificadas.

3.1 Revisão Sistemática da Literatura

Uma Revisão Sistemática da Literatura (RSL) é um método estruturado, transparente e replicável de coletar, avaliar criticamente, integrar e apresentar descobertas de múltiplos estudos sobre uma questão de pesquisa ou tópico de interesse. Considerando essa definição, uma revisão abrangente acerca da segurança em redes 5G e detecção de intrusões foi conduzida. Importante ressaltar que este procedimento foi projetado não como um estudo secundário exaustivo, mas como um mapeamento de literatura (*literature mapping*) direcionado a estabelecer uma base teórica sólida para esta dissertação. A abordagem foi rigorosamente estruturada para ser reproduzível, facilitando sua utilidade para pesquisadores interessados em conduzir investigações similares.

A seleção das bases de dados é essencial para o processo de revisão, uma vez que a escolha de um número limitado de fontes restringe a diversidade metodológica da literatura explorada. Seguindo os três estágios clássicos de uma revisão — Entrada (*Input*), Processamento (*Processing*) e Saída (*Output*) —, os primeiros passos consistiram na identificação das bases de dados primárias e na determinação de uma *string* de busca aderente ao escopo do problema.

Para os fins deste estudo, as bases de dados selecionadas compreenderam repositórios científicos de alto impacto: *Scopus*, *Web of Science (WoS)*, *Crossref*, *Google Scholar*, *Semantic Scholar*, *SpringerLink*, *ScienceDirect* e *IEEE Xplore*. As bases foram consultadas através de mecanismos de busca avançada e acesso com assinatura institucional provida pela universidade, garantindo o alcance à literatura científica qualificada e revisada por pares.

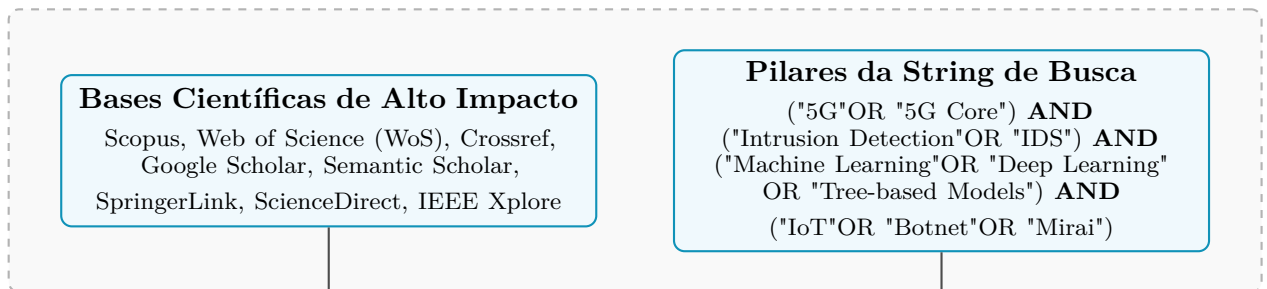
Para assegurar a precisão da literatura mapeada e o seu alinhamento com a Arquitetura Baseada em Serviços (*Service-Based Architecture - SBA*), a *string* de busca foi construída combinando os pilares tecnológicos fundamentais desta pesquisa. A consulta utilizou operadores booleanos aplicados a palavras-chave relacionadas a sistemas móveis de quinta geração ("*5G*" OR "*5G Core*"), segurança de redes ("*Intrusion Detection*" OR "*IDS*"), técnicas analíticas avançadas ("*Machine Learning*" OR "*Deep Learning*" OR "*Tree-based*

Models") e o cenário de ameaças direcionadas (*"IoT"* OR *"Botnet"* OR *"Mirai"*).

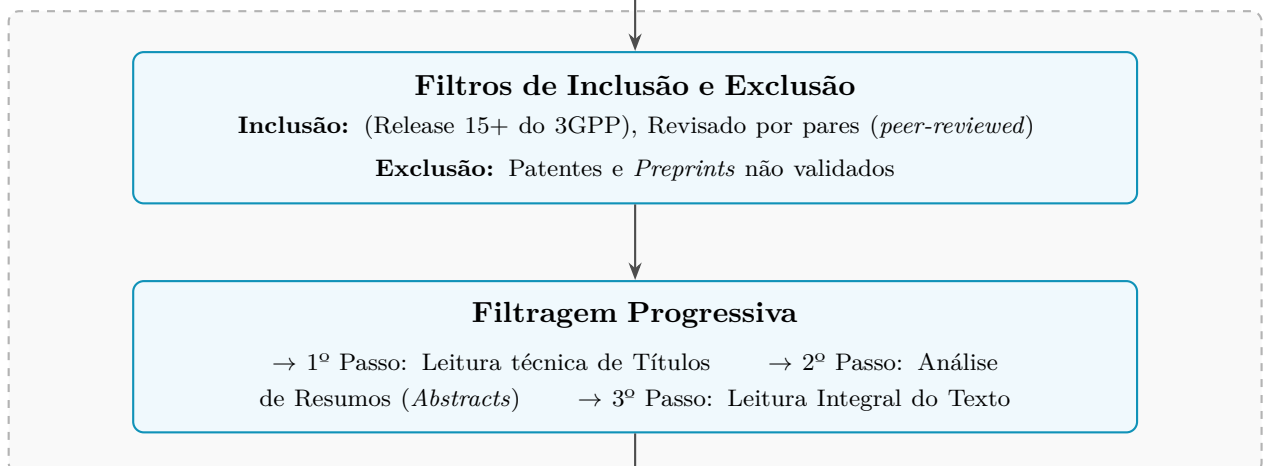
Filtros adicionais de inclusão e exclusão foram aplicados para restringir os resultados a publicações a partir do ano de 2019. Este recorte temporal foi estrategicamente escolhido para refletir a maturidade tecnológica dos *Releases* recentes do 3GPP (Release 15 em diante) (1). Adicionalmente, excluíram-se patentes, preprints não validados e citações não submetidas ao crivo cego por pares (*peer-reviewed*). Os resultados obtidos em cada base foram exportados de forma estruturada, permitindo a filtragem progressiva baseada na leitura técnica de títulos, resumos (*abstracts*) e, no estágio final, leitura integral do texto para compor o portfólio definitivo das obras correlatas.

Figura 7 – Fluxograma da Revisão Sistemática da Literatura (RSL).

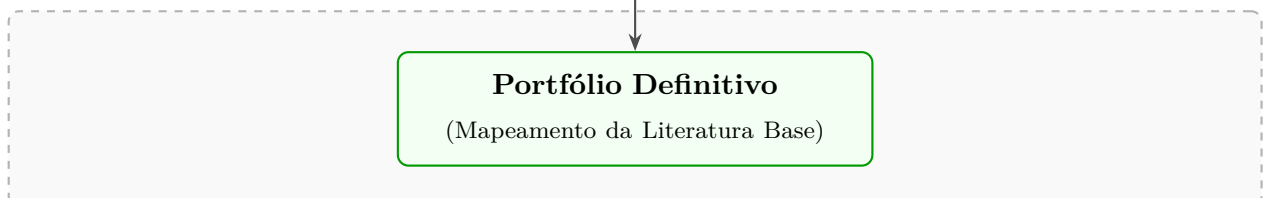
Fase 1: Entrada (*Input*)



Fase 2: Processamento (*Processing*)



Fase 3: Saída (*Output*)



Fonte: Elaborado pelo autor.

3.2 Análise dos Trabalhos Relacionados

A vulnerabilidade intrínseca dos dispositivos IoT, frequentemente desprovidos de mecanismos robustos de autenticação e atualização de *firmware*, tem impulsionado a rápida disseminação de malwares e a formação de botnets de grande escala, a exemplo das variantes da Mirai (43, 13). Para conter essas ameaças, a implementação de Sistemas de Detecção de Intrusões (IDS) baseados em Inteligência Artificial tornou-se o padrão fundamental de defesa (23). Historicamente, diversos estudos fundamentaram o uso de arquiteturas profundas (*Deep Learning*) e modelos tradicionais de aprendizado de máquina para extrair padrões estatísticos e comportamentais de pacotes IoT contaminados (45).

Embora a literatura recente apresente avanços significativos na detecção dessas intrusões — abrangendo desde redes neurais profundas centralizadas até soluções de computação em névoa (*Fog Computing*) —, a integração nativa dessas abordagens à arquitetura 5G permanece um desafio em aberto. As soluções existentes frequentemente negligenciam a complexidade do tráfego celular tunelado (GTP-U) e a dinâmica das funções de rede virtualizadas. Consequentemente, surge uma lacuna arquitetural estrutural na qual modelos de alta precisão algorítmica falham ao serem submetidos ao volume massivo de requisições e inundações volumétricas características do ecossistema mMTC, exigindo uma reengenharia sistêmica dos mecanismos de detecção para evitar a saturação dos recursos da rede.

O principal desafio na transposição destas soluções para o núcleo móvel reside no paradigma de inspeção em nível de pacote, amplamente adotado na literatura, mas cujo custo computacional é incompatível com as taxas de transmissão do 5G (*line-rate*). No escopo das abordagens distribuídas, o sistema D²IOT, proposto por Nguyen *et al.* (2019) (35), buscou mitigar este custo introduzindo uma arquitetura de Aprendizado Federado (*Federated Learning*) para redes domésticas (SOHO). Utilizando redes neurais GRU (*Gated Recurrent Unit*), o modelo mapeia características individuais de pacotes (como *flags* TCP e tempo entre chegadas) para símbolos de estado. Apesar da excelente taxa de detecção reportada (95,6%), a carga iterativa gerou um atraso preditivo de 0,592 ms por pacote em CPU padrão (35). Frente aos milhões de pacotes por segundo roteados pela Função de Plano de Usuário (UPF), esse acúmulo temporal torna a solução impraticável para o 5G Core.

Aprofundando a complexidade de extração focada na inspeção individual de pacotes brutos, Almiani e Aldhyani (2021) (10) propuseram um modelo híbrido estruturado sobre redes neurais convolucionais e recorrentes (CNN-LSTM). Embora a solução tenha alcançado 90,88% de acurácia em Redes Locais (LAN) tradicionais, a sua fundação metodológica assenta-se na Inspeção Profunda de Pacotes (DPI) para a extração de assinaturas espaciais do *payload*. No contexto do núcleo 5G contemporâneo, a abordagem DPI apresenta uma dupla inviabilidade arquitetural. Primeiro, a adoção massiva de tráfego criptografado

de ponta a ponta (como o TLS 1.3) cega a inspeção de *payloads*, tornando o modelo ineficaz contra ataques modernos. Segundo, a reconstrução de estado exigida pela técnica DPI, somada à natureza estritamente sequencial da inferência nas portas da rede LSTM, exacerba o gargalo temporal evidenciado anteriormente no sistema DIOT, retardando ainda mais o tempo de processamento.

Na tentativa de contornar esse atraso preditivo imposto pelo processamento em *software*, abordagens disruptivas recentes, como a de Paolini *et al.* (2024) (55), exploraram a aceleração via *hardware*. Os autores propuseram a conversão estrutural de *bytes* de rede em matrizes bidimensionais de imagem, classificando os pacotes através de CNNs de Visão Computacional. Para sustentar a operação em tempo real, foram forçados a ancorar a inferência em aceleradores de *hardware* dedicados, especificamente matrizes de portas programáveis (FPGAs). Embora tecnicamente funcional, essa dependência de *hardware* exótico fere frontalmente os princípios de virtualização de funções de rede (NFV) e elasticidade da Arquitetura Baseada em Serviços (SBA). A necessidade de acoplar FPGAs a cada nó da UPF onera drasticamente os custos operacionais de implantação, inviabilizando a descentralização do IDS numa arquitetura de Névoa distribuída.

Buscando otimizar a extração computacional sem o uso de aceleradores, Yang *et al.* (2025) (72) propuseram o *Hybrid-NNIDS*. A arquitetura utiliza a eficiência do algoritmo *LightGBM* para filtragem inicial em nível de fluxo e aplica redes *MobileNetV2* para classificação fina de pacotes, alcançando 94,0% de acurácia na borda. Contudo, a proposta esbarra em lacunas fundamentais: a *MobileNetV2* ainda exige carga matricial convolucional significativamente superior a modelos puros de árvores de decisão. Mais crítico ainda, o estudo abstrai completamente a infraestrutura celular. A ausência de suporte nativo ao tráfego tunelado (GTP-U) e a falta de integração com protocolos de controle (PFCP) impedem que as inferências do modelo sejam convertidas em regras ativas no núcleo móvel. Na mesma linha de modelos leves, Awotunde *et al.* (2023) (17) integraram *Random Forest* e lógica *Fuzzy*. Contudo, a validação repousou sobre o *dataset* defasado NSL-KDD, falhando em refletir ameaças IoT contemporâneas e ignorando as complexidades de encapsulamento móvel.

O impacto real da ofuscação pelo encapsulamento celular foi empiricamente demonstrado por Kim *et al.* (2022) (41). Ao avaliarem classificadores de ML operando diretamente sobre pacotes extraídos da UPF (Interface N3), os autores constataram que a precisão da detecção sofreu uma degradação severa, caindo aproximadamente 23%. Este decréscimo é justificado pelo ruído estatístico introduzido pelos cabeçalhos da operadora e pelo Identificador de Ponto Final de Túnel (TEID), que mascaram o comportamento da botnet.

Para mitigar tais perdas e trazer a inteligência de volta ao núcleo, o 3GPP padronizou a função NWDAF. Trabalhos como os de Sevician *et al.* (2020) (62) e Manias *et*

al. (2022) (47) exploraram a sua implementação. Enquanto Manias *et al.* demonstraram um protótipo focado na análise de sinalização do Plano de Controle para balanceamento de carga, Sevgican *et al.* propuseram redes LSTM centralizadas para previsão de tráfego. Contudo, ambas operam de forma puramente centralizada e ignoram a inspeção direta de ameaças no Plano de Usuário, onde ataques volumétricos da Mirai podem ocorrer.

3.3 Síntese Comparativa e Posicionamento do Trabalho

A avaliação crítica do estado da arte evidencia que, embora a detecção de intrusões atinja elevados índices teóricos de acerto no cenário genérico IoT, a transposição dessas metodologias para a arquitetura 5G esbarra em algumas deficiências. Modelos baseados em aprendizado profundo introduzem latências sequenciais ou exigem hardware exótico (10, 55); soluções leves abstraem o núcleo celular (72, 17); a inspeção em interfaces de ingresso sofre com ruídos do GTP-U (41); e arquiteturas NWDAF existentes mantêm-se restritas ao controle centralizado (47). A Tabela 2 consolida as abordagens contrastando-as com a proposta desta dissertação.

Tabela 2 – Síntese comparativa dos trabalhos relacionados sob a ótica dos requisitos operacionais 5G.

Trabalho	Abordagem	Ambiente	Lacunas Identificadas
Almiani <i>et al.</i> (10)	DPI (CNN + LSTM)	LAN (Cab.)	Processamento sequencial intolerável para <i>line-rate</i> ; viola a privacidade.
Paolini <i>et al.</i> (55)	Imagens (CNN)	Line-rate	Elevado custo computacional; exige hardware acelerador exótico (FPGA).
Yang <i>et al.</i> (72)	Híbrido (LGBM+CNN)	Edge (IoT)	Abstrai o núcleo 5G; ignora túneis GTP-U e a arquitetura SBA.
Awotunde <i>et al.</i> (17)	Múltiplos Níveis (RF)	Teórico	Validação em <i>dataset</i> defasado; ignora o tráfego tunelado celular.
Kim <i>et al.</i> (41)	Baseado em Fluxo (ML)	5GC (N3)	Degradação de 23% na acurácia devido à leitura de pacotes sujos (GTP-U).
Manias <i>et al.</i> (47)	Nativa SBA (Clustering)	NWDAF	Foco exclusivo na sinalização do Plano de Controle; abstrai o Plano de Usuário.
Este trabalho	Fluxo (RF/LGBM)	Leve Névoa (N6)	Integra AnLF distribuída; imune ao ruído GTP-U.

Fonte: Elaborado pelo autor.

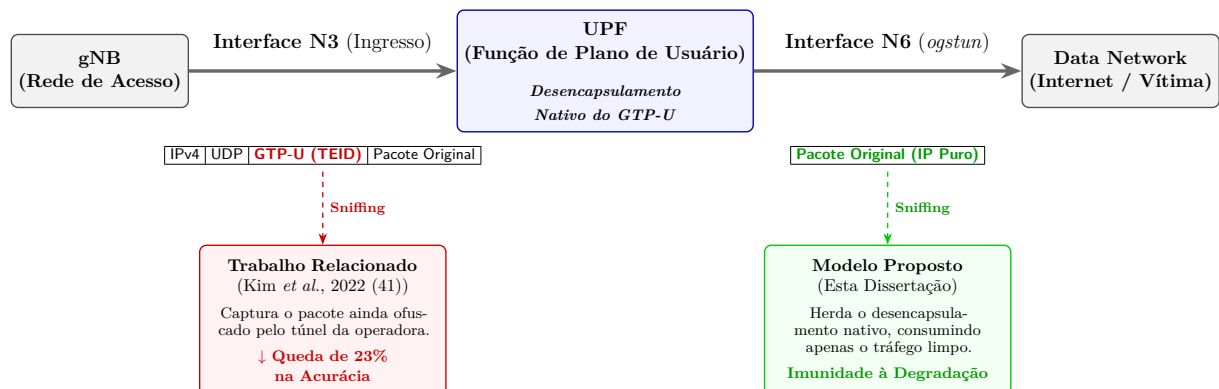
A proposição desta dissertação diferencia-se substancialmente do estado da arte por

não avaliar o contexto sob a métrica de acurácia algorítmica de forma isolada, mas sim sob a viabilidade holística de implantação em infraestruturas móveis em produção. Diferente das abordagens que oneram a rede com arquiteturas convolucionais profundas (10, 55, 35), esta solução opta pela extração ultraleve de apenas 11 características estatísticas de fluxo. Ao associar estes metadados a modelos baseados em particionamento lógico condicional (*Random Forest* e *LightGBM*), a arquitetura exige frações diminutas do custo matemático da literatura, garantindo a agilidade e a escalabilidade necessárias para processar inundações volumétricas sem saturar a borda/névoa no ecossistema mMTC.

Como evidenciado na Tabela 2, o referencial teórico primário que fundamenta o problema de pesquisa desta dissertação é o trabalho de Kim *et al.* (2022) (41). Frente a esse estudo, a presente arquitetura não apenas preenche a lacuna deixada pelos autores como trabalho futuro, mas supera arquitetural e numericamente a solução *baseline* em três frentes metodológicas fundamentais.

Primeiramente, no que tange à imunidade à degradação analítica, o trabalho de Kim *et al.* fracassa em manter a alta precisão no núcleo 5G porque a captura de pacotes foi realizada na interface de ingresso da UPF (Interface N3). Nesse ponto topológico, o tráfego encontra-se obrigatoriamente encapsulado no túnel celular, forçando o motor de Inteligência Artificial a processar ruídos da operadora, como o TEID, o que resultou numa queda reportada de 23% na acurácia da detecção. Em contrapartida, o modelo aqui proposto supera esta barreira ao deslocar o ponto de extração estrategicamente para a interface de saída N6 (representada pela *ogstun*). Ao adotar este posicionamento, o sistema herda o desencapsulamento executado nativamente pelo *hardware* da UPF, recebendo tráfego IP puro e blindando o classificador estatístico contra a degradação sofrida pela literatura.

Figura 8 – Comparativo topológico de extração de tráfego na UPF: Abordagem da literatura *vs* Modelo Proposto.



Fonte: Elaborado pelo autor.

Por fim, destaca-se a materialização de uma arquitetura descentralizada diretamente

na camada de Névoa (*Fog Computing*), inspirada nos preceitos lógicos da função NWDAF. Enquanto Kim *et al.* limitaram-se à análise estática em tempo diferido (*offline*), sugerindo a integração ao padrão 3GPP apenas como uma hipótese teórica, esta pesquisa concretiza essa abordagem de forma otimizada e funcional. Fugindo do paradigma de um núcleo analítico centralizado e de alta latência, a Função Lógica de Análise (AnLF) foi estruturada como um microsserviço descentralizado — orquestrado via API Flask e monitorado continuamente pelo InfluxDB — instanciado em um nó de Névoa adjacente à interface N6. Esta descentralização assegura não apenas a manutenção da precisão algorítmica imune ao encapsulamento, mas também a velocidade de inferência (escala de microssegundos) necessária para mitigar inundações volumétricas da *botnet* Mirai em tempo real

Em suma, enquanto a literatura existente tenta forçar algoritmos de Aprendizado de Máquina a adaptarem-se à complexidade de um túnel celular hostil, a arquitetura proposta manipula a topologia nativa do 5G e a formatação de pacotes para entregar à Inteligência Artificial um ambiente de rede perfeitamente limpo, possibilitando agilidade e superioridade analítica.

3.4 Síntese do Capítulo

A revisão da literatura apresentada neste capítulo evidenciou que, embora a aplicação de Inteligência Artificial para a detecção de intrusões em ambientes IoT seja um campo de pesquisa vasto e ativo, a sua integração nativa à infraestrutura celular 5G ainda carece de maturidade operacional. As abordagens prevalentes no estado da arte frequentemente falham ao transpor os seus modelos para o núcleo móvel, seja por adotarem técnicas de inspeção profunda (DPI) incompatíveis com as restrições de latência do tráfego *line-rate*, seja por ignorarem a ofuscação estrutural imposta pelo protocolo de tunelamento GTP-U.

Ao mapear rigorosamente estas lacunas, o posicionamento desta dissertação consolida-se em torno de uma arquitetura defensiva pragmática e estritamente alinhada às padronizações do 3GPP. A proposta afasta-se da complexidade computacional das redes neurais profundas e da dependência de aceleradores de *hardware* exóticos, priorizando a extração de metadados estatísticos ultraleves aliados à eficiência de algoritmos baseados em árvores de decisão (*LightGBM* e *Random Forest*). Ademais, a inovação topológica de instanciar a Função Analítica Lógica (AnLF) do NWDAF de forma descentralizada na camada de Névoa, especificamente na interface N6 (pós-UPF), resolve estruturalmente o problema de degradação da acurácia reportado na literatura recente.

Com o referencial teórico consolidado e as deficiências do estado da arte devidamente endereçadas pelo posicionamento arquitetural proposto, o capítulo 4 detalhará a metodologia de implementação deste *framework*. Serão abordados a construção da topologia do *testbed* 5G, o motor estocástico de injeção de tráfego, o *pipeline* de extração

de características e a calibração dos modelos preditivos.

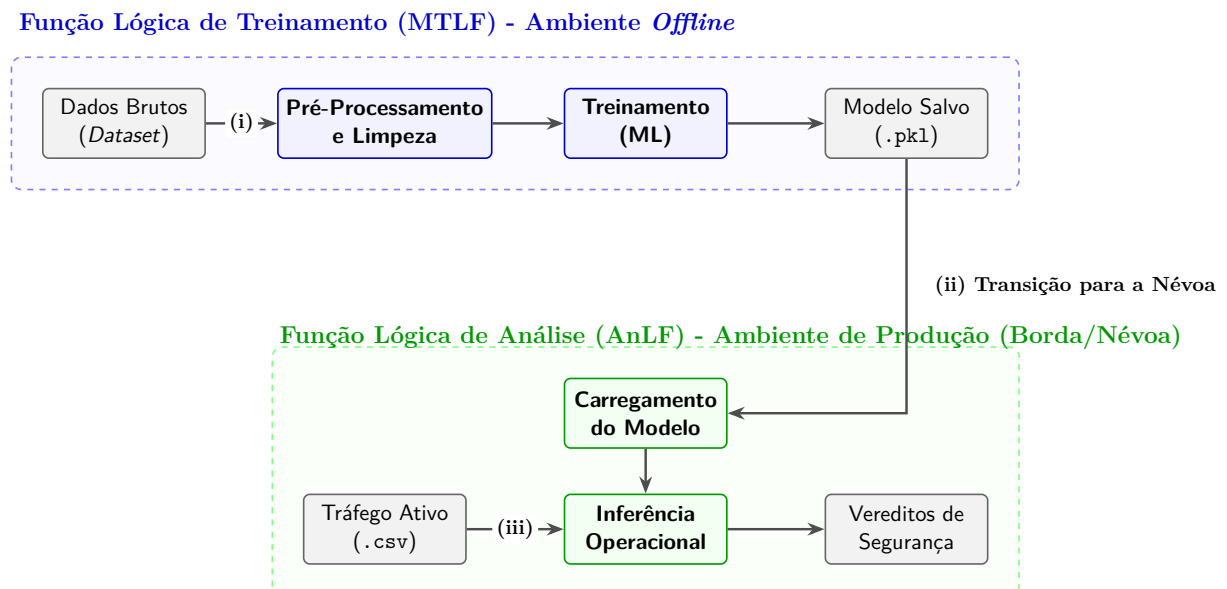
4 Metodologia

A metodologia delineada neste capítulo caracteriza-se como pesquisa experimental e quantitativa, estruturada para garantir a reprodutibilidade técnica e a validação científica do modelo de segurança proposto (18, 11). O capítulo está organizado em componentes lógicos sucessivos: a Seção 4.1 apresenta o *pipeline* de Aprendizado de Máquina alinhado à arquitetura NWDAF do 3GPP. A Seção 4.2 detalha a topologia do ambiente de simulação 5G e os mecanismos de emulação de tráfego. A base de dados primária é introduzida na Seção 4.3, seguida pela implementação técnica, preparação de dados e otimização dos classificadores detalhados na Seção 4.4.

4.1 Pipeline de Aprendizado de Máquina e Arquitetura NWDAF

Em conformidade com as especificações do 3GPP para análise de dados no núcleo 5G (3), o sistema de detecção de intrusões foi desenhado sob os preceitos da Função de Análise de Dados da Rede (NWDAF - *Network Data Analytics Function*). Adotando uma arquitetura Borda-Névoa-Nuvem (*Edge-Fog-Cloud*), este duto computacional (*pipeline*) garante a transição fluida entre a concepção do algoritmo e a sua execução em tempo real, conforme ilustrado na Figura 9.

Figura 9 – Diagrama de blocos do *pipeline* de Aprendizado de Máquina baseado na NWDAF.



Fonte: Elaborado pelo autor.

O fluxo metodológico tem início com a ingestão dos dados brutos (i). Esta etapa alimenta a Função Lógica de Treinamento de Modelo (MTLF - *Model Training Logical Function*), responsável pelo Pré-Processamento e Treinamento *offline*. Nesta fase, o tráfego

de rede passa por rotinas de limpeza, normalização de escalas e seleção de atributos (*features*). Em seguida, os modelos supervisionados selecionados mapeiam as correlações intrínsecas dos dados para distinguir fluxos benignos de inundações maliciosas. Ao término do ajuste e da validação cruzada, o classificador otimizado é exportado fisicamente na forma de um binário encapsulado (*.pk1*).

A transição para o ambiente de produção na camada de Névoa é representada pelo indicador (ii). O classificador treinado assume o papel da Função Lógica de Análise (AnLF - *Analytics Logical Function*), conforme a separação funcional prevista para a NWDAF (3, 42). Paralelamente, o tráfego celular ativo, capturado na Borda e estruturado no formato *.csv*, é injetado no sistema. A convergência entre o algoritmo instanciado e os dados inéditos (iii) resulta na execução operacional do modelo. É neste vértice final que a AnLF atua de forma autônoma, emitindo os vereditos de segurança em frações de milissegundo para resguardar a infraestrutura 5G.

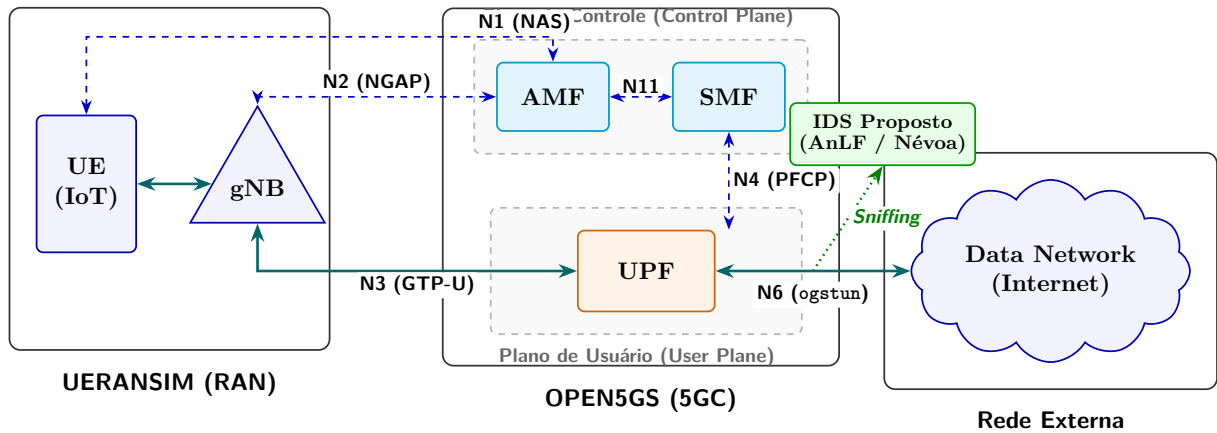
4.2 Ambiente de Simulação 5G e Emulação de Tráfego

Fundamentado no fato de que ambientes emulados facilitam o controle rigoroso de variáveis em redes 5G (54, 32), projetou-se a topologia experimental ilustrada na Figura 10. A arquitetura reproduz em escala de laboratório o enlace de saída de uma infraestrutura celular (como um nó de roteamento de um *Smart Campus* com dispositivos heterogêneos), compreendendo uma Rede de Acesso de Rádio (RAN) emulada — englobando Equipamentos de Usuário (UE) e a estação rádio-base (gNB) — por meio do *software* UERANSIM (32). Esta rede de acesso conecta-se diretamente a um Núcleo 5G (5GC) funcional instanciado pelo Open5GS (54), mimetizando com precisão a convergência do tráfego de transporte desde a origem nos dispositivos IoT até o seu desaguadouro na interface N6 rumo à rede externa (Internet).

Para a implementação do núcleo móvel (5GC), adotou-se o *Open5GS* (54). Desenvolvida em linguagem C e aderente às especificações do *Release 16* do 3GPP, esta plataforma implementa nativamente a Arquitetura Baseada em Serviços (SBA) e a Separação entre Plano de Controle e Plano de Usuário (CUPS). A adoção do Open5GS permitiu a instanciação de todas as Funções de Rede (NFs) vitais para o roteamento da IoT, com destaque para a AMF (Gerenciamento de Acesso), SMF (Gerenciamento de Sessão) e, sobretudo, a UPF (Função de Plano de Usuário), responsável pelo desencapsulamento do tráfego na camada de Névoa. Visando garantir o isolamento do tráfego anômalo e refletir a implantação comercial, o núcleo foi configurado com um fatiamento de rede (*Network Slicing*) cujo identificador NSSAI foi ajustado para o Tipo de Serviço SST=3, padrão do 3GPP para Comunicações Massivas do Tipo Máquina (mMTC).

O domínio da Rede de Acesso (RAN) foi instanciado pelo simulador *UERANSIM* (32). Distinguindo-se de ferramentas triviais de repetição de pacotes, o UERANSIM atua

Figura 10 – Arquitetura do ambiente experimental: Integração UERANSIM, Open5GS (com separação CUPS entre Plano de Controle e Plano de Usuário) e Internet.



Fonte: Elaborado pelo autor.

como um emulador completo do plano de controle de rádio (RRC) e do estrato de não-acesso (NAS). Ele introduz Equipamentos de Usuário (UEs) virtuais com identificadores IMSI autênticos e estabelece o *Next Generation NodeB* (gNB). O aspecto técnico mais crítico dessa escolha é a criação da interface de rede virtual TUN no sistema operacional do cliente (e.g., `uesimtun0`). Qualquer tráfego injetado nesta interface pelo gerador é compulsoriamente criptografado e encapsulado nos túneis GTP-U pelo gNB antes de ser transmitido à UPF via Interface N3, reproduzindo com exatidão o encapsulamento enfrentado pelas operadoras.

O ambiente incorpora um mecanismo customizado de geração de tráfego que transita sobre estas interfaces virtuais. O *script* injetor é responsável por emular tanto o comportamento esparsa da telemetria legítima IoT quanto a microcadência das inundações do *malware Mirai* (incluindo as complexas variantes encapsuladas *GRE-IP*, *GRE-ETH* e *UDP-Plain*).

Para viabilizar a extração dos metadados e alimentar a Função Lógica de Análise (AnLF) sem penalizar os recursos do núcleo ou da rede de acesso, o IDS foi posicionado para operar na modalidade *sniffing* passivo. Descartou-se a inspeção direta na estação rádio-base (gNB) para não onerar o processamento crítico de radiofrequência e mobilidade, bem como na interface N3 devido à ofuscação do túnel. Assim, a captura contínua (*Packet Capture* - PCAP) ocorre estritamente na interface *ogstun* do Open5GS. Esta interface representa fisicamente o Ponto de Referência N6, local exato onde o tráfego de transporte agregado emerge limpo do túnel GTP-U para ser roteado rumo à rede de dados externa, tornando-se o ponto focal ideal para a inspeção estatística em camada de Névoa proposta por este trabalho.

A reprodução de ameaças em redes 5G exige que a injeção de dados transcenda a

simples saturação volumétrica de banda. Ferramentas tradicionais de injeção de pacotes (como *iPerf* ou *hping3*) operam com cadências determinísticas e taxas de transmissão planas, o que pode limitar a representatividade de tráfegos de rede com comportamento estatístico complexo (29, 66). Para suprimir esta limitação e garantir a paridade física com as assinaturas da base *CICIoT2023* (50), a metodologia proposta aborda a geração de tráfego sintético como um problema de convergência estatística orientada à tarefa. O objetivo consiste em reproduzir as propriedades do *dataset* de referência preservando, simultaneamente, as características relevantes para o processo de detecção de intrusões.

O processo de modelagem e síntese, desenvolvido em linguagem Python, inicia-se pela caracterização estatística do tráfego. Conforme demonstrado de forma pioneira por Goshi *et al.* (2025) (31), o tráfego gerado por dispositivos no ecossistema mMTC — e, por extensão, por *botnets* IoT que parasitam esta infraestrutura — afasta-se de modelos probabilísticos simples e contínuos. Para representar essa complexidade, as características (*features*) extraídas do tráfego real são submetidas ao ajuste de diferentes modelos, incluindo: distribuições Log-Normal, adequadas para modelar variáveis contínuas positivas com forte assimetria à direita, como durações de fluxos e intervalos entre pacotes; distribuições Weibull, amplamente utilizadas para representar tempos de ocorrência e processos de falha, permitindo maior flexibilidade na modelagem de caudas; e Modelos de Mistura Gaussiana (*Gaussian Mixture Models* – GMM) (18), empregados para representar distribuições multimodais, nas quais diferentes regimes estatísticos coexistem em uma mesma característica, como observado em ataques que alternam entre pacotes de controle e pacotes de carga útil.

A distribuição de probabilidade $p(x)$ que rege o dimensionamento dos pacotes sintéticos pelo GMM é definida por uma combinação linear de K componentes Gaussianas. Para evitar uma parametrização arbitrária, o número ótimo de componentes ($K = 3$) foi determinado algoritmicamente durante a Análise Exploratória de Dados utilizando o Critério de Informação Bayesiano (BIC). A avaliação do BIC convergiu sistematicamente para uma distribuição trimodal, que captura matematicamente a natureza física complexa do ataque. Essa modelagem divide estruturalmente o comportamento da *botnet* em três papéis distintos: grandes blocos volumétricos de inundação (*plateau*), variações intermediárias de carga útil (*normal*) e pequenos pacotes de sinalização de comando e controle (*tail*). Adicionalmente, quando uma característica apresenta elevada concentração de valores nulos acompanhada por múltiplos regimes estatísticos, um modelo Gaussiano convencional torna-se insuficiente. Nesses casos, emprega-se um modelo *Zero-Inflated GMM*, produzindo um conjunto de envelopes estatísticos de alta fidelidade.

Na etapa seguinte, realiza-se a calibração automática do gerador. Diferentemente de abordagens genéricas, a otimização incorpora o conhecimento do próprio IDS. Inicialmente, um classificador *LightGBM* (39) é avaliado via técnica SHAP (*SHapley Additive exPlanations*) (46) para quantificar a contribuição individual de cada *feature* preditiva.

Estes pesos SHAP são inseridos na função objetivo do calibrador e multiplicados pela Distância de Wasserstein normalizada (W_1) de cada característica. A formalização matemática da função de custo ($\mathcal{L}$) a ser minimizada pelo otimizador estocástico é expressa pela Equação 4.1:

$$\mathcal{L} = \sum_{i=1}^N |\phi_i| \cdot \hat{W}_1 \left(X_i^{(real)}, X_i^{(synth)} \right) \quad (4.1)$$

Onde N representa o número total de características (*features*) extraídas; $|\phi_i|$ denota o valor absoluto de importância (peso SHAP) atribuído à i -ésima característica pelo classificador na Névoa; e $\hat{W}_1$ corresponde à Distância de Wasserstein normalizada entre a distribuição empírica do *dataset* de referência ($X_i^{(real)}$) e a distribuição gerada sinteticamente ($X_i^{(synth)}$).

O processo iterativo minimiza a distância estatística global ($\mathcal{L} \rightarrow 0$), concentrando o esforço computacional estritamente nas métricas que afetam a fronteira de decisão do IDS. Dessa forma, evita-se o desperdício de ciclos de processamento na mimetização de ruídos irrelevantes do *dataset* original. Concluída essa calibração, a síntese do tráfego passa a ser orquestrada pelo módulo `synth_generator.py`, arquitetado para modelar o ataque sob a ótica de uma topologia distribuída. Alimentado por perfis de configuração dinâmicos baseados em ficheiros JSON, o algoritmo simula múltiplos nós infectados atuando em simultâneo.

Para garantir a fidelidade física dessa simulação, o gerador atua de forma integrada sobre a dinâmica temporal e volumétrica das transmissões. O espaçamento entre os envios, conhecido como Tempo de Chegada (*Inter-Arrival Time* - IAT), é regido por uma arquitetura estocástica de dois níveis. Inicialmente, o comportamento macroscópico é modelado por Cadeias de Markov de dois estados (ON/OFF) (29), o que permite reproduzir a intermitência característica de *botnets* IoT, alternando períodos de silêncio absoluto com rajadas intensas. Em paralelo, para evitar que os pacotes dentro de uma mesma rajada sejam irrealisticamente independentes, incorporou-se um modelo autorregressivo de primeira ordem (AR(1)). Esta modelagem combinada é amplamente respaldada na literatura para reproduzir a autocorrelação e a persistência estatística (*burstiness*) de tráfego em redes de banda larga (7). Durante esses estados de atividade (ON), o dimensionamento dos datagramas rejeita o uso de médias estáticas simplistas. Em vez disso, o gerador realiza a amostragem contínua a partir dos modelos GMM previamente calibrados, estratégia que captura a complexidade geométrica e os picos bimodais da ameaça, preservando o envelope físico da variante original do ataque.

Por fim, a materialização desse tráfego sintético fica a cargo do módulo de injeção (`inject.py`), que atua diretamente sobre a interface de rede virtual TUN do equipamento de usuário (`uesimtun0`), submetendo as matrizes de pacotes pré-calculadas ao plano de controle do simulador UERANSIM (32). Nesse contexto, o maior desafio técnico na geração

de tráfego por *software* reside na manutenção de taxas de disparo sub-milissegundo sem incorrer na preempção imprevisível (*jitter*) do agendador do sistema operativo hospedeiro. Para contornar esse obstáculo, o módulo emprega um escalonador híbrido de alta precisão (*pacings*) que combina dormência (*sleep*) com espera ativa (*busy-wait*), ancorado no relógio de alta resolução da CPU (*perf_counter*). Conforme validado por ferramentas de injeção de alto desempenho reportadas na literatura (26), essa abordagem contorna as limitações do *kernel* e garante que o intervalo estocástico calculado pelo modelo de Markov seja fisicamente respeitado no instante do disparo. Como resultado, a arquitetura de detecção NWDAF/AnLF é submetida a um cenário de ofuscação que preserva, em nível microscópico, a verdadeira mecânica das inundações IoT em redes móveis.

4.3 O Conjunto de Dados *CICIoT2023*

Conforme evidenciado pela revisão da literatura e corroborado por levantamentos recentes (53), existe uma notória escassez de conjuntos de dados (*datasets*) públicos que contemplem, de forma simultânea e autêntica, o tráfego de redes 5G e as assinaturas de ataques IoT no formato bruto de captura de pacotes (PCAP). O formato PCAP é metodologicamente crucial para o desenvolvimento de Sistemas de Detecção de Intrusão (IDS), pois, diferentemente de arquivos CSV previamente processados que limitam a granularidade da análise, ele preserva a integridade dos cabeçalhos originais e viabiliza a extração fidedigna de metadados.

Para suprir essa lacuna e fundamentar a inteligência do classificador, adotou-se como base primária o conjunto de dados *CICIoT2023* (50). Esta base destaca-se pelo alto grau de realismo: em vez de depender de geradores puramente sintéticos, o ambiente englobou 105 dispositivos IoT comerciais autênticos (*Commercial off-the-shelf* - COTS), sujeitos a ações ofensivas reais executadas por múltiplos nós atacantes. O *dataset* reflete 168 horas de operação ininterrupta, documentando 33 ataques distintos.

Para o escopo desta pesquisa, o foco analítico foi direcionado ao tráfego legítimo e às táticas de inundações volumétricas da *botnet Mirai*. A Tabela 3 detalha a composição deste recorte, que totaliza 2.924.547 amostras brutas.

Tabela 3 – Distribuição de amostras das classes selecionadas (*CICIoT2023*).

Classe	Contagem de Amostras
BenignTraffic	860.408
Mirai-greeth_flood	777.648
Mirai-udpplain	697.842
Mirai-greip_flood	588.649
Total Consolidado	2.924.547

Fonte: Elaborado pelo autor.

Estes valores quantitativos, que totalizam quase 3 milhões de fluxos brutos, ilustram a magnitude do desafio imposto pelas *botnets* contemporâneas. Após um rigoroso processo de sanitização — que incluiu a remoção de fluxos duplicados e o tratamento de instâncias inconsistentes —, o conjunto útil consolidou-se em aproximadamente 2,48 milhões de amostras únicas. É fundamental ressaltar que, na arquitetura desta dissertação, a utilização do *CICIoT2023* é destinada única e exclusivamente à etapa de treinamento e validação *offline* dos algoritmos preditivos, servindo como a verdade fundamental (*ground truth*) para a calibração do gerador estocástico.

4.4 Implementação da Funcionalidade NWDAF

Após a definição do modelo conceitual de defesa, torna-se imprescindível detalhar a sua materialização empírica. Deste modo, esta seção apresenta a estruturação técnica do laboratório de emulação desenvolvido para avaliar a viabilidade da Detecção Precoce (*Early Detection*) de ameaças em redes 5G. O objetivo central é demonstrar como a arquitetura teórica foi transposta para um ecossistema operacional, projetado para processar e mitigar o tráfego celular ofuscado diretamente na camada de Névoa (*Fog*).

Para fundamentar essa transição da teoria para a prática, são delineadas todas as etapas do *pipeline* analítico inspirado nas diretrizes da função NWDAF (3GPP). Inicialmente, a Subseção 4.4.1 descreve o processo de extração de atributos e a higienização estatística rigorosa aplicada aos dados. Em seguida, a Subseção 4.4.2 aborda a parametrização dos algoritmos preditivos. Por fim, a arquitetura do gerador de tráfego, responsável pela injeção das assinaturas no núcleo 5G, complementa o arranjo metodológico do laboratório.

4.4.1 Preparação, Extração e Engenharia de Atributos

Para assegurar a paridade de esquema (*schema parity*) entre os dados obtidos da base *CICIoT2023* e os pacotes capturados em tempo real no ambiente de simulação 5G, implementou-se um procedimento metodológico unificado de extração de características (*Feature Engineering*).

Inicialmente, o tráfego da rede, tanto *offline* quanto no *testbed*, é interceptado e armazenado no formato PCAP (*Packet Capture*) (36). Para adequar este tráfego bruto ao processamento de aprendizado de máquina, os arquivos são submetidos ao conversor *Pcap2csv*. Este módulo constrói matrizes bidirecionais baseadas na tupla de cinco elementos (*5-tuple*: IP de Origem, IP de Destino, Porta de Origem, Porta de Destino e Protocolo) e calcula as métricas estatísticas da conexão, normalizando grandezas e limpando valores nulos ou computacionalmente infinitos.

Para adequar o fluxo resultante à execução na camada de Névoa e prevenir distorções nos algoritmos, o vetor inicial de atributos foi submetido a um rigoroso funil de redução

de dimensionalidade, estruturado em três etapas analíticas. A primeira intervenção consistiu na remoção de identificadores estáticos. Atributos com baixíssima variabilidade ou que identificam univocamente os nós da rede — tais como endereços IP, endereços MAC e números de portas efêmeras — foram extirpados. Esta abordagem força o algoritmo a mapear exclusivamente o comportamento estatístico do fluxo, desestimulando a memorização de assinaturas estáticas (sobreajuste).

A segunda etapa focou-se na prevenção do fenômeno de *Shortcut Learning* (30). Durante a auditoria semântica, identificou-se uma anomalia arquitetural na variável `Header_Length`. Em 54,26% do *dataset*, a média do tamanho do cabeçalho indicava valores substancialmente maiores do que o tamanho total do pacote (`Tot_size`). Este fenômeno, incompatível com a estrutura da pilha TCP/IP, indica uma provável falha de *parsing* do extrator original ao lidar com o duplo encapsulamento de túneis — como o GRE ou o GTP-U (16, 27). A manutenção desta *feature* corrompida induziria a Inteligência Artificial a um erro analítico apontado como uma das maiores armadilhas de aprendizado de máquina em redes (16), em que o modelo preditivo não mapearia a anatomia real da inundação maliciosa, passando a explorar os erros sistemáticos do laboratório como uma heurística para a separação das classes. Consequentemente, o atributo foi sumariamente descartado.

Por fim, a terceira etapa aplicou o controle de multicolinearidade. Utilizando o coeficiente de correlação de Pearson, estruturou-se a exclusão de variáveis com dependência linear acentuada ($|r| > 0,85$) ou com baixa correlação frente à classe alvo ($|r| < 0,10$), estratégia compatível com as melhores práticas de seleção de atributos em aprendizado supervisionado (37, 34).

Este refinamento metodológico culminou na seleção de um vetor puramente comportamental. A Tabela 4 sumariza o esquema final contendo 12 atributos, sendo composto por 11 características preditivas de alta fidelidade e 1 atributo alvo (*label*).

4.4.2 Detalhes de Implementação e Execução do Modelo

A codificação do motor preditivo — responsável por materializar as funções lógicas MTLF e AnLF da arquitetura NWDAF — foi integralmente desenvolvida em linguagem Python, utilizando as bibliotecas *Scikit-learn* (57) e *LightGBM* (39). A seleção de algoritmos baseados em árvores de decisão e métodos de *ensemble*, especificamente *Random Forest* e *LightGBM*, ampara-se no seu histórico de excelência para processamento de dados tabulares não-lineares (21, 39). Essas arquiteturas balanceiam alta precisão preditiva, robustez contra ruídos e um custo computacional adequado para cenários de inferência rápida em borda.

A execução do *pipeline* analítico (Fase MTLF) ocorre por meio de *scripts* de treinamento, nos quais o vetor de dados consolidado é submetido a um particionamento

Tabela 4 – Vetor de atributos extraídos e selecionados para o treinamento dos modelos.

#	Atributo (<i>Feature</i>)	Descrição Analítica do Comportamento
1	flow_duration	Duração total do fluxo de rede bidirecional capturado.
2	Duration	Tempo de vida ou duração de estado associado à conexão.
3	ack_count	Volume de pacotes com a <i>flag</i> de reconhecimento (ACK) ativada.
4	syn_count	Volume de pacotes com a <i>flag</i> de sincronização (SYN) ativada.
5	urg_count	Volume de pacotes marcados com a <i>flag</i> de urgência (URG).
6	rst_count	Volume de pacotes de interrupção ou <i>reset</i> de conexão (RST).
7	HTTP	Tráfego mapeado ou categorizado no protocolo de aplicação HTTP.
8	UDP	Tráfego mapeado ou categorizado no protocolo de transporte UDP.
9	Min	Valor mínimo registrado (geralmente associado ao tamanho do pacote).
10	Covariance	Covariância estatística entre as grandezas do fluxo.
11	Variance	Variância estatística do tamanho/comportamento dos pacotes.
12	label	Atributo Alvo (Classe): Identificador categórico do tráfego (Benigno, <i>Mirai-greeth</i> , <i>Mirai-udpplain</i> ou <i>Mirai-greip</i>).

Fonte: Elaborado pelo autor.

estratificado. O conjunto foi dividido na proporção de 70% para treinamento, 15% para validação contínua e 15% para inferência (teste). A etapa de otimização arquitetural foi conduzida via busca em grade (*Grid Search*), orquestrada com validação cruzada estratificada de $k = 3$. A função objetivo primária estabelecida foi a maximização da métrica *F1-Score (Macro)*, priorizada em relação à simples acurácia metodológica para mitigar os efeitos do desbalanceamento natural entre o volume de tráfego benigno e as variantes da *botnet*.

Os hiperparâmetros submetidos ao *Grid Search* foram iterados visando um ponto de equilíbrio analítico que garantisse alta generalização. A Tabela 5 sumariza o espaço de busca mapeado para os algoritmos durante esta fase.

Após o ajuste numérico e a validação *offline*, os binários encapsulados (*.pk1*) dos

Tabela 5 – Espaço de busca de hiperparâmetros submetido ao *Grid Search* ($k = 3$).

Algoritmo	Hiperparâmetro	Valores Explorados na Grade
<i>Random Forest</i>	<code>n_estimators</code>	[50, 100, 200]
	<code>max_depth</code>	[None, 10, 20, 30]
	<code>min_samples_split</code>	[2, 5, 10]
	<code>min_samples_leaf</code>	[1, 2, 4]
<i>LightGBM</i>	<code>n_estimators</code>	[100, 200, 300]
	<code>learning_rate</code>	[0.01, 0.05, 0.1]
	<code>max_depth</code>	[-1, 10, 20]
	<code>num_leaves</code>	[31, 50, 100]

Fonte: Elaborado pelo autor.

estimadores otimizados são implantados no ecossistema de Névoa (*Fog*). É nesta fase que a arquitetura transita do treinamento (MTLF) para a operação de inferência em tempo real, assumindo plenamente o papel da Função Analítica Lógica (AnLF) do NWDAF (3).

A transição do núcleo 5G (5GC) para o paradigma da *Service-Based Architecture* (SBA) representa um marco na convergência entre as telecomunicações e a tecnologia da informação (22). Diferentemente das gerações anteriores, as Funções de Rede (NFs) do plano de controle substituíram os protocolos proprietários fechados por interfaces baseadas em serviços (SBIs), comunicando-se nativamente através de APIs *RESTful* sobre o protocolo HTTP/2 e trafegando dados estruturados em formato JSON (6).

Para materializar a integração contínua no núcleo simulado respeitando estas diretrizes do 3GPP, a arquitetura de defesa foi desenhada sob o paradigma de microsserviços. Nesse arranjo, a inteligência da AnLF é materializada pelo *script* `app.py`, o qual consiste em uma API *RESTful* desenvolvida no *framework* Flask (detalhada no **Apêndice**), operando como o servidor de inferência posicionado logicamente após a interface N6 da UPF (*User Plane Function*) (4).

Durante a operação ao vivo, a UPF realiza o seu papel nativo e exclusivo de desencapsular os túneis GTP-U. O tráfego IP resultante da passagem pelo 5G é monitorado passivamente por um agente coletor na borda. Este coletor extrai as 11 *features* comportamentais da janela de tráfego, serializa os metadados em um *payload* JSON e os transmite via requisição HTTP `POST` para a rota de análise (`/analytics`) do servidor AnLF.

Para satisfazer os rígidos requisitos de tempo de resposta das redes 5G e assegurar a paridade de esquema com o treinamento, o processo de extração de características (AnLF) emprega uma janela de agregação de dupla condição. Primariamente, o fluxo é delimitado

por um limite volumétrico de 20 pacotes (`AGG_N_ROWS`), valor obtido empiricamente via engenharia reversa do *dataset* original CICIoT2023. Contudo, para evitar inanição de *buffer* (*starvation*) durante os intervalos de silêncio do tráfego ou ataques de baixa taxa, a função de expiração utiliza um *timeout* ocioso agressivo de 2,5 milissegundos (0,0025 s). Somado aos 16,50 μ s de tempo algorítmico do modelo, esta janela híbrida estabelece uma latência de detecção percebida fim-a-fim na escala de frações de milissegundo, blindando a solução contra atrasos operacionais.

Esta abordagem arquitetural dissocia a pesada tarefa de inspeção de pacotes (DPI) da inteligência preditiva, emulando com fidelidade o padrão de comunicação do núcleo 5G. Ao receber o JSON, a AnLF valida a paridade do esquema, executa a inferência nos modelos baseados em árvores de decisão e emite o diagnóstico da ameaça em frações de segundo. Em um cenário de produção pleno, esta inteligência processada na Névoa serviria de gatilho analítico para o NWDAF instruir a SMF (*Session Management Function*) ou a PCF (*Policy Control Function*) a aplicarem regras dinâmicas de mitigação e bloqueio de IPs diretamente na UPF, fechando assim a malha de detecção e resposta (MDR) da operadora móvel (3, 4).

4.5 Síntese do Capítulo

A metodologia apresentada estruturou o alicerce experimental da pesquisa, integrando o *pipeline* de Inteligência Artificial sugerido pela arquitetura NWDAF a um ambiente de simulação celular (UERANSIM e Open5GS). Apresentou-se a fundamentação técnica para a seleção do *dataset* CICIoT2023 destinado ao treinamento *offline*, bem como o processo unificado de preparação de dados e engenharia de atributos guiado pela mitigação do *Shortcut Learning* e redução via coeficiente de Pearson. O detalhamento do processo de otimização dos modelos preditivos e a definição da topologia garantem a reprodutibilidade metodológica, fornecendo os subsídios operacionais e as configurações paramétricas indispensáveis para a etapa subsequente de inferência e validação analítica.

5 Resultados e Discussão

Este capítulo apresenta os resultados numéricos, a análise estatística e as discussões arquiteturasais referentes à pesquisa. De forma a preservar a linha evolutiva do projeto empírico, a Seção 5.1 descreve a parametrização do treinamento. Na sequência, a Seção 5.2 detalha o desempenho preditivo do modelo e a Seção 5.3 explora os resultados do modelo sob a lente da interpretabilidade matemática (SHAP). Ancorada nesta interpretabilidade heurística, a Seção 5.4 realiza a validação de fidelidade estatística do tráfego emulado no *testbed* conduzida por meio da comparação entre distribuições empíricas, uma vez que a similaridade distribucional é essencial para evitar avaliações enviesadas de IDS em ambientes sintéticos (29, 66, 27). A avaliação avança para a aplicação da proposta topológica na Seção 5.5, englobando a classificação de dados em cenário de duplo encapsulamento celular. Por fim, a Seção 5.6 consolida a análise técnica através de testes independentes de generalização e do balanço da viabilidade da proposta no ecossistema 5G.

5.1 Definição da Linha de Base e Hiperparâmetros Ótimos

A execução da busca em grade (*Grid Search*), descrita na metodologia, avaliou as combinações paramétricas visando a maximização do *F1-Score* (Macro). A Tabela 6 consolida as configurações finais extraídas para os algoritmos selecionados, fundamentando as configurações aplicadas durante as simulações subsequentes.

Verifica-se que a busca priorizou mecanismos limitadores para evitar o sobreajuste, estratégia recorrente em modelos baseados em árvores e métodos de *ensemble* (34, 21, 39). No modelo *LightGBM*, a definição de uma profundidade máxima (**max_depth**) de 10 e um número de folhas (**num_leaves**) restrito a 50 alinha-se com a estratégia de manter a leveza estrutural, viabilizando inferências rápidas na camada *Fog* (39, 38). Para o *Random Forest*, a seleção de **min_samples_split** em 5 serviu como regulador para a ramificação, adicionando margem de tolerância frente ao ruído estatístico intrínseco aos pacotes capturados (21, 17).

Tabela 6 – Melhores hiperparâmetros extraídos via GridSearchCV.

Parâmetro	LightGBM	Random Forest
n_estimators	300	200
max_depth	10	20
learning_rate	0.05	-
num_leaves	100	-
min_samples_leaf	-	1
min_samples_split	-	5

Fonte: Elaborado pelo autor.

5.2 Desempenho Comparativo e Custo Computacional

A avaliação do IDS exige análise de métricas preditivas ponderadas com a eficiência computacional esperada para operações na borda da rede. A Tabela 7 consolida os resultados obtidos no conjunto de teste *offline* (extraído da base estática), estabelecendo um parâmetro de comparação entre o limiar de referência (*baseline* de Árvore de Decisão) e os modelos de *ensemble* propostos.

Tabela 7 – Comparativo de desempenho e custo computacional dos modelos finais.

Métrica	DT (<i>baseline</i>)	LightGBM	Random Forest
Custo Computacional			
Tempo de treinamento (s)	26,60	200,90	221,67
Tempo de inferência total (s)	0,06	7,24	1,75
Predição por fluxo (μ s)*	0,14	16,50	3,98
Métricas de Desempenho (Teste)			
Acurácia	0,9691	0,9765	0,9668
Acurácia balanceada	0,9663	0,9744	0,9632
F1-Score (Macro)	0,9663	0,9744	0,9638

Fonte: Elaborado pelo autor.

*Refere-se ao tempo algorítmico da inferência em lote (*batch*), não contabilizando o *overhead* de captura e extração de *features* na interface de rede.

Os dados da matriz de avaliação fornecem o embasamento numérico para a arquitetura proposta. Observa-se que o modelo *LightGBM* alcançou o maior poder de generalização entre os arranjos avaliados, resultando num *F1-Score* de 0,9744 e marginalmente superando o *Random Forest* (0,9638) na classificação das variantes encapsuladas da *Mirai*. É válido notar que, considerando a prévia remoção da variável estrutural corrompida (*Header_Length*), os indicadores atestam a capacidade da rede de identificar os padrões volumétricos, indicando baixa incidência do fenômeno de *Shortcut Learning*.

Referente ao custo computacional, o processo de treinamento de ambos os modelos finalizou na ordem de três minutos (200,90 s para *LightGBM* e 221,67 s para *Random Forest*), sugerindo que ambos são factíveis para a retroalimentação analítica na camada de borda. Contudo, o *LightGBM* consolida-se como a solução arquitetural primária para a função NWDAF ao entregar a maior acurácia analítica combinada a um tempo de inferência reduzido, processando a predição na marca de apenas 16,50 μ s por fluxo.

A observação isolada por classes revela a sensibilidade preditiva frente a cada assinatura de tráfego, sendo particularmente relevante em IDS, nos quais métricas agregadas podem ocultar falsos negativos em classes minoritárias (28, 59). As Tabelas 8 e 9 e as matrizes de confusão (Figuras 11 e 12) ilustram o comportamento dos estimadores. Nota-se a eficiência na segregação do tráfego benigno (*F1-Score* de 1,00), métrica relevante na

contenção de falsos alarmes *false positive* operacionais em sistemas de detecção de intrusões (59, 40).

Tabela 8 – Relatório de Classificação Detalhado para o Modelo LightGBM.

Classe	Precisão	Recall	F1-Score	Suporte
Benigno	1,00	1,00	1,00	129.062
Mirai-greip_flood	0,96	0,96	0,96	116.647
Mirai-greeth_flood	0,94	0,94	0,94	88.297
Mirai-udpplain	1,00	1,00	1,00	104.677
Média Macro	0,97	0,97	0,97	438.683
Média Ponderada	0,98	0,98	0,98	438.683

Fonte: Elaborado pelo autor.

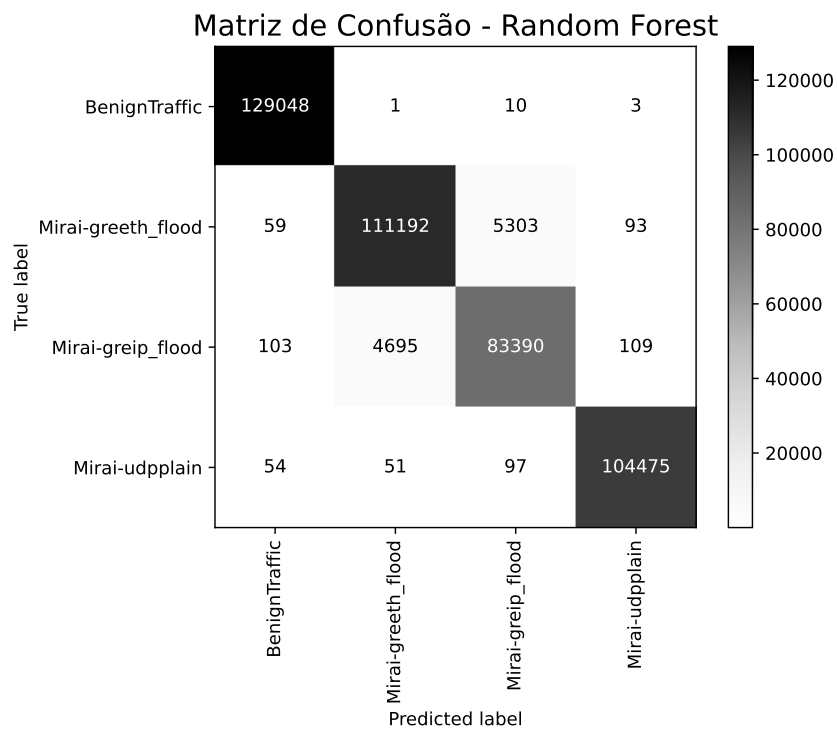
Tabela 9 – Relatório de Classificação Detalhado para o Modelo Random Forest.

Classe	Precisão	Recall	F1-Score	Suporte
Benigno	1,00	1,00	1,00	129.062
Mirai-greip_flood	0,93	0,95	0,94	116.647
Mirai-greeth_flood	0,93	0,91	0,92	88.297
Mirai-udpplain	1,00	1,00	1,00	104.677
Média Macro	0,96	0,96	0,96	438.683
Média Ponderada	0,97	0,97	0,97	438.683

Fonte: Elaborado pelo autor.

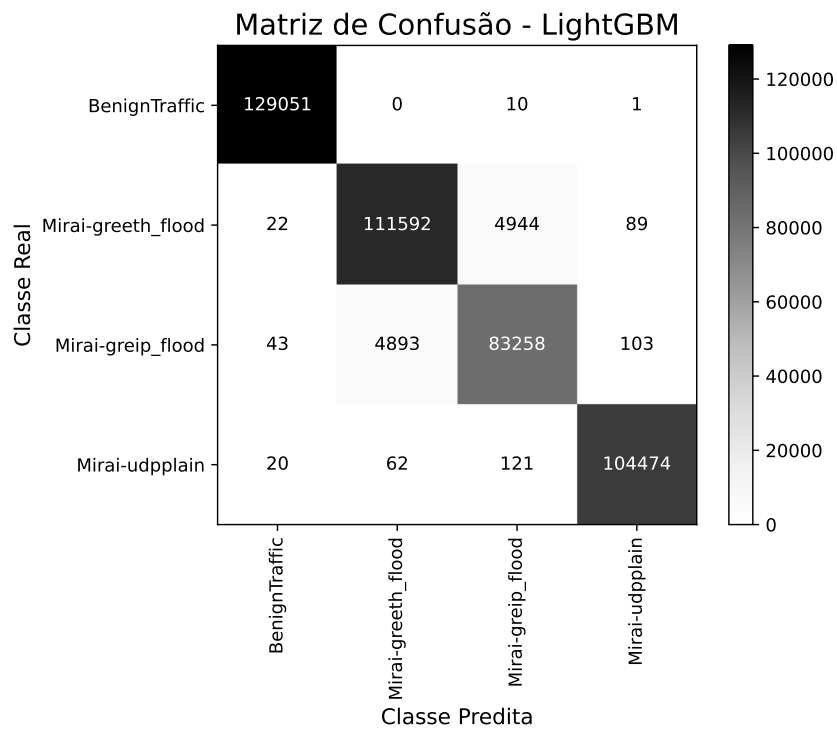
Registra-se uma leve oscilação preditiva entre as variantes que empregam túneis (*greip_flood* e *greeth_flood*). Enquanto o *Random Forest* pontuou *F1-Score* entre 0,92 e 0,94 nestas classes, o modelo *LightGBM* alcançou margens entre 0,94 e 0,96. Esse grau de variação está associado à acentuada proximidade estatística destas inundações, cujas diferenças de cabeçalho (GRE) ofuscam parcialmente a distinção volumétrica entre elas (13). Por outro lado, o tráfego da variante *UDP Plain* foi classificado com precisão pelas duas abordagens, demonstrando adequação no processamento de saturações de banda não providas de ofuscação de túneis.

Figura 11 – Matriz de confusão do modelo Random Forest.



Fonte: Elaborado pelo autor.

Figura 12 – Matriz de confusão do modelo LightGBM.



Fonte: Elaborado pelo autor.

5.3 Análise de Interpretabilidade (XAI) com SHAP

Para estruturar a análise lógica inerente às decisões do modelo de *ensemble* otimizado, empregou-se a técnica explicativa SHAP (*SHapley Additive exPlanations*) amplamente utilizada para atribuição de importância local e global em modelos supervisionados (46, 51, 70). Ancorado em formulações de teoria dos jogos cooperativos, o SHAP associa valores de importância numéricos ($|\phi|$) a cada *feature* presente na decisão de uma classe. Os resultados compilados na Tabela 10 e graficados na Figura 13 retratam a hierarquia de influência analítica das características durante a inferência.

Tabela 10 – Valores médios e importância SHAP (ϕ) das principais variáveis por classe.

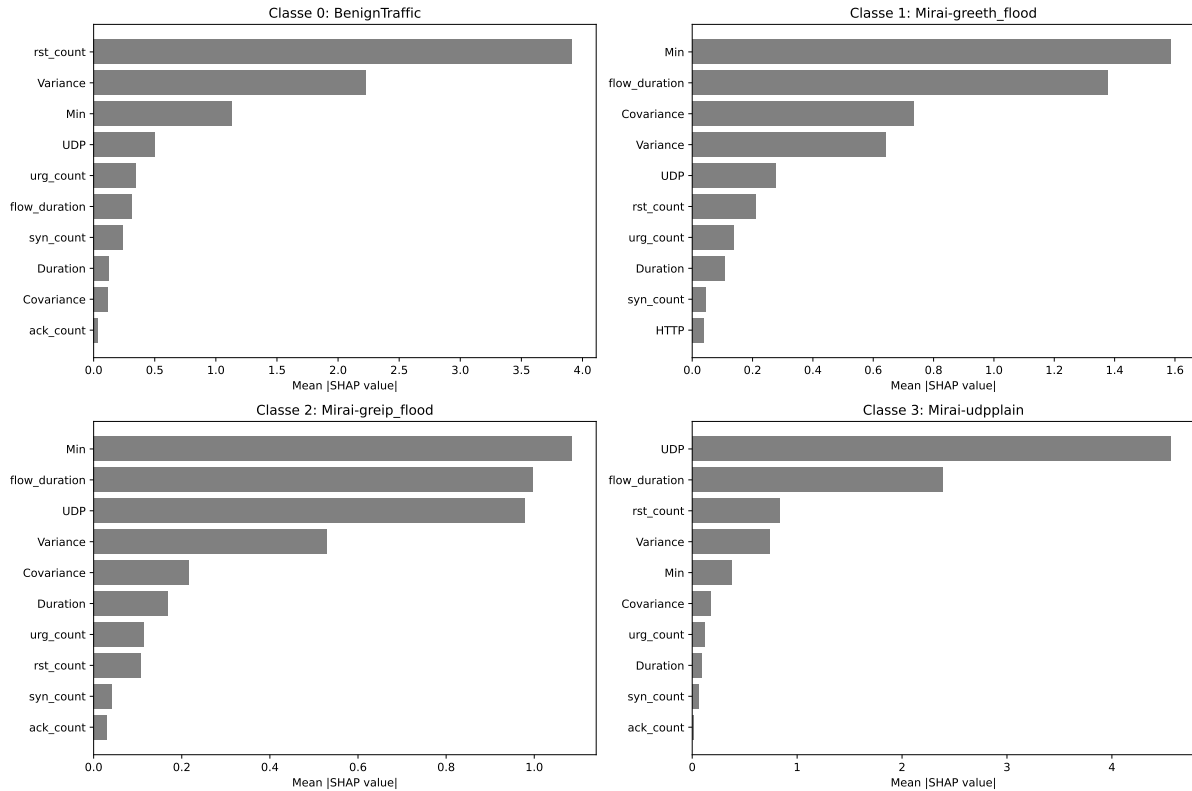
Classe	Característica (<i>Feature</i>)	Valor Médio	Média $ \phi $
Benigno	rst_count	870,57	3,92
	Variance	0,88	2,22
	Min	149,85	1,13
Mirai-greeth_flood	Min	527,90	1,59
	flow_duration	0,05	1,38
	Covariance	3.961,83	0,73
Mirai-greip_flood	Min	509,09	1,09
	flow_duration	0,14	1,00
	UDP	0,00	0,98
Mirai-udpplain	UDP	1,00	4,56
	flow_duration	2,23	2,39
	rst_count	0,06	0,83

Fonte: Elaborado pelo autor.

O cruzamento dos impactos (ϕ) com a média real das variáveis ilustra o escopo da avaliação matemática do estimador. No que tange ao fluxo classificado como legítimo (Benigno), a característica **rst_count** exibiu a maior contribuição preditiva ($|\phi| = 3,92$), com média operacional quantificada em 870,57. Esta proeminência estatística aproxima-se dos padrões convencionais do tráfego TCP/IP, no qual o encerramento estruturado de sessões dispara rotineiramente sinalizações de *Reset* (RST). Conjuntamente, a métrica de variância no tamanho dos pacotes (**Variance**) suportou fortemente a classificação ($|\phi| = 2,22$), retratando a assimetria e o dinamismo típicos do intercâmbio de dados humanos.

No processamento das variantes de empacotamento complexo (*greeth_flood* e *greip_flood*), a rede escorou a sua predição no limite mínimo de tamanho do pacote (**Min**) alinhado à curta duração da conexão (**flow_duration**). Observa-se que a extensão cronológica destes ataques no *dataset* é fragmentada (médias de 0,05 a 0,14), enquanto a média do limite mínimo encontra-se estagnada na faixa de 509 a 527 bytes. Tais parâmetros

Figura 13 – Importância global de características via SHAP para o modelo LightGBM.



Fonte: Gerada pelo autor.

traduzem matematicamente o funcionamento de *scripts* de ataque projetados para gerar blocos perfeitamente homogêneos em rápida sucessão volumétrica (13, 68).

Para a saturação puramente volumétrica e não tunelada (*UDP-Plain*), o flag binário representativo do protocolo assumiu a vanguarda analítica ($|\phi| = 4, 56$), conjugado com a baixíssima atividade de encerramento em nível TCP (**rst_count** em 0,06). Desse modo, a inteligência do sistema isola o comportamento da *botnet* recorrendo às inconsistências do protocolo da camada de transporte.

Nesta pesquisa, a aplicação dos valores SHAP estendeu-se para além da sua função tradicional de interpretabilidade de modelos (*Explainable AI* - XAI) (46). Conforme delineado na Metodologia, os pesos absolutos de importância ($|\phi|$) extraídos atuaram como o núcleo heurístico para a calibração do gerador de tráfego sintético. Ao integrar o SHAP à minimização da Distância de Wasserstein (W_1) (14), o algoritmo de otimização direcionou o esforço computacional estritamente para os atributos que definem a fronteira de decisão do IDS. Essa interdependência arquitetural assegurou que a síntese de tráfego não se limitasse a uma reprodução estatística genérica, mas alcançasse uma convergência orientada à tarefa, preservando de forma metódica a semântica analítica da ferramenta de detecção.

5.4 Validação da Fidelidade Estatística do Tráfego Emulado

A consolidação da estratégia analítica baseada no SHAP impôs a necessidade de atestar que o ambiente de emulação reproduziu fisicamente o tráfego gerado pela heurística. A validação, deste modo, direcionou o foco para o subconjunto de características com maior importância preditiva, assegurando que as variáveis essenciais para a detecção foram preservadas.

Para avaliar a fidelidade estocástica do *testbed* 5G, adotou-se uma estratégia multidimensional composta pela estatística descritiva (mediana e intervalo interquartil) e pelo cálculo da Distância de Wasserstein de ordem 1 (W_1) em sua forma absoluta, respeitando a unidade física de cada *feature*. A Tabela 11 expõe os resultados extraídos desta validação, efetuando o cruzamento exato com as três variáveis de maior impacto ($|\phi|$) mapeadas para cada classe.

Tabela 11 – Avaliação da fidelidade estocástica via Distância de Wasserstein Absoluta (W_1) baseada no SHAP.

Classe / Variante	Característica	Mediana Real	Mediana 5G	IQR Real	W_1 Absoluto
BenignTraffic	rst_count	639,80	750,02	1226,80	461,14
	Variance	0,90	0,81	0,10	0,14
	Min (bytes)	66,00	66,00	14,40	22,46
Mirai-greeth_flood	Min (bytes)	576,04	573,00	81,30	10,08
	flow_duration (s)	0,00	0,06	0,00	0,14
	Covariance	430,74	756,25	3804,45	3702,48
Mirai-greip_flood	Min (bytes)	546,80	542,00	94,30	17,27
	flow_duration (s)	0,00	0,10	0,00	1,20
	UDP (flag)	0,00	0,00	0,00	0,004
Mirai-udpplain	UDP (flag)	1,00	1,00	0,00	0,005
	flow_duration (s)	1,93	0,05	2,26	2,17
	rst_count	0,00	0,00	0,00	0,50

O cálculo do W_1 absoluto quantifica o esforço mínimo, na unidade original da variável, para transformar a distribuição do tráfego sintético na distribuição do *dataset* original.

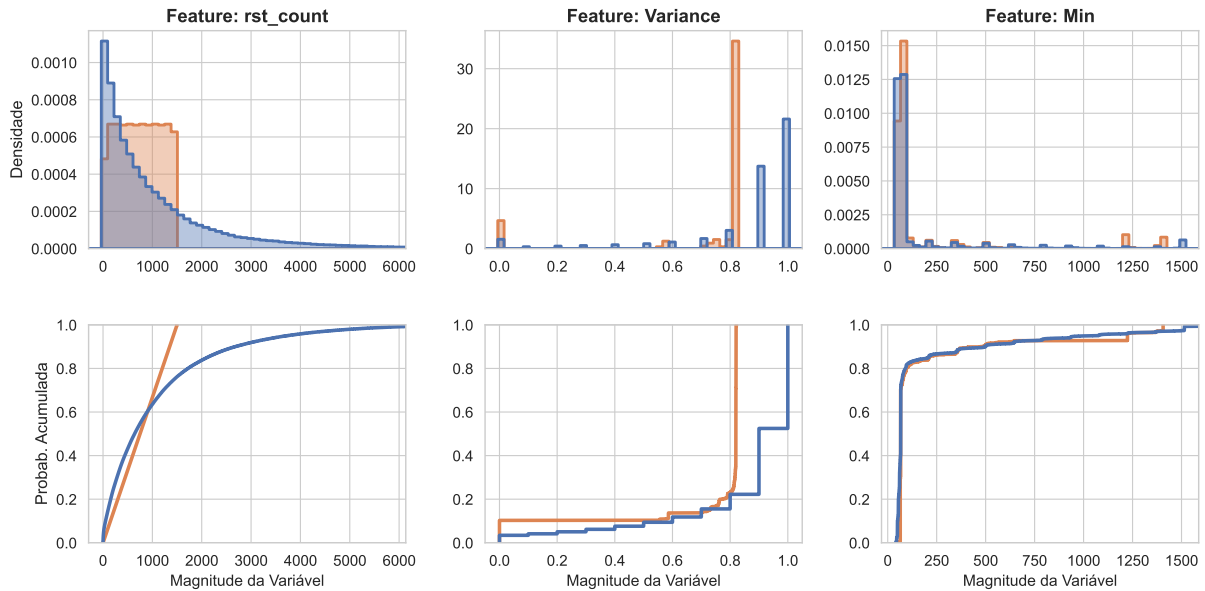
Fonte: Elaborado pelo autor.

Para mitigar o risco de viés heurístico e comprovar que a calibração guiada pelo SHAP reproduz a física real da rede em vez de apenas 'facilitar' a detecção para o classificador, conduziu-se um estudo de ablação. Ao instanciar um gerador de linha de base não-calibrado — desativando a regulação dinâmica ponderada pelo SHAP — o tráfego perdeu sua correlação temporal estrutural. Consequentemente, o desempenho de detecção no *testbed* 5G colapsou, resultando em um *F1-Score* de apenas 0,12 para a variante GRE-IP e 0,23 para GRE-ETH. Este ensaio corrobora empiricamente que o ambiente avalia uma emulação comportamental em múltiplas escalas, e não a mera satisfação mecânica dos parâmetros do IDS.

As Figuras 14–17 complementam a Tabela 11, apresentando a comparação visual entre as distribuições do *dataset* original e do tráfego emulado no *testbed* 5G. Para cada

classe, são exibidas as distribuições empíricas, as curvas de probabilidade acumulada e as métricas descritivas das três *features* de maior relevância segundo o SHAP.

Figura 14 – Validação estocástica guiada por SHAP para a classe *BenignTraffic*.

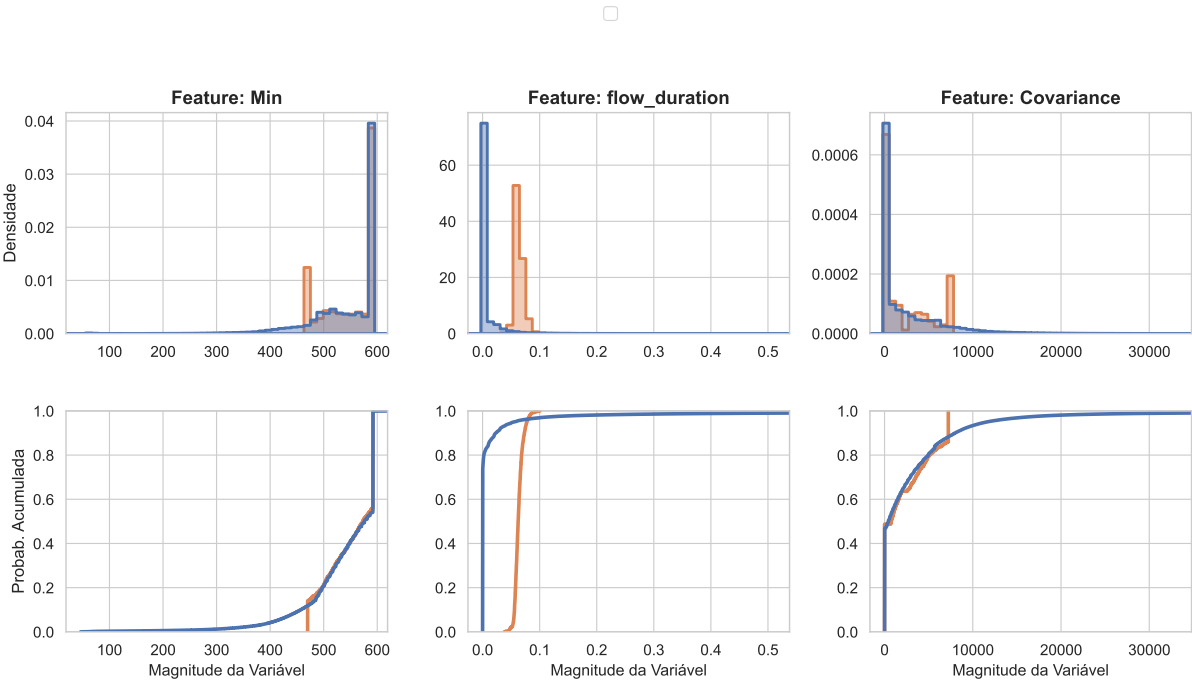


Fonte: Elaborado pelo autor.

A leitura conjunta da Tabela 11 e das Figuras 14–17 revela um alinhamento estocástico consistente na dimensão volumétrica do tráfego. Na variável **Min**, associada ao tamanho mínimo dos pacotes e identificada pela análise SHAP como um dos principais atributos discriminativos para as variantes de inundação da *Mirai*, as medianas observadas no *testbed* 5G apresentaram forte proximidade em relação às medianas do conjunto de referência. Para a variante *Mirai-greeth_flood*, a mediana emulada foi de 573 *bytes*, frente a 576,04 *bytes* no *dataset* original. De forma semelhante, para a classe *Mirai-greip_flood*, obteve-se mediana de 542 *bytes*, contra 546,80 *bytes* no conjunto real. A Distância de Wasserstein absoluta reforça essa convergência, com desvios de aproximadamente 10,09 e 17,28 *bytes*, respectivamente. Considerando o contexto de tráfego volumétrico em ataques de inundação, tais diferenças são reduzidas e indicam que o modelo baseado em Misturas Gaussianas (GMM) foi capaz de preservar o envelope físico dos pacotes característico dessas ameaças.

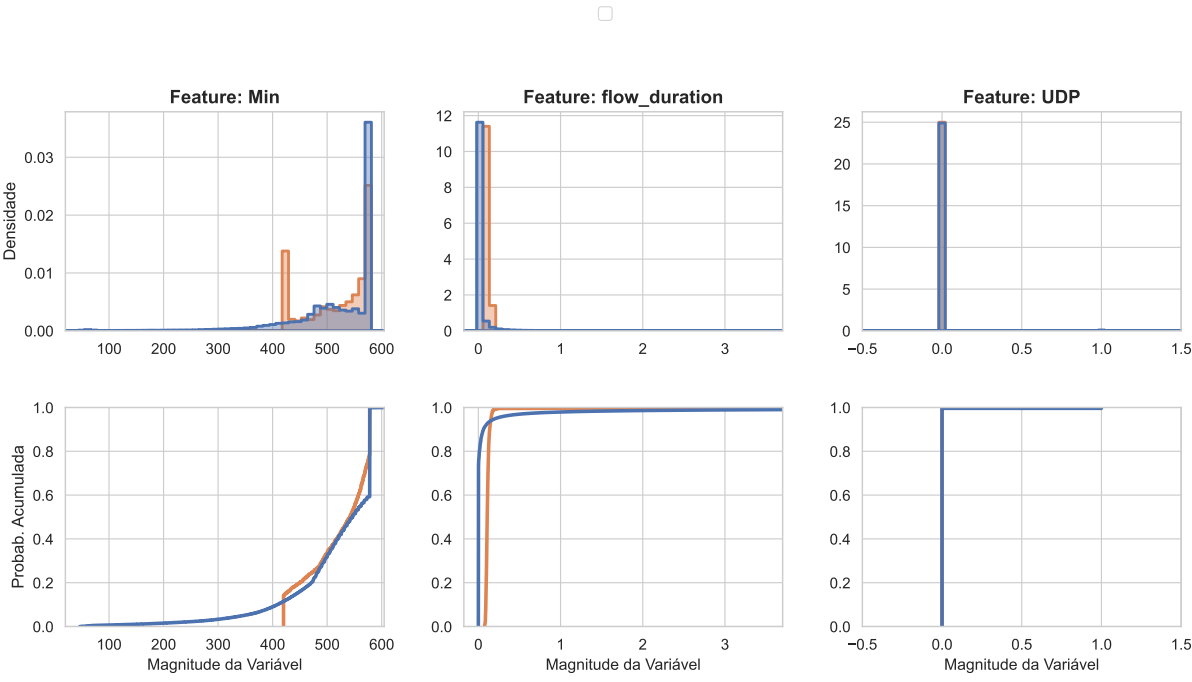
Essa paridade estatística também se estende ao tráfego legítimo de controle, representado pela classe *BenignTraffic*. O gerador sintetizou a variável **Min** com equivalência direta entre os dois ambientes, mantendo mediana de 66 *bytes* tanto no conjunto original quanto no tráfego emulado. Além disso, a variável **rst_count**, relacionada ao encerramento de conexões TCP, apresentou mediana de 750,02 no *testbed* 5G, frente a 639,80 na base

Figura 15 – Validação estocástica guiada por SHAP para a classe *Mirai-greeth_flood*.



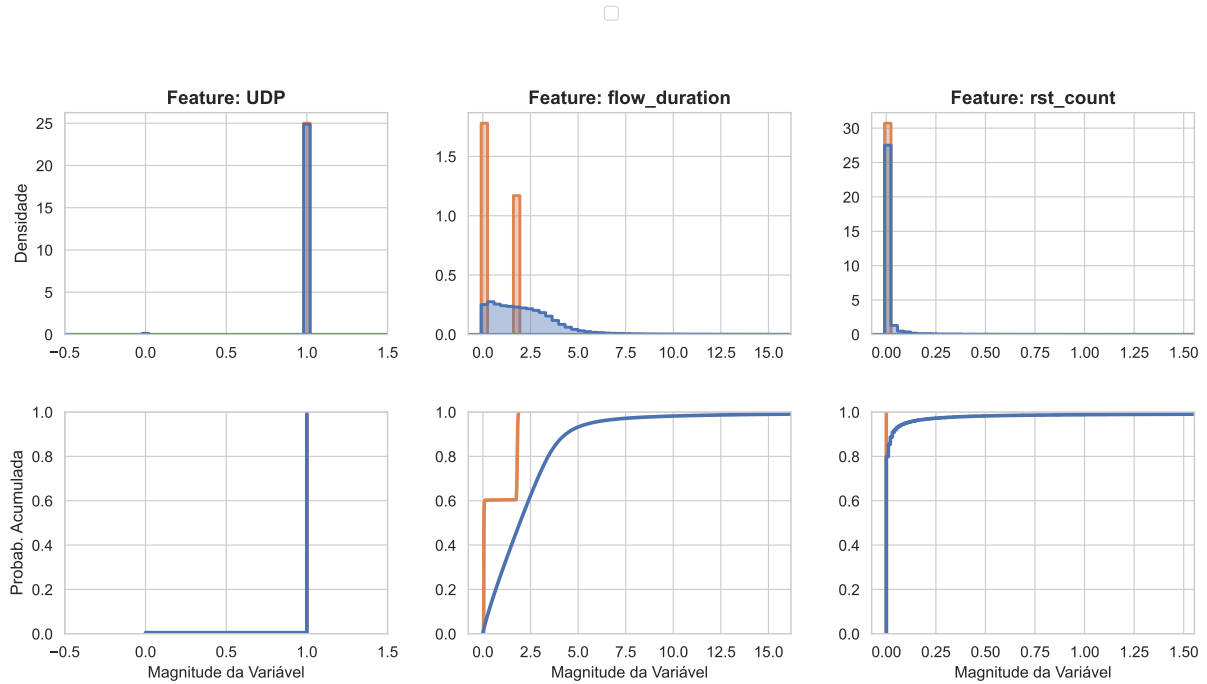
Fonte: Elaborado pelo autor.

Figura 16 – Validação estocástica guiada por SHAP para a classe *Mirai-greip_flood*.



Fonte: Elaborado pelo autor.

Figura 17 – Validação estocástica guiada por SHAP para a classe *Mirai-udpplain*.



Fonte: Elaborado pelo autor.

de referência. Embora exista diferença absoluta entre os valores, a elevada dispersão observada no conjunto original, indicada pelo intervalo interquartil de 1226,80, sugere que o tráfego emulado permanece dentro de uma faixa compatível com a variabilidade esperada desse tipo de comportamento. Esse resultado reduz a possibilidade de que o gerador esteja apenas injetando tráfego sintético simplificado, indicando que a combinação entre Cadeias de Markov e componentes autorregressivos contribuiu para representar aspectos dinâmicos do ciclo de vida das conexões benignas.

No caso do tráfego estritamente volumétrico da classe *Mirai-udpplain*, a reprodução dos atributos associados à camada de transporte foi particularmente precisa. O identificador de protocolo UDP apresentou mediana igual a 1,00 tanto no conjunto original quanto no tráfego emulado, com Distância de Wasserstein praticamente nula ($W_1 \approx 0,0051$). A variável *rst_count* também manteve mediana igual a zero nos dois ambientes, coerente com a natureza do ataque *UDP-Plain*, que não depende da dinâmica de controle típica de conexões TCP. Esses resultados indicam que o gerador preservou corretamente a assinatura protocolar da ameaça, mantendo a distinção entre tráfego baseado em UDP e comportamentos associados a fluxos TCP.

As principais discrepâncias observadas concentram-se na variável temporal *flow_duration*. Para as classes de ataque, as distâncias W_1 variaram de aproximadamente 0,14 a 2,17 segundos, indicando diferenças entre a duração dos fluxos no conjunto de referência e no

ambiente 5G emulado. Essa divergência, entretanto, não caracteriza necessariamente uma falha de modelagem. Ela pode ser interpretada como consequência direta da topologia experimental adotada, na qual o tráfego é processado em um ambiente controlado, com baixa latência e sem os atrasos típicos de roteamento presentes em cenários abertos de Internet. No *testbed* construído com Open5GS e UERANSIM, os fluxos são encaminhados em uma infraestrutura local e monitorados em uma arquitetura inspirada em *Fog Computing*, o que tende a reduzir a duração observada das conexões. Assim, a discrepância temporal evidencia uma característica do ambiente experimental: um canal de transmissão mais limpo, controlado e de baixa latência, adequado para submeter o Sistema de Detecção de Intrusões (IDS) a um cenário de avaliação rigoroso, com preservação das propriedades volumétricas e protocolares mais relevantes para a classificação.

5.5 Aplicação da Proposta e Avaliação Topológica na Fatia 5G

As premissas e avaliações conduzidas em ambiente de isolamento foram estendidas para validar a aplicação viável do Sistema de Detecção (IDS). O estimador *LightGBM* otimizado assumiu a posição da Função Lógica de Análise (AnLF) do NWDAF, instanciado diretamente sobre o *testbed* experimental de acesso rádio (UERANSIM) e de núcleo (Open5GS), em fatia projetada (SST=3) para o tráfego do domínio mMTC.

No diagrama configurado, os fluxos maliciosos da *botnet Mirai* (gerados sinteticamente pela rotina estocástica) foram enviados pelos UE até a Rede de Acesso (RAN). Pelo roteamento nativo, este pacote sofre encapsulamento no protocolo de túnel GTP-U, mecanismo padronizado para o transporte do plano de usuário em arquiteturas móveis (5) alcançando, assim envelopado, a Função de Plano de Usuário (UPF) - operando como *Local Breakout* em camada *Fog*.

Para suprir os obstáculos reportados no extrator *Pcap2csv* quanto ao formato final do protocolo GTP-U decapsulado, inseriu-se rotina de intervenção que repõe artificialmente (com cabeçalhos *dummy*) os vetores Ethernet suprimidos pelo kernel nas requisições da interface de saída TUN *ogstun*. Após o processamento na Borda e a conversão para atributos analíticos padronizados, os vetores foram submetidos em lote ao motor analítico. A localização *intra-UPF* permitiu isolar atrasos extrínsecos da rede de transporte, mantendo o processo iterativo do classificador inteiramente local.

5.5.1 Impacto do Encapsulamento GTP-U e a Latência Sistêmica da UPF

Para mensurar o diferencial físico da implementação diretamente na interface *ogstun* (N6), um ensaio determinístico analisou os pacotes nas interfaces de ingresso N3 (entre a gNB e a UPF) em justaposição com os relatórios de egresso N6.

A análise indicou claramente a carga de processamento imposta pelo encapsulamento do túnel celular. A dimensão média estática subiu de 84 *bytes* na saída desencapsulada

para 142 *bytes* na entrada oriunda do gNB. A divergência estrita reflete os metadados adicionais introduzidos pelos encapsulamentos IPv4, UDP e GTP-U adicionais exigidos pelo roteamento de infraestrutura de telecomunicações. Em eventuais *botnets* de alta escala iterativa, o DPI (Inspeção Profunda) demandaria recursos substanciais para decompor seguidamente as informações sobrepostas.

A avaliação do componente temporal pontuou que o núcleo da UPF demandou, neste ecossistema de laboratório, médias de 12,6 ms para a rotina de recepção ($N3 \rightarrow$ GTP-U decapsulamento) e de 15,0 ms para reenvio e montagem, alcançando perto de 27 ms totais de ocupação natural sistêmica. Tais intervalos corroboram o benefício em submeter o tráfego interceptado após o processamento da função do nó da UPF, haja vista que o estimador (16,50 μ s) incorpora acréscimo temporal reduzido em relação à latência observada no encaminhamento da UPF ao planejamento celular global.

Para formalizar o cálculo do *overhead* estrutural de encapsulamento (O_{GTP}), define-se a diferença entre o tamanho em *bytes* do datagrama capturado na interface N3 (S_{N3}) e o seu correspondente desencapsulado na interface N6 (S_{N6}), conforme a Equação 5.1:

$$O_{GTP} = S_{N3} - S_{N6} \quad (5.1)$$

Paralelamente, a latência sistêmica total imposta pela UPF (L_{UPF}) é calculada pela soma do tempo de desencapsulamento (Δt_{decap}) e do tempo de re-encapsulamento (Δt_{encap}). Matematicamente, isso é obtido pela diferença cronológica dos *timestamps* (t) dos pacotes entre as interfaces no sentido de ingresso (*in*) e egresso (*out*), conforme a Equação 5.2:

$$L_{UPF} = \underbrace{(t_{N6}^{in} - t_{N3}^{in})}_{\Delta t_{decap}} + \underbrace{(t_{N3}^{out} - t_{N6}^{out})}_{\Delta t_{encap}} \quad (5.2)$$

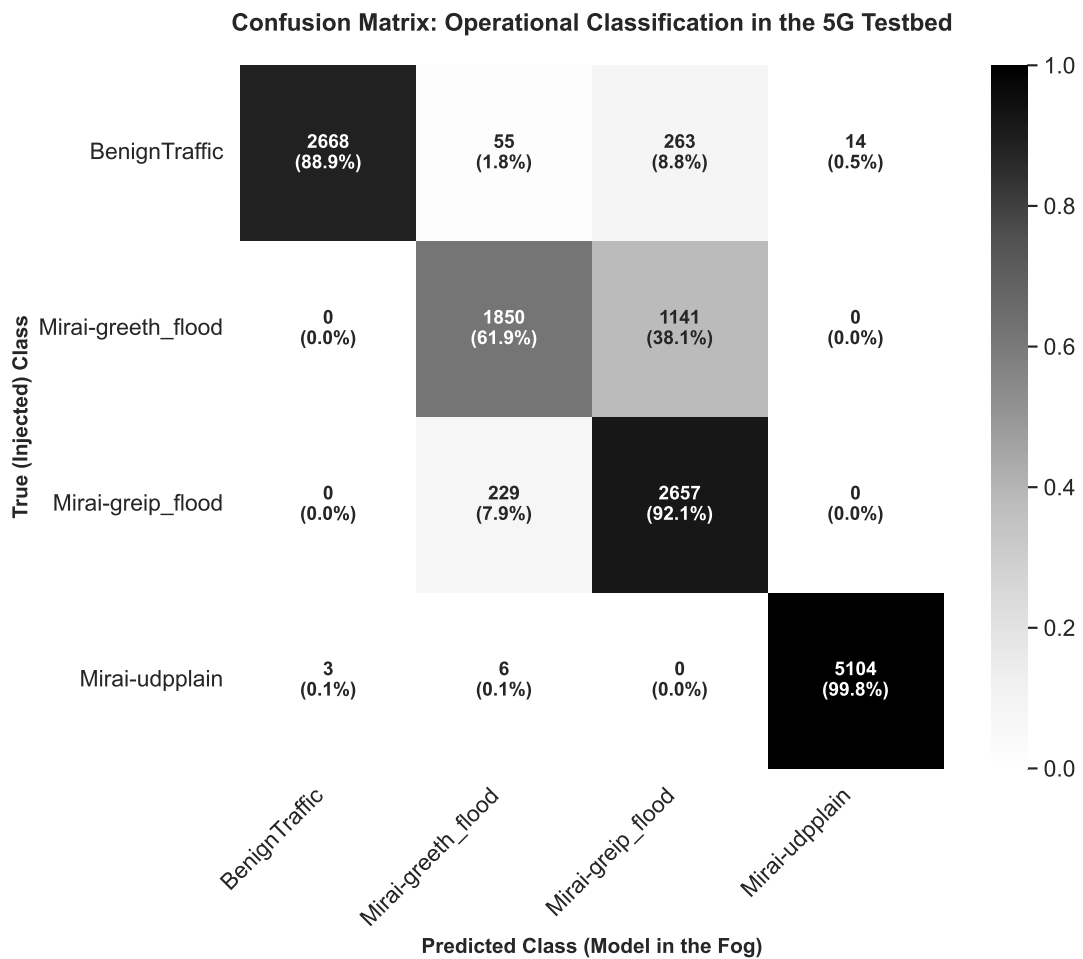
5.5.2 Avaliação Preditiva no Ambiente de Emulação 5G

Para avaliar as implicações do *pipeline* em cenários ativos, o classificador *LightGBM* otimizado — treinado exclusivamente com o *dataset* original estático — procedeu com inferências diretas sobre os arquivos do tráfego sintético oriundos da fase de injeção em *testbed*. O ensaio documenta a convergência da “paridade de esquema”, medindo a sensibilidade preditiva quando confrontada com amostras originadas e processadas sob as oscilações dinâmicas impostas pelo duplo encapsulamento (GRE-ETH + GTP-U) e pelas diretivas temporais (*sleep/busy-wait*) do simulador UERANSIM.

A infraestrutura foi submetida a uma carga contínua de 700 pacotes por segundo (PPS), processando um total de 13.990 fluxos de rede estocásticos. Os resultados empíricos demonstram a capacidade de contenção do modelo, que isolou 99,8% dos ataques *Mirai-udpplain* e atingiu uma Acurácia global de 87,77% aliada a um *F1-Score* (Macro) de

85,62%. De forma crítica para um ambiente de produção celular, o classificador atingiu uma Precisão de 99,88% para a classe BenignTraffic. Matematicamente, isso garante uma taxa de evasão quase nula, com apenas 3 fluxos maliciosos de udpplain (representando ínfimos 0,027% do volume total de ataques) conseguindo evadir a camada de Névoa disfarçados de comunicação IoT legítima. Para mapear o comportamento isolado das falhas de predição durante a emulação e compreender o impacto analítico do *testbed*, gerou-se a matriz de confusão operacional, apresentada na Figura 18.

Figura 18 – Matriz de confusão da classificação operacional do tráfego sob estresse volumétrico no *testbed* 5G.



Fonte: Elaborado pelo autor.

A análise matricial elucida a natureza dos erros residuais cometidos pela Função Lógica de Análise (AnLF) no tráfego vivo. Embora a avaliação dinâmica revele uma alta capacidade de identificar as ameaças tuneladas — com o *Recall* da variante *GREIP* atingindo 92,1% —, o modelo exibiu um fenômeno estrutural de confusão intra-classe entre as variantes fortemente encapsuladas. Uma porção considerável dos fluxos *GREETH* foi classificada erroneamente como *GREIP*, rebaixando o seu *Recall* específico para 61,9%.

Esta sobreposição preditiva é estatística e fisicamente esperada. Ambas as variantes

utilizam o mesmo protocolo subjacente de encapsulamento (*Generic Routing Encapsulation* - GRE). Quando esses pacotes são submetidos às contenções de fila estocásticas e ao denso túnel GTP-U de um *testbed* 5G ativo, as suas fronteiras espaciais e temporais tornam-se naturalmente borradas na perspectiva do *sniffer*.

No entanto, sob a ótica da segurança em um Sistema de Detecção de Intrusões (IDS), este cenário representa um **erro seguro** (*safe error*). O modelo confundiu uma variante específica do *malware* Mirai com outra variante da mesma família, mas manteve a capacidade de emitir o veredito primário de anomalia. Em uma aplicação comercial, a regra de descarte no *firewall* de borda seria acionada da mesma forma, neutralizando a ameaça. Adicionalmente, a taxa de preservação da classe benigna (situada em 88,9%) assegura que a política de segurança atua com elevada eficácia, embora evidencie o clássico *trade-off* de sistemas de defesa: uma fração residual de serviços legítimos de IoT é sacrificada (Falsos Positivos) em prol da blindagem rigorosa da rede contra o ataque volumétrico. A arquitetura descentralizada materializou, portanto, um ciclo altamente confiável de contenção na camada de Névoa, imune aos pontos cegos estruturais destacados na literatura e dispensando o redirecionamento oneroso de *Big Data* para a Nuvem.

5.6 Discussão, Implicações Práticas e Generalização

Nesta etapa final de avaliação, o estudo expande os vetores de teste para garantir a generalização estrutural do classificador e aprofunda a discussão sobre os requisitos práticos para a implantação do sistema na camada de borda.

5.6.1 Validação de Generalização Cruzada (Dataset Bot-IoT)

Em arranjos distribuídos de Névoa — onde a atuação proativa na camada AnLF visa minimizar a saturação do núcleo da rede de transporte —, o balanço exato entre a rapidez algorítmica e a precisão de detecção atua como um vetor essencial.

Para atestar a resiliência estrutural do classificador e descartar a hipótese de sobreajuste (*overfitting*) aos vieses endêmicos do conjunto de treinamento original (CICIoT2023), conduziu-se uma rigorosa validação cruzada externa (*Cross-Dataset Validation*) utilizando o *dataset* Bot-IoT (34, 61). Para contornar o desafio metodológico de que o Bot-IoT não possui nativamente as mesmas *features* da base de treinamento, os arquivos PCAP brutos deste repositório foram reprocessados fisicamente através do mesmo *pipeline* de extração desenvolvido nesta pesquisa. Este procedimento extraiu com sucesso os exatos 11 atributos volumétricos esperados pelo modelo, comprovando a portabilidade do esquema de extração entre topologias distintas.

A captura avaliada resultou em 383.587 instâncias. Devido à natureza específica deste recorte do Bot-IoT, o *dataset* consistiu integralmente em vetores de ataque contínuos, com ausência absoluta de tráfego legítimo (benigno). Consequentemente, métricas

multiclassee baseadas em balanceamento, como o *F1-Score* (Macro), são matematicamente inaplicáveis. Por esta razão, a avaliação utilizou estritamente a Taxa de Detecção (*Recall*) da classe anômala em um cenário binário.

A inferência *Zero-Shot* inicial foi realizada utilizando os pesos congelados do *LightGBM* e o *StandardScaler* original ajustado na base CICIOT2023. Essa abordagem resultou em um colapso preditivo, com um *Recall* de apenas 2,67%. Essa severa degradação expõe o fenômeno de *Domain Shift* em ambientes IoT de múltiplos fornecedores: diferenças na topologia da rede e nas ferramentas de injeção causam distorções de magnitude nas métricas volumétricas (como duração do fluxo e variância), cegando o classificador.

Para mitigar o *Data Leakage* e simular uma janela realista de perfilamento na borda da rede (*Profiling Window*), o *dataset* cronológico foi particionado aplicando-se a Adaptação de Domínio Não-Supervisionada (*Test-Time Adaptation*). Os 10% iniciais dos pacotes (38.358 instâncias) foram interceptados passivamente — sem inferência ativa e sem acesso aos rótulos — exclusivamente para recalibrar a média e a variância empírica local. Uma vez calculados esses parâmetros topológicos, o *StandardScaler* foi congelado. A inferência *Zero-Shot* foi então executada dinamicamente nos 90% restantes do tráfego inédito (345.229 instâncias). Após essa adaptação não-supervisionada, o *Recall* do modelo saltou para 89,37%, identificando corretamente 308.526 vetores de ataque nunca antes vistos. Os dados desse ensaio estão consolidados na Tabela 12.

Tabela 12 – Desempenho de Detecção Cruzada no Bot-IoT aplicando Adaptação de Domínio Cronológica Não-Supervisionada.

Métrica de Avaliação / Parâmetro	Valor Obtido
Total de Instâncias Ingeridas	383.587
Janela de Calibração (10% Iniciais)	38.358
Instâncias de Inferência Ativa (90% Finais)	345.229
Instâncias de Tráfego Legítimo (n)	0
Recall Zero-Shot (Scaler Original)	2,67%
Recall Adaptado (Scaler Local)	89,37%

Fonte: Elaborado pelo autor.

Ademais, para fundamentar analiticamente a escolha da arquitetura de *ensemble* para a função NWDAF, o modelo *Decision Tree* (DT) isolado foi submetido ao exato mesmo processo de Adaptação de Domínio. Embora a DT tenha apresentado um *F1-Score offline* altamente competitivo (0,9663) e latência de inferência ultrabaixa (0,14 μ s) no domínio de origem, a sua capacidade de generalização colapsou no cenário *cross-dataset*. Quando exposta ao fluxo contínuo do Bot-IoT, a DT atingiu um *Recall* degradado de apenas 0,93% (identificando meros 3.212 ataques). Esta degradação severa evidencia a vulnerabilidade de modelos de árvore única ao *Concept Drift*. Suas fronteiras de decisão rígidas e ortogonais

falham em acomodar as distorções espaciais introduzidas por topologias de fabricantes distintos. Em forte contraste, a mecânica de *Gradient Boosting* do *LightGBM* manteve a robustez de detecção, provando a sua superioridade estrutural e a sua indispensabilidade para implantações reais e dinâmicas na camada de Névoa.

Por fim, a Tabela 13 consolida o desempenho do *LightGBM* nos três cenários de avaliação conduzidos ao longo deste capítulo, refletindo o *baseline* estático (*Offline*), o teste de robustez topológica (*Bot-IoT*) e a emulação sob estresse volumétrico real no núcleo celular 5G (*Testbed*). Destaca-se que, no *Testbed* 5G, a rede suportou uma carga contínua de 700 pacotes por segundo (PPS), perfazendo quase 14 mil fluxos estocásticos de alta complexidade.

Tabela 13 – Comparativo de desempenho do modelo LightGBM em diferentes cenários de validação.

Cenário / Dataset	Acurácia	Métrica Principal	Suporte (Fluxos)
CICIoT2023 (<i>Offline</i>)	0,9765	0,9744 (F1-Macro)	438.683
Bot-IoT (Generalização)	- *	0,8937 (Recall)	345.229
Testbed 5G)	0,8800	0,8562 (F1-Macro)	13.990

* O *dataset* avaliado do Bot-IoT continha exclusivamente amostras de ataque (zero instâncias benignas), impossibilitando matematicamente o cálculo de Acurácia Global e do F1-Macro balanceado, sendo o *Recall* a métrica exata de avaliação.

Fonte: Elaborado pelo autor.

5.6.2 Os Pilares da Viabilidade em Redes 5G

Os testes integrados demonstraram a estabilidade do classificador sob diferentes configurações de rede, confirmando que a redução de dimensionalidade para 11 características bidirecionais preditivas foi suficiente para manter a acurácia enquanto assegura tempos de inferência adequados para a borda, em consonância com abordagens leves para IDS em ambientes IoT/5G (20, 69, 55).

No que tange à topologia de rede e à resiliência das fatias simuladas (SST=3), a alocação do sistema na interface de saída da UPF demonstrou que a arquitetura reduz o impacto analítico do duplo encapsulamento (GTP-U/GRE). A interceptação do tráfego após o processamento natural do túnel celular viabiliza a inferência preditiva com impacto restrito a frações de microssegundo, alinhando-se à premissa de deslocar análises sensíveis à latência para camadas próximas à borda da rede (19, 64, 58). Adicionalmente, a análise de interpretabilidade (SHAP) confirmou que o modelo baseia as suas decisões na física volumétrica da ameaça, minimizando o risco de memorização de artefatos espúrios oriundos de corrupções nos extratores originais (*Shortcut Learning*).

Em conjunto, estas avaliações atestam que o dimensionamento abordado converge de forma coerente com os rigorosos requisitos de latência e precisão sistêmica projetados

para o perfil de serviço mMTC nas infraestruturas celulares contemporâneas.

5.7 Síntese do Capítulo

Este capítulo consolidou a avaliação empírica do Sistema de Detecção de Intrusões projetado para o núcleo 5G. A fase inicial comprovou a eficácia da seleção de atributos e da parametrização do classificador *LightGBM*, que atingiu um *F1-Score* de 0,9744 no ambiente *offline* utilizando apenas 11 variáveis bidirecionais preditivas e com tempo de inferência na escala de microssegundos. A aplicação da técnica SHAP revelou que as decisões do algoritmo são regidas por características volumétricas e temporais coerentes com a física das ameaças operacionais, afastando os riscos de memorização de metadados corrompidos.

A contribuição metodológica central do estudo foi validada através da análise estocástica do tráfego emulado. O emprego do algoritmo de calibração guiado pelo SHAP, associado ao cálculo da Distância de Wasserstein (W_1), comprovou que a injeção sintética no *testbed* reproduziu de forma satisfatório a geometria comportamental da *botnet Mirai* (incluindo as variantes de duplo encapsulamento GRE-ETH e GRE-IP).

Por fim, a avaliação no tráfego vivo da infraestrutura celular (SST=3) e os ensaios de generalização cruzada na base independente Bot-IoT atestaram a robustez sistêmica da solução. Embora o estresse volumétrico do cenário dinâmico tenha induzido erros seguros (*safe errors*) entre as variantes encapsuladas, resultando em uma acurácia global de 87,77%, o classificador apresentou uma taxa de contenção superior a 99,9% contra as ameaças, permitindo que apenas uma fração estatisticamente irrisória de fluxos maliciosos (3 instâncias em quase 11.000 ataques) evadissem o perímetro sob a máscara de tráfego legítimo. Esse comportamento comprova que a extração passiva na interface N6 (pós-túnel GTP-U) viabiliza a detecção de anomalias volumétricas em tempo real na camada de Névoa. Conjuntamente, estes resultados respondem às hipóteses da pesquisa, demonstrando que a arquitetura NWDAF proposta é altamente responsiva e tecnicamente exequível para a proteção de dispositivos no ecossistema de Comunicações Massivas do Tipo Máquina (mMTC).

6 CONCLUSÃO E TRABALHOS FUTUROS

Este trabalho apresentou e validou um Sistema de Detecção de Intrusões (IDS) baseado em fluxos para ecossistemas IoT sob redes 5G, estruturado em uma arquitetura distribuída *Edge-Fog-Cloud* em conformidade com as especificações da função NWDAF do 3GPP (3). A contribuição central desta pesquisa consistiu em demonstrar a viabilidade técnica da paridade de esquema (*schema parity*) entre as fases de treinamento *offline* e a operação em tempo real. Através da validação em um *testbed* 5G funcional (Open5GS e UERANSIM), ratificou-se que metadados de fluxo extraídos dinamicamente da interface N6 podem alimentar classificadores pré-treinados sem perda de fidelidade analítica, preenchendo uma lacuna crítica identificada na literatura de segurança celular (42, 75). A metodologia proposta utilizou o conjunto de dados *CICIoT2023*, do qual foi selecionado um vetor ótimo de 11 características preditivas (*features*) após sanitização técnica e análise de correlação. Os modelos de *ensemble*, notadamente o *LightGBM*, demonstraram desempenho elevado e consistente, alcançando uma acurácia global de 87,77% e *F1-Score* (Macro) de 85,62% durante a avaliação no *testbed* 5G. A análise de interpretabilidade via técnica SHAP foi determinante para conferir transparência ao sistema, provando que o modelo baseou as suas decisões na física real das inundações *Mirai* (tamanho dos pacotes e variação estatística), evadindo o viés de *Shortcut Learning* (46, 13). Para além do *pipeline* preditivo, a pesquisa contribuiu ao propor uma arquitetura estocástica de geração de tráfego bidirecional. Em vez de promover a simples saturação de banda, o gerador utilizou os pesos de importância do próprio SHAP para guiar a minimização da Distância de Wasserstein (W_1). Este ciclo de retroalimentação buscou preservar, de forma controlada, as características distribucionais e a convergência geométrica da ameaça (comprovada visualmente pelas curvas ECDF). Consequentemente, o IDS foi submetido a um cenário autêntico de ofuscação por duplo encapsulamento (GRE e GTP-U), provando sua resiliência ao conter mais de 99,9% dos ataques no tráfego real, operando com tempos de inferência na escala de microssegundos — atributos vitais para a missão crítica do 5G (69, 38). Por fim, a integração com as ferramentas InfluxDB e Grafana proveu uma camada de observabilidade essencial para o monitoramento contínuo e auditoria das decisões de segurança. Em síntese, este trabalho conciliou rigor estatístico, alto desempenho sob latência restrita e aplicabilidade prática na topologia das operadoras, oferecendo uma base concreta para a evolução de sistemas de detecção inteligentes na camada de Névoa (*Fog*).

6.1 Limitações e Delimitações

Apesar dos resultados promissores da arquitetura *Edge-Fog-Cloud* proposta, esta pesquisa apresenta delimitações metodológicas que definem o seu escopo atual.

Primeiramente, ao transpor estrategicamente o monitoramento analítico para a

interface N6 (após o desencapsulamento da UPF), o sistema perde visibilidade estrutural de ataques intra-túnel do tipo UE-to-UE (*User Equipment to User Equipment*), ou seja, ameaças que transitam exclusivamente dentro do núcleo celular e não desaguardam na rede externa (Internet).

Em segundo lugar, a avaliação experimental restringiu-se primariamente à emulação das variantes de inundação volumétrica da *botnet Mirai* e a anomalias específicas do *dataset Bot-IoT*, exigindo validações futuras contra Ameaças Persistentes Avançadas (APTs) mais furtivas. Ademais, embora o gerador estocástico preserve o envelope físico e temporal das inundações, o *framework* foi validado em um *testbed* que utiliza uma Rede de Acesso de Rádio (RAN) simulada via *software* (UERANSIM). Consequentemente, o impacto prático de variáveis do mundo real, como a interferência física de rádio, o desvanecimento de canal (*fading*) e a latência de *handover* na extração das características volumétricas, permanece um desafio em aberto.

Por fim, não foram avaliadas estratégias de resposta automática e reconfiguração dinâmica em malha fechada (*closed-loop*) para o bloqueio de fluxos diretamente na UPF, nem a sobrecarga de orquestração gerada pelo escalonamento da AnLF em cenários de nuvem de borda (*MEC*) contendo múltiplas UPFs distribuídas operando de forma simultânea.

Adicionalmente, em consonância com desafios amplamente documentados na literatura de redes móveis, registra-se como limitação a ausência de uma caracterização formal da carga de trabalho (*traffic workload*). Em virtude da escassez de conjuntos de dados 5G públicos com tráfego de fundo (*background traffic*) real e da complexidade de modelar matematicamente a concorrência de milhares de dispositivos heterogêneos (como em um *Smart Campus* em horário de pico), os experimentos no *testbed* concentraram-se na injeção estocástica controlada das classes de interesse, sem a sobreposição de matrizes formais de tráfego concorrente de larga escala.

6.2 Trabalhos Futuros

A continuidade desta linha de pesquisa permite a exploração de diversas frentes de maturidade técnica e científica. No âmbito da arquitetura e integração de rede, vislumbra-se a implementação de um ciclo de resposta automatizado (*closed-loop*). Essa evolução integraria mecanismos de mitigação dinâmica, como a quarentena de fluxos via *firewall* de Borda ou a reconfiguração autônoma de fatias de rede (*Network Slicing*), acionados a partir dos vereditos da AnLF, concretizando o paradigma *Detect-Decide-Act*. Aliada a essa automação, destaca-se a importância de conduzir testes de escalabilidade em topologias massivas, mensurando o impacto da contenção sob múltiplos saltos de UPF (*User Plane Function*) e quantificando o consumo energético do classificador em plataformas de *hardware* dedicadas.

No que tange ao aprimoramento dos algoritmos de *Machine Learning*, investigações futuras devem priorizar a capacidade de generalização frente a novas arquiteturas de *malware*. É fundamental expandir o escopo analítico para englobar famílias de *botnets* contemporâneas e modulares, a exemplo de *Gafgyt* e *Mozi*, avaliando a resiliência do vetor de *features* sob tráfego nativamente criptografado. Adicionalmente, recomenda-se submeter o classificador a ataques adversariais (*Adversarial Machine Learning*) projetados especificamente para evadir a fronteira de decisão, fomentando o desenvolvimento de métodos de treinamento robustos contra a perturbação de dados.

Por fim, para suportar a natureza capilarizada e de altíssima densidade do ecossistema 5G mMTC, recomenda-se a investigação do paradigma de Aprendizado Federado (*Federated Learning*). A adoção dessa arquitetura de consenso permitiria que múltiplos nós distribuídos na camada de Névoa colaborassem no refinamento contínuo dos limiares do modelo, sem a exigência de exfiltrar o tráfego sensível dos usuários para a nuvem. Tal abordagem não apenas fortaleceria a privacidade (*privacy-preserving*), mas também elevaria a adaptabilidade do sistema contra mudanças estocásticas abruptas nos padrões da rede (*concept drift*).

REFERÊNCIAS

- 1 3GPP. **5G System Overview**. Disponível em:
<https://www.3gpp.org/technologies/5g-system-overview>. Acesso em: 27 abr. 2026.
- 2 3GPP. **TS 23.401: General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access**. Versão 17.5.0, Release 17. Sophia Antipolis, France: 3rd Generation Partnership Project, 2023.
- 3 3GPP. **TS 23.288: Architecture enhancements for 5G System (5GS) to support network data analytics services**. Versão 17.4.0, Release 17. 3rd Generation Partnership Program (3GPP), 2023.
- 4 3GPP. **TS 23.501: System architecture for the 5G System (5GS); Stage 2**. Versão 18.2.0, Release 18. Sophia Antipolis, France: 3rd Generation Partnership Project, 2023.
- 5 3GPP. **TS 29.281: General Packet Radio System (GPRS) Tunnelling Protocol User Plane (GTPv1-U)**. Versão 17.5.0, Release 17. Sophia Antipolis, France: 3rd Generation Partnership Project, 2023.
- 6 3GPP. **TS 29.500: 5G System; Technical Realization of Service Based Architecture; Stage 3**. Versão 17.7.0, Release 17. Sophia Antipolis, France: 3rd Generation Partnership Project, 2022.
- 7 ADAS, A. Traffic models in broadband networks. **IEEE Communications Magazine**, v. 35, n. 7, p. 82–89, 1997.
- 8 AFOLABI, I. *et al.* Network Slicing and Softwarization: A Survey on Principles, Enabling Technologies, and Solutions. **IEEE Communications Surveys & Tutorials**, v. 20, n. 3, p. 2429–2453, 2018.
- 9 AKPAKWU, G. A. *et al.* A survey on 5G networks for the Internet of things: Communication technologies and challenges. **IEEE Access**, v. 5, p. 3619–3647, 2017.
- 10 ALMIANI, Hasan; ALDHYANI, Turki H. Botnet Attack Detection by Using CNN-LSTM Model for Internet of Things Applications. **Security and Communication Networks**, v. 2021, p. 1–23, 2021. DOI: 10.1155/2021/3806459.
- 11 ALPAYDIN, E. **Introduction to machine learning**. 4. ed. Cambridge, MA: MIT press, 2020.
- 12 ANDREWS, J. G. *et al.* What Will 5G Be?. **IEEE Journal on Selected Areas in Communications**, v. 32, n. 6, p. 1065–1082, 2014. DOI: 10.1109/JSAC.2014.2328098.
- 13 ANTONAKAKIS, Manos *et al.* Understanding the Mirai Botnet. In: 26th USENIX Security Symposium (USENIX Security 17), 2017. **Proceedings....** USENIX Association, p. 1093–1110.
- 14 ARJOVSKY, M.; CHINTALA, S.; BOTTOU, L. Wasserstein GAN. In: INTERNATIONAL CONFERENCE ON MACHINE LEARNING (ICML), 34., 2017, Sydney. **Proceedings [...]**. Brookline: PMLR, 2017. p. 214–223.

- 15 ARMBRUST, M. *et al.* A view of cloud computing. **Communications of the ACM**, v. 53, n. 4, p. 50–58, 2010.
- 16 ARP, D. *et al.* Dos and don'ts of machine learning in computer security. In: **31st USENIX Security Symposium (USENIX Security 22)**. Boston, MA: USENIX Association, 2022. p. 3971–3988.
- 17 AWOTUNDE, Joseph Bamidele *et al.* A Multi-level Random Forest Model-Based Intrusion Detection Using Fuzzy Inference System for Internet of Things Networks. **International Journal of Computational Intelligence Systems**, v. 16, n. 1, p. 31, 2023. DOI: 10.1007/s44196-023-00205-w.
- 18 BISHOP, Christopher M. **Pattern Recognition and Machine Learning**. New York: Springer, 2006.
- 19 BONOMI, F. *et al.* Fog computing and its role in the Internet of things. In: **Proceedings of the first edition of the MCC workshop on Mobile cloud computing**. Helsinki, Finland: ACM, 2012. p. 13–16.
- 20 BOVENZI, G.; CIUONZO, D.; PULIAFITO, V.; PESCAPÉ, A. A hierarchical distributed intrusion detection system for Internet of Things. **IEEE Internet of Things Journal**, v. 7, n. 7, p. 5841–5852, 2020. DOI: 10.1109/JIOT.2019.2958741.
- 21 BREIMAN, Leo. Random Forests. **Machine Learning**, v. 45, p. 5–32, 2001. Springer. DOI: 10.1023/A:1010933404324.
- 22 BROWN, Gabriel. **Service-Based Architecture for 5G Core Networks**. A Heavy Reading White Paper. Londres, 2017.
- 23 CHAABOUNI, Nadia; MOSBAH, Mohamed; ZEMMARI, Akka; SAUVIGNAC, Cyrille; FARUKI, Parvez. Network Intrusion Detection for IoT Security Based on Learning Techniques. **IEEE Communications Surveys & Tutorials**, v. 21, n. 3, p. 2671–2701, 2019.
- 24 CHOUMAN, A.; MANIAS, D. M.; SHAMI, A. Towards supporting intelligence in 5G/6G core networks: NWDAF implementation and initial analysis. In: **2022 IEEE International Conference on Communications (ICC)**. [S.l.]: IEEE, 2022. p. 1–6.
- 25 COLAKOVIĆ, A.; HADŽIALIĆ, M. Internet of Things (IoT): A review of enabling technologies, challenges, and open research issues. **Computers&Networks**, v. 144, p. 17–39, 2018. DOI: 10.1016/j.comnet.2018.07.016.
- 26 EMMERICH, P. *et al.* MoonGen: A scriptable high-speed packet generator. In: Internet MEASUREMENT CONFERENCE, 2015, Nova York. **Proceedings [...]**. Nova York: ACM, 2015. p. 275–287.
- 27 ENGELEN, G.; RIMMER, V.; JOOSEN, W. Troubleshooting an intrusion detection dataset: the CICIDS2017 case. In: **2021 IEEE Security and Privacy Workshops (SPW)**. San Francisco, CA: IEEE, 2021. p. 7–12.
- 28 FAWCETT, T. An introduction to ROC analysis. **Pattern Recognition Letters**, v. 27, n. 8, p. 861–874, 2006.

- 29 FROST, Victor S.; MELAMED, Benjamin. Traffic modeling for telecommunications networks. **IEEE Communications Magazine**, v. 32, n. 3, p. 70-81, 1994.
- 30 GEIRHOS, R. et al. Shortcut learning in deep neural networks. **Nature Machine Intelligence**, London, v. 2, n. 11, p. 665–673, 2020.
- 31 GOSHI, E.; MEHMETI, F.; LA PORTA, T. F.; KELLERER, W. Modeling and analysis of mMTC traffic in 5G core networks. **IEEE Transactions on Network and Service Management**, v. 22, n. 1, p. 409–425, 2025. DOI: 10.1109/TNSM.2024.3481240.
- 32 GÜNGÖR, A. **UERANSIM: Open source 5G UE and RAN (gNodeB) implementation**. GitHub, 2023. Disponível em: <<https://github.com/aligungr/UERANSIM>>. Acesso em: 30 abr. 2026.
- 33 HABIBZADEH, H.; DINESH, K.; SHISHVAN, O. R.; BOGGIO-DANDRY, A.; SHARMA, G.; SOYATA, T. A survey of healthcare Internet of Things (HIoT): A clinical perspective. **IEEE Internet of Things Journal**, v. 7, p. 53–71, 2019. DOI: 10.1109/JIOT.2019.2939293.
- 34 HASTIE, T.; TIBSHIRANI, R.; FRIEDMAN, J. **The Elements of Statistical Learning: Data Mining, Inference, and Prediction**. 2. ed. Springer Science & Business Media, 2009.
- 35 HUGUENIN, Nathalie; HELMUS, Jonas; HOF, Hans-Joachim; HECKER, Arthur. DIoT: A Federated Self-learning Anomaly Detection System for IoT. *In: Proceedings of the 28th USENIX Security Symposium*, 2021. **Proceedings....** USENIX Association.
- 36 JACOBSON, V.; LERES, C.; MCCANNE, S. The tcpdump manual page. *Lawrence Berkeley Laboratory, Berkeley, CA*, v. 143, 1989.
- 37 JAMES, G.; WITTEN, D.; HASTIE, T.; TIBSHIRANI, R. *An introduction to statistical learning*. v. 112. Nova York: Springer, 2013.
- 38 JIN, Ding *et al.* SwiftIDS: Real-time intrusion detection system based on LightGBM and parallel intrusion detection mechanism. **Computers & Security**, v. 97, p. 101984, 2020. DOI: 10.1016/j.cose.2020.101984.
- 39 KE, Guolin; MENG, Qi; FINLEY, Thomas; WANG, Taifeng; CHEN, Wei; MA, Weidong; YE, Qiwei; LIU, Tie-Yan. LightGBM: A Highly Efficient Gradient Boosting Decision Tree. *In: Advances in Neural Information Processing Systems*, v. 30, 2017.
- 40 KHAN, R.; KUMAR, P.; JAYAKODY, D. N. K.; LIYANAGE, M. A Survey on Security and Privacy of 5G Technologies: Potential Solutions, Recent Advancements, and Future Directions. *IEEE Communications Surveys & Tutorials*, vol. 22, no. 1, pp. 196–248, 2020.
- 41 KIM, Y.-E.; KIM, M.-G.; KIM, H., “Detecting IoT Botnet in 5G Core Network Using Machine Learning,” *Computers, Materials & Continua*, vol. 72, no. 3, pp. 4467–4488, 2022.

- 42 KIM, Taeyun *et al.* An Implementation Study of Network Data Analytic Function in 5G. *In: 2022 IEEE International Conference on Consumer Electronics (ICCE)*, 2022, Las Vegas. **Proceedings....** IEEE, 2022. p. 1–3. DOI: 10.1109/ICCE53296.2022.9730290.
- 43 KOLIAS, C.; KAMBOURAKIS, G.; STAVROU, A.; VOAS, J. DDoS in the IoT: Mirai and Other Botnets. **Computer**, v. 50, n. 7, p. 80–84, 2017. DOI: 10.1109/MC.2017.201.
- 44 KONG, L. *et al.* Edge-Computing-Driven Internet of Things: A Survey. **ACM Computing Surveys**, v. 55, n. 8, p. 1–34, 2022.
- 45 LEFOANE, Moemedi; GHAFIR, Ibrahim; KABIR, Sohag; AWAN, Irfan-Ullah. Internet of Things botnets: A survey on Artificial Intelligence based detection techniques. **Journal of Network and Computer Applications**, [S. l.], v. 236, p. 104110, 2025.
- 46 LUNDBERG, Scott M; LEE, Su-In. A Unified Approach to Interpreting Model Predictions. *In: Advances in Neural Information Processing Systems*, v. 30. Curran Associates, Inc., 2017. p. 4765–4774.
- 47 MANIAS, D.; CHOUMAN, A.; SHAMI, A., “An NWDAF Approach to 5G Core Network Signaling Traffic: Analysis and Characterization,” *2022 IEEE Global Communications Conference (GLOBECOM)*, pp. 6001–6006, 2022.
- 48 NAVARRO-ORTIZ, J. *et al.* A survey on 5G usage scenarios and traffic models. **IEEE Communications Surveys & Tutorials**, v. 22, n. 2, p. 905-929, 2020.
- 49 NESHENKO, N. *et al.* Demystifying IoT Security: An Exhaustive Survey on IoT Vulnerabilities and a First Empirical Look on Internet-Scale IoT Exploitations. **IEEE Communications Surveys & Tutorials**, v. 21, n. 4, p. 2702–2733, 2019. DOI: 10.1109/COMST.2019.2910750.
- 50 NETO, Euclides Carlos Pinto; DADKHAH, Sajjad; FERREIRA, Raphael; ZOHOURIAN, Alireza; LU, Rongxing; GHORBANI, Ali A. CICIoT2023: A Real-Time Dataset and Benchmark for Large-Scale Attacks in IoT Environment. **Sensors**, v. 23, n. 13, p. 5941, 2023. MDPI. DOI: 10.3390/s23135941.
- 51 NEUPANE, B.; PERERA, I.; OBAIDAT, M. A. Explainable Intrusion Detection Systems (X-IDS): A Survey of Current Methods, Challenges, and Opportunities. **IEEE Access**, v. 10, p. 111246–111267, 2022. DOI: 10.1109/ACCESS.2022.3214812.
- 52 NGUYEN, V.-G. *et al.* SDN/NFV-Based Mobile Packet Core Network Architectures: A Survey. **IEEE Communications Surveys & Tutorials**, v. 19, n. 3, p. 1567–1602, 2017.
- 53 OLIVEIRA, L. A. **User Equipment Traffic Classification in the 5G Core**. 2025. 217 f. Dissertação (Mestrado em Ciência da Computação) – Universidade Federal de Juiz de Fora, Juiz de Fora, 2025.
- 54 OPEN5GS. **Open5GS: Open Source 5G Core Network**. 2023. Disponível em: <<https://open5gs.org/>>. Acesso em: 30 abr. 2026.

- 55 PAOLINI, E. *et al.*, “Real-Time Network Packet Classification Exploiting Computer Vision Architectures,” *IEEE Open Journal of the Communications Society*, vol. 5, pp. 1155–1166, 2024.
- 56 PATEROMICHELAKIS, Emmanouil *et al.* End-to-End Data Analytics Framework for 5G Architecture. **IEEE Access**, v. 7, p. 40295–40312, 2019. DOI: 10.1109/ACCESS.2019.2902984.
- 57 PEDREGOSA, F. *et al.*, “Scikit-learn: Machine Learning in Python,” *Journal of Machine Learning Research*, vol. 12, pp. 2825–2830, 2011.
- 58 PHAM, Q.-V. *et al.* A survey of multi-access edge computing in 5G and beyond: Fundamentals, technology integration, and state-of-the-art. **IEEE Access**, v. 8, p. 116974–117017, 2020.
- 59 POWERS, D. M. W. Evaluation: from precision, recall and F-measure to ROC, informedness, markedness and correlation. **Journal of Machine Learning Technologies**, v. 2, n. 1, p. 37–63, 2011.
- 60 SAFI, M. *et al.* Behavioural Monitoring and Security Profiling in the Internet of Things (IoT). In: 2021 IEEE 23rd International Conference on High Performance Computing & Communications, 2021. **Proceedings....** IEEE, 2021. p. 1203–1210.
- 61 SARKER, I. H. Machine learning: Algorithms, real-world applications and research directions. **SN Computer Science**, v. 2, n. 3, p. 1–21, 2021.
- 62 SEVGICAN, S. *et al.*, “Intelligent network data analytics function in 5G cellular networks using machine learning,” *Journal of Communications and Networks*, vol. 22, no. 3, pp. 269–280, 2020.
- 63 SHAFI, M. *et al.* 5G: A tutorial overview of standards, trials, challenges, deployment, and practice. **IEEE Journal on Selected Areas in Communications**, v. 35, n. 6, p. 1201–1221, 2017.
- 64 SHI, W. *et al.* Edge Computing: Vision and Challenges. **IEEE Internet of Things Journal**, v. 3, n. 5, p. 637–646, 2016.
- 65 SICARI, Sabrina *et al.* Security, privacy and trust in Internet of Things: The road ahead. **Computer Networks**, v. 76, p. 146–164, 2015. DOI: 10.1016/j.comnet.2014.11.008.
- 66 SPEROTTO, A. *et al.*, “An Overview of IP Flow-Based Intrusion Detection,” *IEEE Communications Surveys & Tutorials*, vol. 12, no. 3, pp. 343–356, 2010.
- 67 THOMÉ, Thiago Goldoni. **Um estudo da arquitetura Edge-Fog-Cloud com foco na otimização distribuída do processamento e na redução da latência.** 2024. Dissertação (Mestrado em Ciência da Computação) – Instituto de Ciências Exatas, Universidade Federal de Juiz de Fora, Juiz de Fora, 2024.
- 68 TUSHIR, B. *et al.* The impact of DoS attacks on resource-constrained IoT devices: A study on the Mirai attack. **arXiv preprint arXiv:2104.09041**, 2021.

- 69 VUKOBRATOVIC, Dejan *et al.* Edge Machine Learning in 3GPP NB-IoT: Architecture, Applications and Demonstration. *In: 30th European Signal Processing Conference (EUSIPCO)*, 2022, Belgrade, Serbia. **Proceedings....** IEEE, 2022. p. 707–711.
- 70 WANG, M.; ZHENG, K.; YANG, Y.; WANG, X. An Explainable Machine Learning Framework for Intrusion Detection Systems. **IEEE Access**, v. 8, p. 73127–73141, 2020. DOI: 10.1109/ACCESS.2020.2988359.
- 71 XU, L. Da; HE, W.; LI, S. Internet of things in industries: A survey. **IEEE Transactions on Industrial Informatics**, v. 10, n. 4, p. 2233–2243, 2014. DOI: 10.1109/TII.2014.2309294.
- 72 YANG, Yi-Min; CHANG, Ko-Chin; LUO, Jia-Ning. Hybrid Neural Network-Based Intrusion Detection System: Leveraging LightGBM and MobileNetV2 for IoT Security. **Symmetry**, v. 17, n. 3, p. 314, 2025. DOI: 10.3390/sym17030314.
- 73 M. Zancanella, E. F. Silva, R. M. Peixoto, M. Stenner, and A. B. Vieira, “Machine Learning for Mirai Attack Detection in 5G-Enabled IoT Networks,” in *2025 13th Wireless Days Conference (WD)*, 2025, pp. 1–6.
- 74 ZHANG, Xiaolu; UPTON, Oren; BEEBE, Nicole; CHOO, Kim-Kwang Raymond. IoT Botnet Forensics: A Comprehensive Digital Forensic Case Study on Mirai Botnet Servers. **Forensic Science International: Digital Investigation**, v. 32, p. 300926, 2020. Elsevier.
- 75 ZOLOTUKHIN, M.; ZHANG, D.; HAMALAINEN, T.; MIRAGHAEI, P. On Attacking Future 5G Networks with Adversarial Examples: Survey. **Network**, v. 3, n. 1, p. 39–90, 2023.

APÊNDICE A – Descrição das *features* selecionadas

A Tabela 14 descreve as 11 características preditivas selecionadas após análise de correlação no conjunto CICIoT2023, além do atributo alvo utilizado somente nas etapas de treinamento e avaliação dos modelos Random Forest e LightGBM.

Tabela 14 – Conjunto final de 11 características preditivas e atributo alvo.

Atributo	Descrição
<code>flow_duration</code>	Duração total do fluxo em segundos. Diferencia fluxos curtos (ataques) de longos (benignos).
<code>Duration</code>	Tempo de vida do fluxo (alternativa/derivada de <code>flow_duration</code>).
<code>ack_count</code>	Número de pacotes com <i>flag</i> ACK. Fluxos legítimos apresentam valores consistentes.
<code>syn_count</code>	Número de pacotes com <i>flag</i> SYN. Detecta tentativas excessivas de abertura de conexões.
<code>urg_count</code>	Número de pacotes com <i>flag</i> URG. Raramente usado em tráfego legítimo.
<code>rst_count</code>	Número de pacotes com <i>flag</i> RST. Comum no encerramento limpo de conexões benignas.
<code>HTTP</code>	Indicador binário de tráfego HTTP. Diferencia tráfego web legítimo de tráfego malicioso.
<code>UDP</code>	Indicador binário de tráfego UDP. Essencial para detecção de Mirai-udpplain e GRE encapsulado.
<code>Min</code>	Menor tamanho de pacote no fluxo. Pacotes curtos são característicos de ataques de <i>flooding</i> .
<code>Covariance</code>	Covariância do tamanho dos pacotes no fluxo. Valores baixos sugerem repetição sistemática.
<code>Variance</code>	Variância do tamanho dos pacotes no fluxo. Fluxos benignos tendem a apresentar maior diversidade.
<code>label</code>	Rótulo da classe (Benign/Mirai-greeth/Mirai-greip/Mirai-udpplain). Usado somente em treinamento e avaliação.

Fonte: Elaborado pelo autor.

APÊNDICE B – Código-Fonte: Motor Estocástico de Geração de Tráfego (`synth_generator.py`)

Este apêndice detalha o *script* `synth_generator.py`, que consolida a arquitetura unificada para a emulação do tráfego benigno e das variantes da *botnet* Mirai (GRE-IP, GRE-ETH e UDP-Plain). A sua implementação substitui ferramentas estáticas de geração de pacotes por um modelo preditivo calibrável estruturado em Python.

Propósito, Funcionalidade e Tecnologias Empregadas: O motor foi desenvolvido para resolver a limitação da multiplicidade de fluxos e da intermitência frequentemente ignoradas em emulações 5G. O *script* modela o envelope temporal e volumétrico do ataque através de processos estocásticos complexos ancorados nas bibliotecas *NumPy* e *SciPy*. No que tange à dinâmica temporal, o algoritmo utiliza Cadeias de Markov (estados ON/OFF) combinadas com modelos autorregressivos AR(1) para reproduzir o comportamento de rajada (*bursts*) e os tempos de silêncio absolutos observados no tráfego IoT autêntico. Paralelamente, para definir a morfologia volumétrica, o gerador rejeita tamanhos estáticos de *payload*, recorrendo a amostragens contínuas a partir de Modelos de Misturas Gaussianas (GMM) e distribuições Log-Normal, o que permite ajustar matematicamente propriedades vitais do fluxo, como a Variância e o tamanho Mínimo (*Min*). Adicionalmente, para conferir realismo à topologia distribuída da ameaça, o código emula a multiplicidade de nós infectados através da geração de fluxos com diferentes endereços IP de origem, simulando a escala de uma verdadeira *botnet* e garantindo a paridade com a densidade da base *CICIOT2023*.

Disponibilidade do Código: O código-fonte completo está disponível para análise no repositório oficial da pesquisa e pode ser consultado diretamente através da URL, enquanto a raiz do projeto encontra-se hospedada em <https://github.com/MichaelZancanellaUFJF/ids-5g>.

APÊNDICE C – Código-Fonte: Injetor e Escalonador de Alta Fidelidade (`inject.py`)

Este apêndice descreve o *script* `inject.py`, responsável pela materialização física das matrizes estocásticas pré-calculadas e pela sua injeção direta no *testbed* 5G.

Propósito, Funcionalidade e Tecnologias Empregadas: A principal barreira tecnológica superada por este módulo é a garantia do rigor temporal. O envio de pacotes em interfaces virtuais (como a `uesimtun0` gerada pelo UERANSIM) recorrendo a funções de dormência triviais do sistema operacional sofre drásticas distorções, causadas pela preempção imprevisível (*jitter*) do *kernel*. Para assegurar que o *Inter-Arrival Time* (IAT) exigido pela calibração SHAP seja rigorosamente respeitado durante o disparo das inundações, este injetor implementa um escalonador atuando sobre *sockets* L3 nativos. Utilizando a biblioteca *Scapy* para a construção bruta dos cabeçalhos de rede e o relógio de *hardware* da CPU (através do método `time.perf_counter`), o algoritmo combina macro-dormências (*sleep*) com ciclos de espera ativa sub-milissegundo (*busy-wait*). Essa abordagem técnica contorna os estrangulamentos de *software* do hospedeiro e permite sustentar taxas de pacotes por segundo (PPS) constantes, permitindo que o tráfego a transitar pelas interfaces do núcleo 5G apresente fidelidade de cadência (*spacing*) das ameaças reais.

Disponibilidade do Código: O código-fonte relativo ao motor de injeção encontra-se devidamente versionado no repositório público do projeto e pode ser acessado pelo endereço <https://github.com/MichaelZancanellaUFJF/ids-5g>.

APÊNDICE D – Código-Fonte: Servidor de Inferência (`app.py`)

Este apêndice descreve o script `app.py`, que implementa o servidor de inferência do IDS, componente central da camada *Fog* na arquitetura proposta.

Propósito e Funcionalidade: Este script implementa uma API web utilizando o microframework Flask. Suas principais responsabilidades são:

- **Carregamento dos Modelos:** Ao iniciar, o servidor carrega em memória os modelos de Machine Learning (Random Forest e LightGBM) previamente treinados e salvos em arquivos `.pkl`.
- **Endpoint de Inferência (`/analytics`):** Expõe uma rota que recebe, via POST, um lote de fluxos de rede em formato JSON.
- **Pipeline de Validação e Limpeza:** Antes da inferência, o script executa um robusto pipeline de pré-processamento nos dados recebidos. Este pipeline garante a *paridade de esquema* com os dados de treinamento, tratando valores ausentes, convertendo tipos de dados e criando colunas faltantes com valores padrão. Essa etapa é crucial para a estabilidade do sistema em um ambiente de produção.
- **Endpoints Auxiliares:** Inclui uma rota `/data-report` para auditoria (armazenando o tráfego recebido) e uma rota `/health` para monitoramento da saúde do serviço.

Disponibilidade do Código: O código-fonte completo do servidor de inferência está disponível no repositório do projeto.

- **Link para o script:** <https://github.com/MichaelZancanellaUFJF/ids-5g>
- **Link para o repositório completo:** <https://github.com/MichaelZancanellaUFJF/ids-5g>

APÊNDICE E – Configuração Detalhada do Ambiente de Testes e Componentes 5G

Este apêndice consolida as especificações de *hardware*, *software* e as configurações dos principais componentes de rede utilizados no *testbed* 5G para a validação experimental desta dissertação.

Arquitetura do Testbed: A infraestrutura de virtualização foi segregada em três nós distintos para garantir o isolamento físico das funções de rede. A Tabela 15 detalha as especificações das máquinas virtuais, enquanto a Tabela 16 lista as versões das principais ferramentas de *software* empregadas no ambiente.

Tabela 15 – Especificações das Máquinas Virtuais (VMs) no Oracle VM VirtualBox.

Componente	Especificação
VM 1: Servidor IDS	
Papel	Análise de dados, API de inferência (Fog), InfluxDB e Grafana
Endereço IP	10.0.0.10
Sistema Operacional	Debian (64-bit)
Memória Principal	6937 MB
Armazenamento (HD)	80 GB
VM 2: Core 5G / Coletor	
Papel	Core 5G (Open5GS), captura e extração de <i>features</i>
Endereço IP	10.0.0.12
Sistema Operacional	Ubuntu (64-bit)
Memória Principal	2048 MB
Armazenamento (HD)	50 GB
VM 3: Cliente / Atacante	
Papel	Cliente 5G (UERANSIM) e geração de tráfego
Endereço IP	10.0.0.11
Sistema Operacional	Ubuntu (64-bit)
Memória Principal	2048 MB
Armazenamento (HD)	50 GB

Fonte: Elaborado pelo autor.

Tabela 16 – Versões das Ferramentas de Software Utilizadas.

Software	Versão
Open5GS	2.5.7
UERANSIM	v3.2.7

Fonte: Elaborado pelo autor.

Configuração dos Componentes 5G: As subseções seguintes detalham os parâmetros críticos utilizados nos arquivos YAML para orquestrar o núcleo móvel (Core) e a rádio (RAN) simulados.

Configuração do gNodeB (`open5gs-gnb.yaml`)

- **Identificadores de Rede:**
 - MCC (*Mobile Country Code*): '999'
 - MNC (*Mobile Network Code*): '70'
 - NCI (*NR Cell Identity*): '0x00000010'
 - Comprimento do ID NR: 32 bits
 - TAC (*Tracking Area Code*): 1
- **Endereços IP do gNB:**
 - IP para Simulação de Rádio (`linkIp`): 10.0.0.11
 - IP para Interface N2 (`ngapIp`): 10.0.0.11
 - IP para Interface N3 (`gtpIp`): 10.0.0.11
- **Segurança:**
 - Ordem dos algoritmos de integridade: [NIA1]
 - Ordem dos algoritmos de criptografia: [NEA1]

Configuração do User Equipment (`open5gs-ue.yaml`)

- **Identificadores do Assinante:**
 - SUPI (IMSI): 'imsi-999700000000002'
 - MCC: '999'
 - MNC: '70'
 - IMEI: '356930035643800'
 - IMEISV: '4370816125816151'
- **Configuração de Rede do UE:**
 - Máscara da interface TUN: '255.255.255.0'
 - Lista de gNBs para conexão: 10.0.0.11

Configuração da User Plane Function (`upf.yaml`)

- **Endereçamento do Plano de Usuário:**
 - IP da interface PFCP (Controle): `10.0.0.12`
 - IP da interface GTP-U (Dados/N3): `10.0.0.12`
- **Session (Sessão de Dados do Usuário):**
 - Sub-rede (IPv4) para UEs alocados: `10.45.0.0/16`
 - Gateway (IPv4): `10.45.0.1`
 - Interface TUN hospedeira: `ogstun`

Disponibilidade das Configurações: O conjunto completo de manifestos YAML estruturados para a topologia CUPS deste laboratório encontra-se versionado e disponível no repositório do projeto.

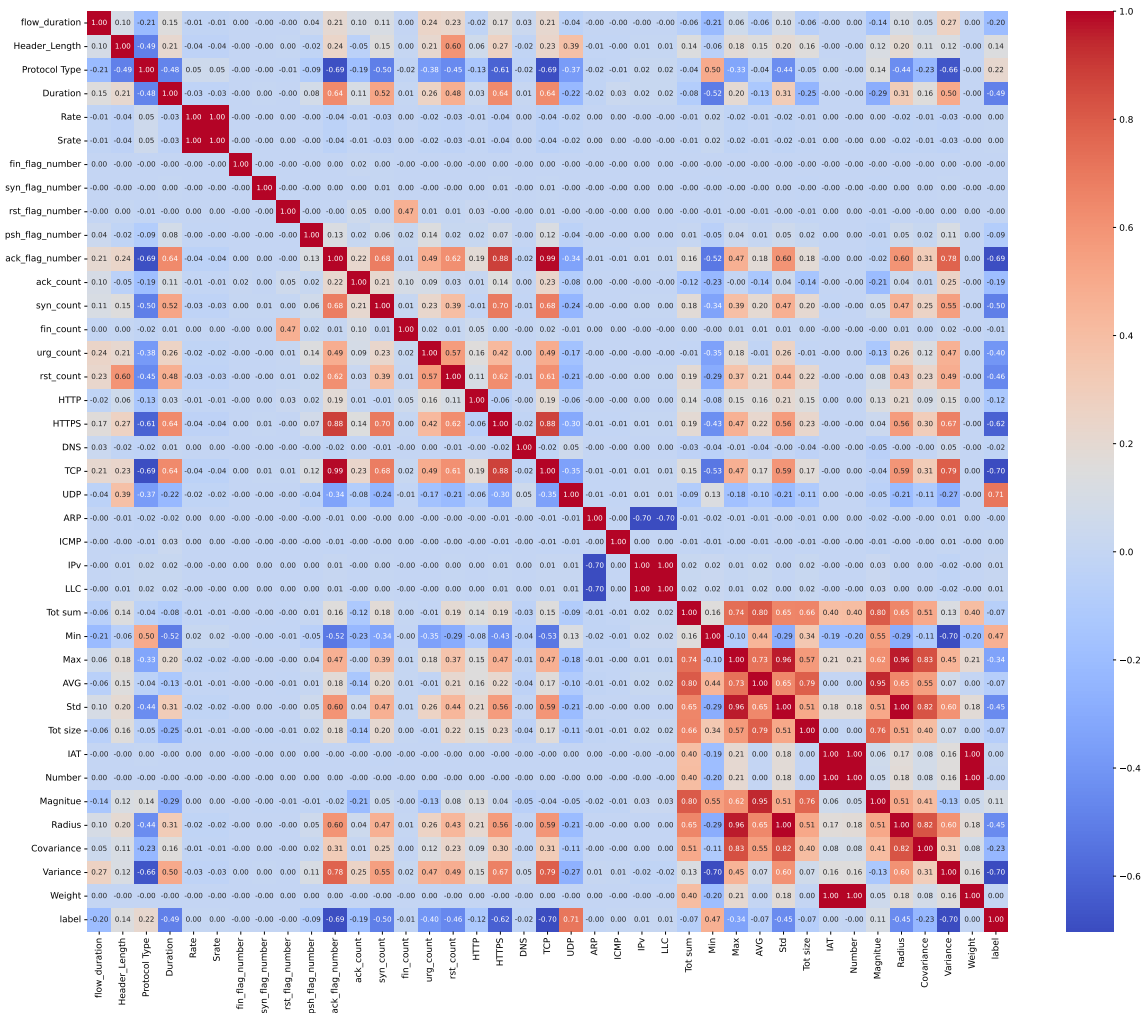
- **Link para o ambiente (*testbed*):** <https://github.com/MichaelZancanellaUFJF/ids-5g>

APÊNDICE F – Matrizes de Correlação Linear (Seleção de Atributos)

Este apêndice apresenta os mapas de calor (*heatmaps*) contendo as matrizes de correlação de Pearson, geradas durante a etapa de Engenharia de Atributos (*Feature Engineering*) para mitigar a multicolinearidade dos dados.

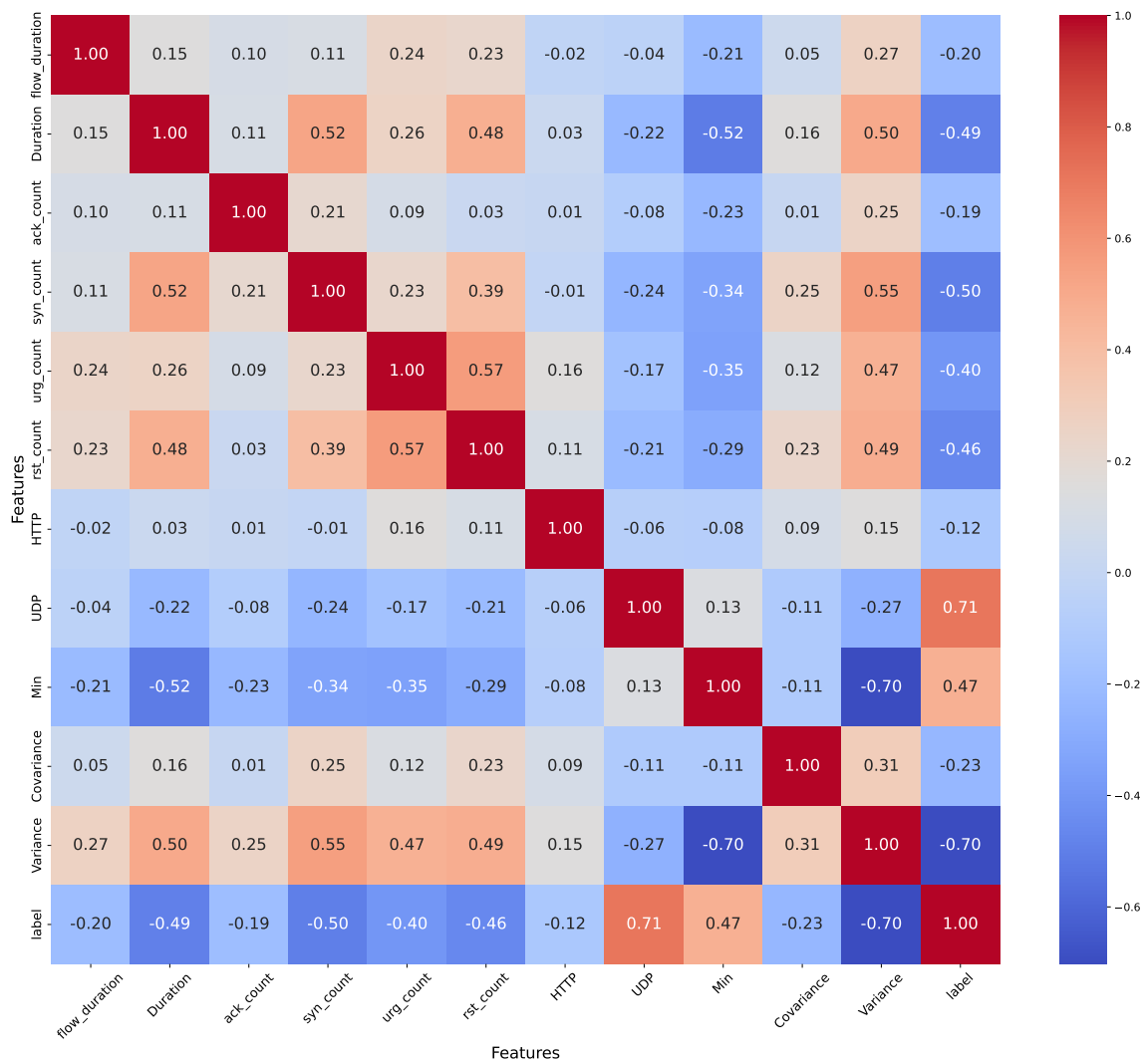
A Figura 19 ilustra o cenário inicial, demonstrando a elevada dependência linear entre diversas métricas de rede extraídas. A Figura 20 apresenta a matriz resultante após a aplicação rigorosa do filtro de exclusão (limiares de $|r| > 0,85$ e $|r| < 0,10$), consolidando o vetor final de 11 *features* preditivas de alta fidelidade utilizadas no treinamento dos modelos.

Figura 19 – Matriz de correlação inicial de Pearson antes da redução de dimensionalidade.



Fonte: Elaborado pelo autor.

Figura 20 – Matriz de correlação final com o subconjunto das 11 *features* preditivas.



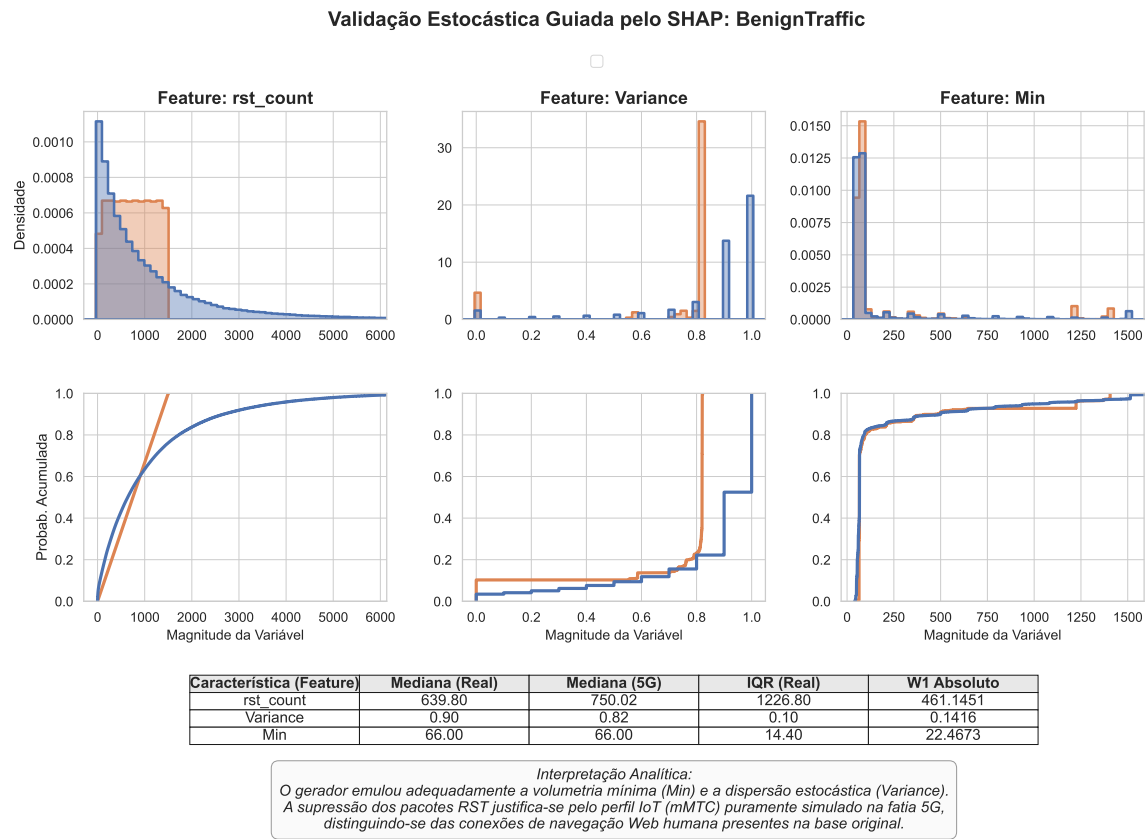
Fonte: Elaborado pelo autor.

APÊNDICE G – Validação Estocástica do Tráfego Sintético (XAI)

Este apêndice apresenta as evidências visuais da eficácia do motor de geração e calibração de tráfego, evidenciando a sobreposição estatística entre os dados originais da base *CICIoT2023* (tráfego real) e o tráfego sintético emulado no *testbed* 5G.

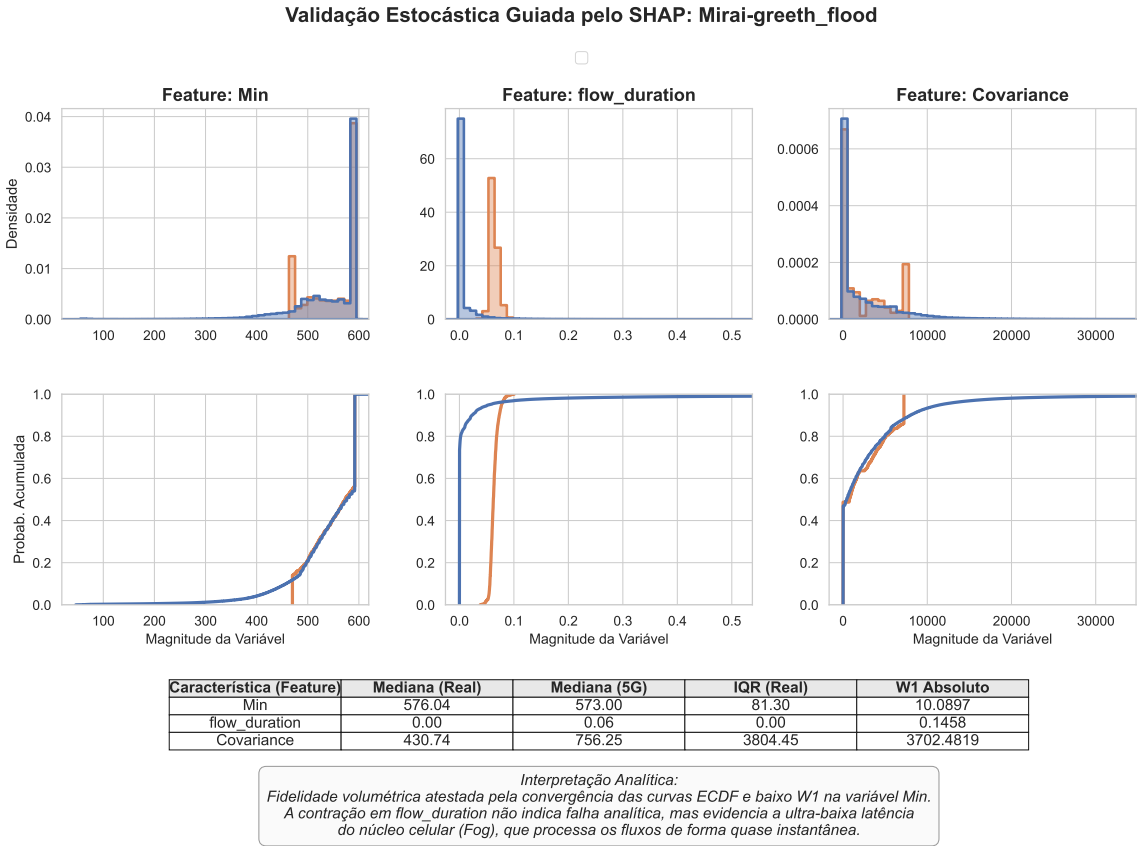
As figuras subsequentes ilustram as curvas de Densidade e de Probabilidade Acumulada (ECDF) para as características (*features*) de maior peso preditivo, definidas previamente pela análise de explicabilidade (SHAP). O alinhamento visual entre as curvas comprova a minimização da Distância de Wasserstein (W_1), garantindo a alta fidelidade física das amostras injetadas na camada de Névoa para o tráfego benigno e para as três variantes da *botnet* Mirai.

Figura 21 – Validação estocástica guiada pelo SHAP: Tráfego Benigno (*BenignTraffic*).



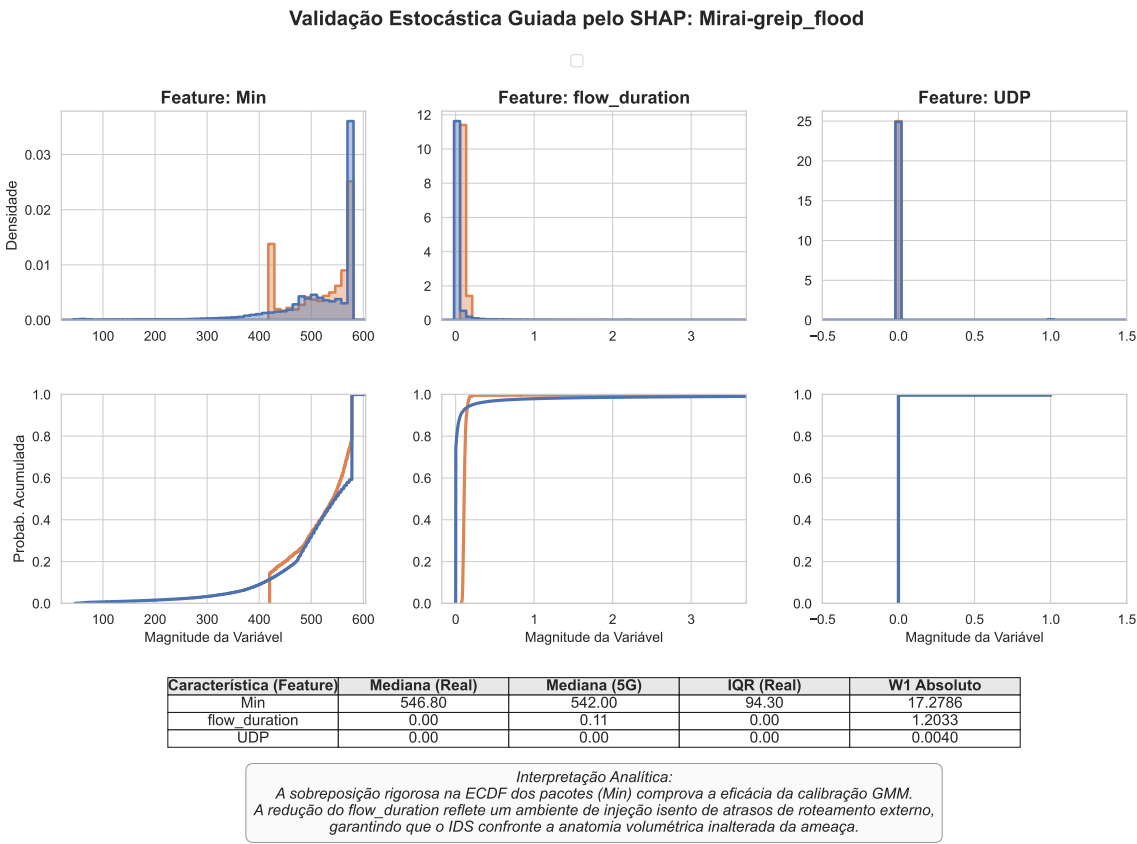
Fonte: Elaborado pelo autor.

Figura 22 – Validação estocástica guiada pelo SHAP: Inundação Mirai GRE-ETH.



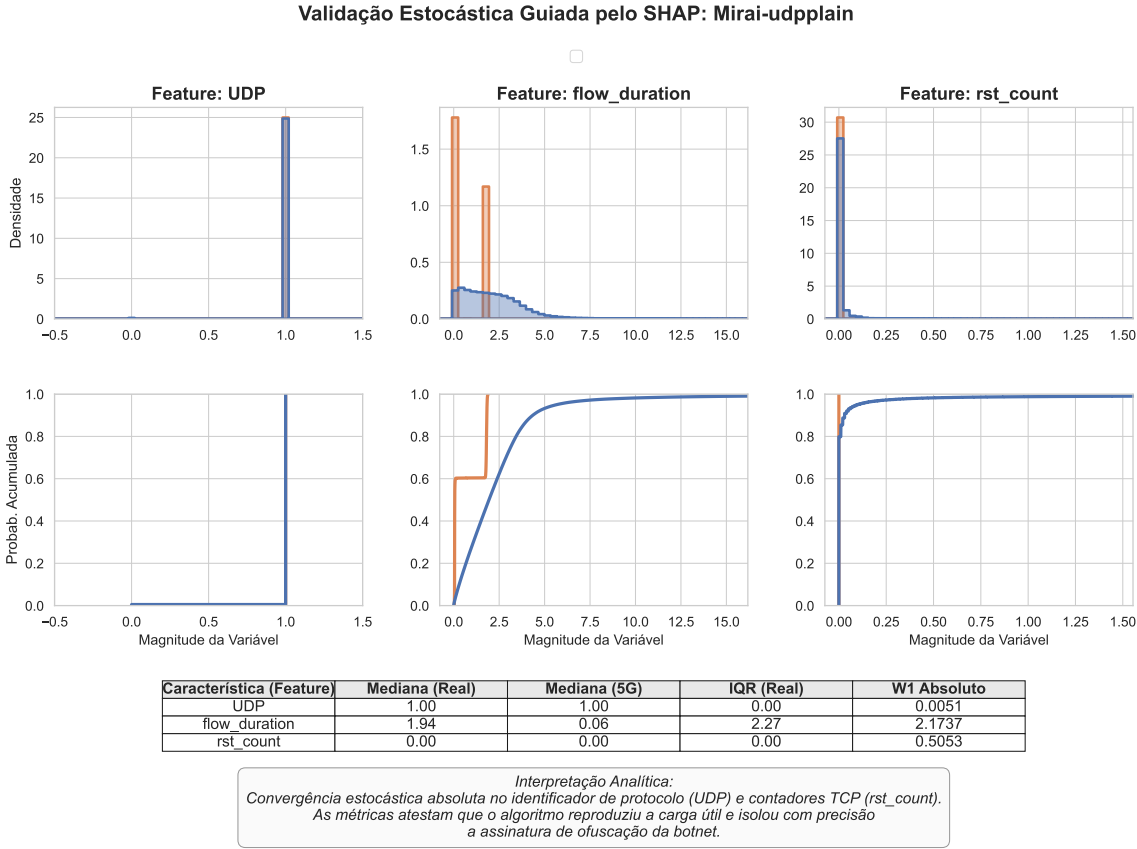
Fonte: Elaborado pelo autor.

Figura 23 – Validação estocástica guiada pelo SHAP: Inundação Mirai GRE-IP.



Fonte: Elaborado pelo autor.

Figura 24 – Validação estocástica guiada pelo SHAP: Inundação Mirai UDP-Plain.



Fonte: Elaborado pelo autor.