Detecção de Intrusão Através de Redes Neurais Profundas com Saídas Antecipadas para Inferência Rápida e Confiável

João Andre Simioni, Eduardo Kugler Viegas, Altair Olivo Santin, Pedro Horchulhack

Programa de Pós-Graduação em Informática - Pontifícia Universidade Católica do Paraná
{joao.asimioni, eduardo.viegas, santin, pedro.horchulhack}@ppgia.pucpr.br

SBSeg 2024
Simpósio Brasileiro em Segurança da Informação (SBSeg)

PUCPR

SecPLab
Disclosing your future needs for Security & Privacy

Agenda

- Introdução
- Proposta
- Pré-avaliação
- Implementação
- Avaliação
- Conclusões

Introdução

Contextualização - Dispositivos de IoT

PUCPR

SecPLab
Disclosing your future needs for Security & Privacy

Introdução

Contextualização - Dispositivos de IoT

NÚMERO CRESCENTE DE DISPOSITIVOS

PUCPR

SecPLab
Disclosing your future needs for Security & Privacy

Introdução

Contextualização - Dispositivos de IoT

NÚMERO CRESCENTE DE DISPOSITIVOS

PRINCIPAIS ALVOS DE CIBERATAQUES

PUCPR

SecPLab
Disclosing your future needs for Security & Privacy

Introdução

Contextualização - Dispositivos de IoT

- NÚMERO CRESCENTE DE DISPOSITIVOS
- PRINCIPAIS ALVOS DE CIBERATAQUES
- RECURSOS LIMITADOS

PUCPR

SecPLab
Disclosing your future needs for Security & Privacy

Introdução

Contextualização - Sistemas de Detecção de Intrusão de Rede (NIDS)

PUCPR

SecPLab
Disclosing your future needs for Security & Privacy

Introdução

Contextualização - Sistemas de Detecção de Intrusão de Rede (NIDS)

PUCPR

SecPLab
Disclosing your future needs for Security & Privacy

Introdução

Contextualização - Sistemas de Detecção de Intrusão de Rede (NIDS)

AQUISIÇÃO DE DADOS

PUCPR

SecPLab
Disclosing your future needs for Security & Privacy

Introdução

Contextualização - Sistemas de Detecção de Intrusão de Rede (NIDS)

AQUISIÇÃO DE DADOS

EXTRAÇÃO DE CARACTERÍSTICAS

PUCPR

SecPLab
Disclosing your future needs for Security & Privacy

Introdução

Contextualização - Sistemas de Detecção de Intrusão de Rede (NIDS)

AQUISIÇÃO DE DADOS

EXTRAÇÃO DE CARACTERÍSTICAS

CLASSIFICAÇÃO

PUCPR

SecPLab
Disclosing your future needs for Security & Privacy

Introdução

Contextualização - Sistemas de Detecção de Intrusão de Rede (NIDS)

AQUISIÇÃO DE DADOS

EXTRAÇÃO DE CARACTERÍSTICAS

CLASSIFICAÇÃO

ALERTA

PUCPR

SecPLab
Disclosing your future needs for Security & Privacy

Introdução

Contextualização - Sistemas de Detecção de Intrusão de Rede (NIDS)

AQUISIÇÃO DE DADOS

EXTRAÇÃO DE CARACTERÍSTICAS

CLASSIFICAÇÃO

ALERTA

PUCPR

SecPLab
Disclosing your future needs for Security & Privacy

Introdução

Contextualização - Desafios

Introdução

Contextualização - Desafios

DNNs: + ACURÁCIA + COMPLEXIDADE

Introdução

Contextualização - Desafios

DNNs: + ACURÁCIA + COMPLEXIDADE

ACURÁCIA ↑ CUSTO COMPUTACIONAL ↑

PUCPR

SecPLab

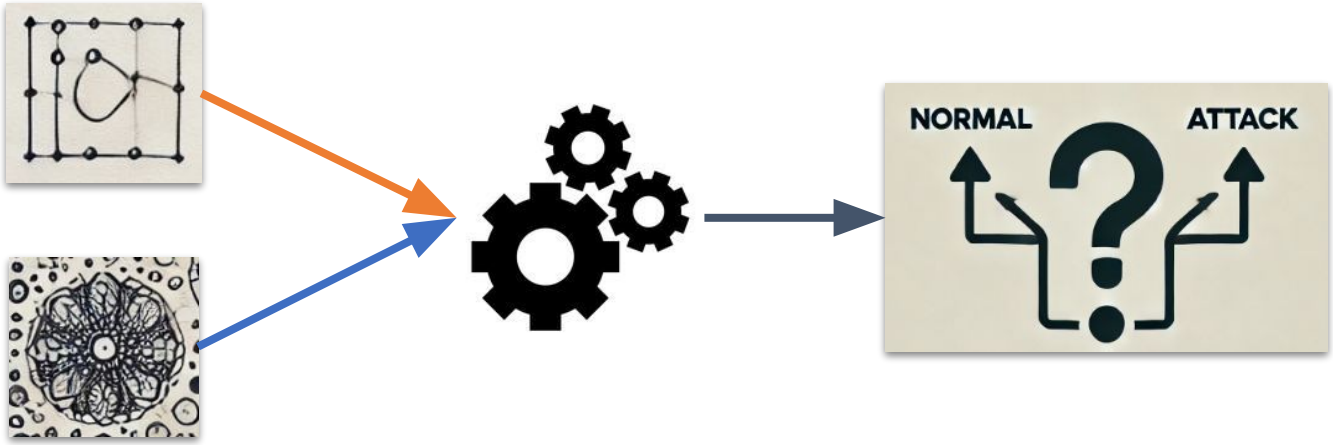
Disclosing your future needs for Security & Privacy

Introdução

Contextualização - Desafios

DNNs: + ACURÁCIA + COMPLEXIDADE

ACURÁCIA ↑ CUSTO COMPUTACIONAL ↑



PUCPR

SecPLab
Disclosing your future needs for Security & Privacy

Introdução

Contextualização - Desafios

DNNs: + ACURÁCIA + COMPLEXIDADE

ACURÁCIA ↑ CUSTO COMPUTACIONAL ↑

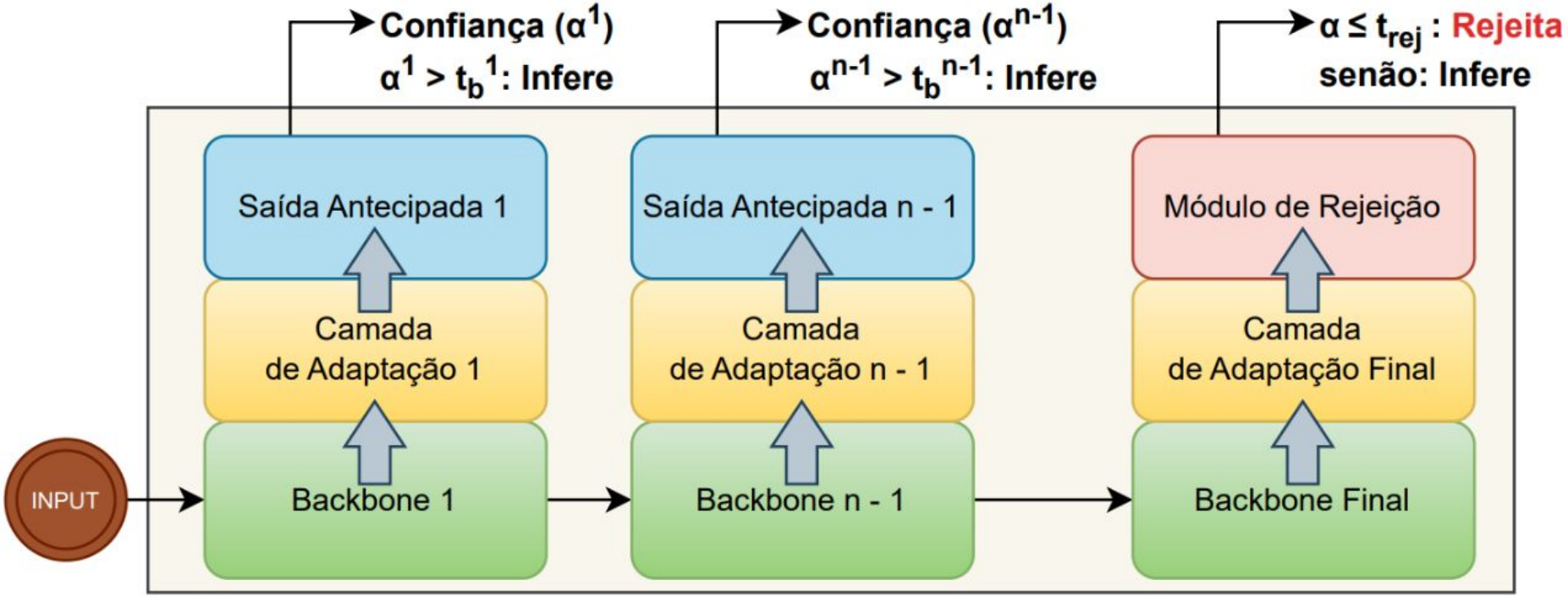
MESMO CUSTO
INDEPENDENTE DA ENTRADA

PUCPR

SecPLab
Disclosing your future needs for Security & Privacy

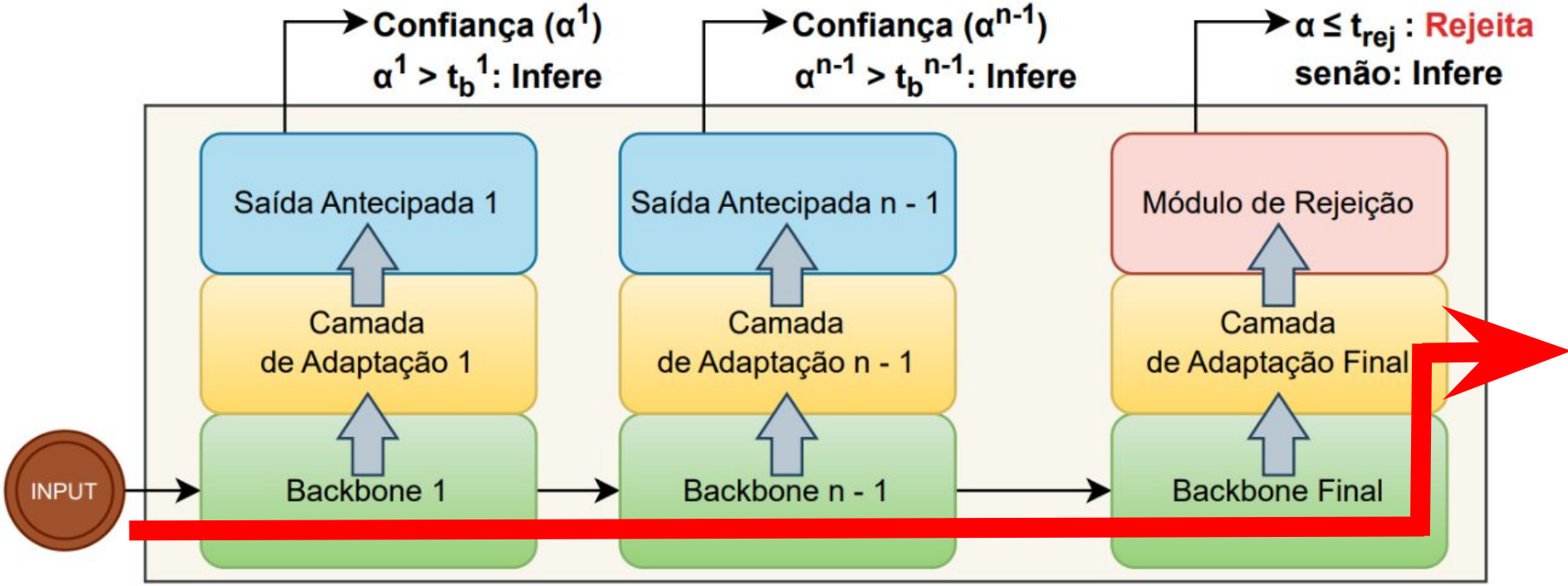
Introdução

Early Exits



Introdução

Early Exits



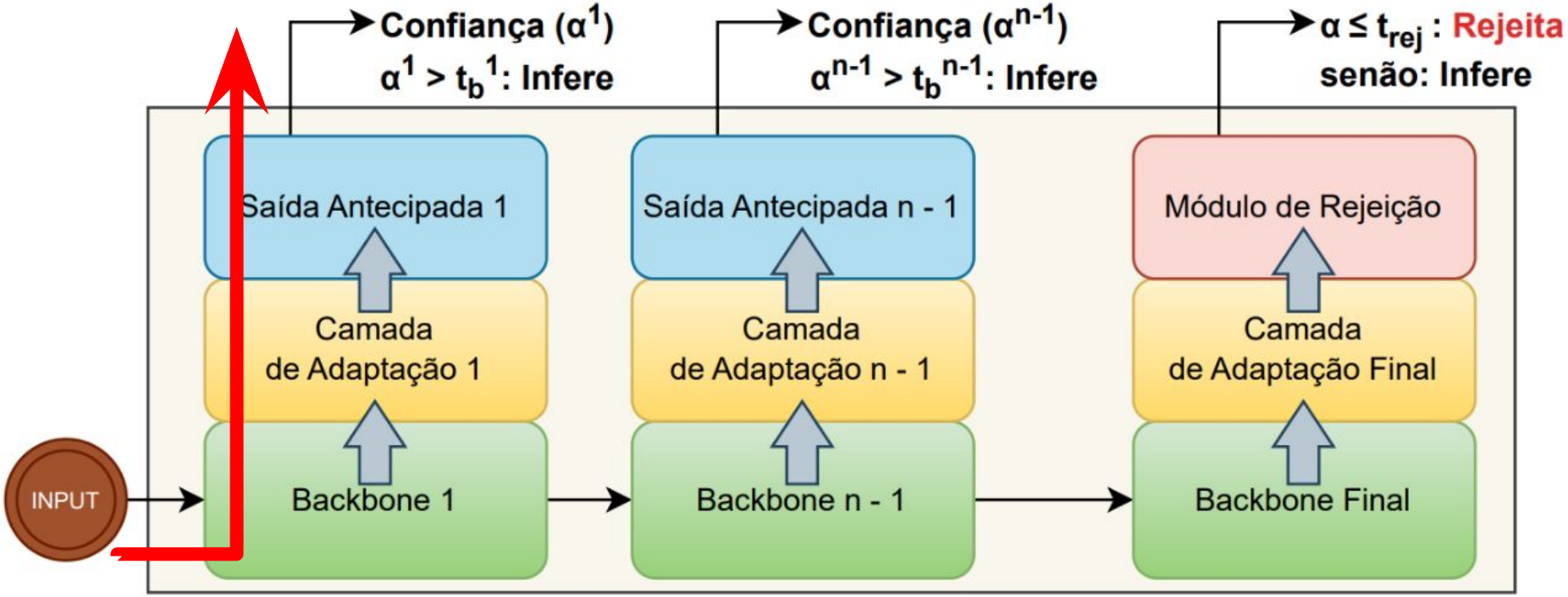
COMPORTAMENTO TRADICIONAL

PUCPR

SecPLab
Disclosing your future needs for Security & Privacy

Introdução

Early Exits



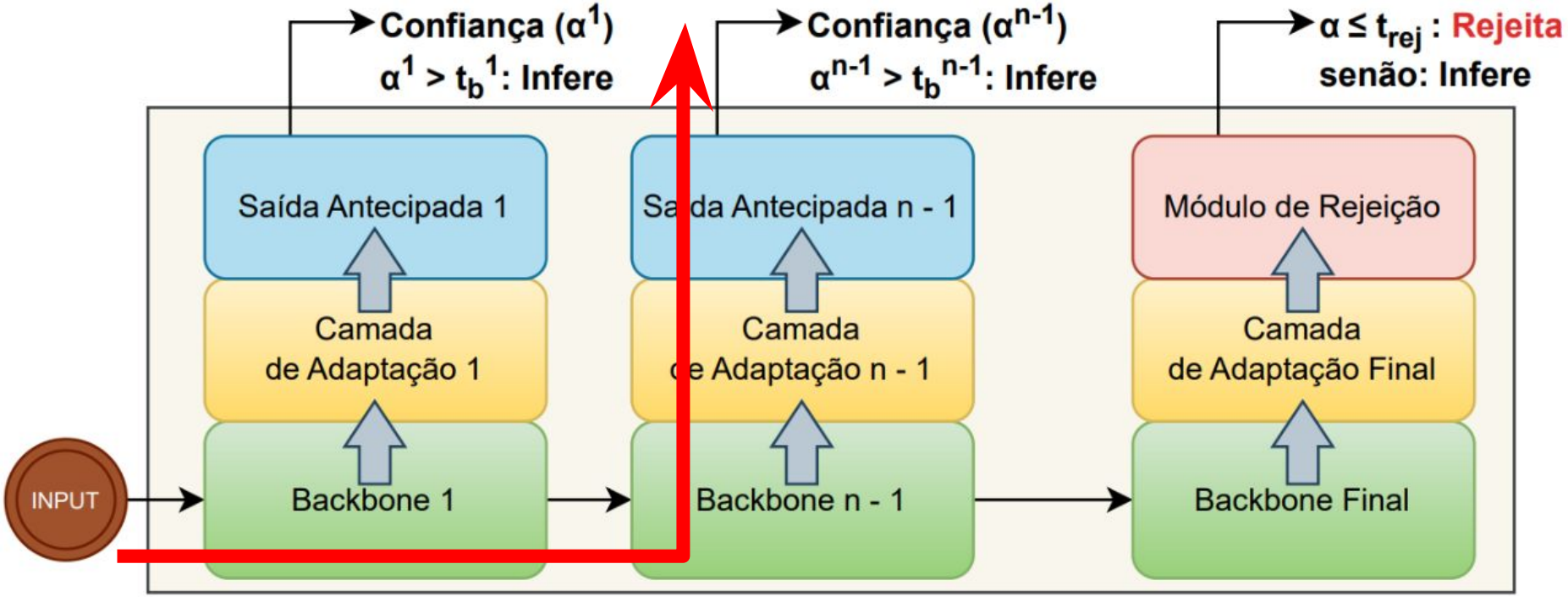
TESTANDO SAÍDA 1

PUCPR

SecPLab
Disclosing your future needs for Security & Privacy

Introdução

Early Exits



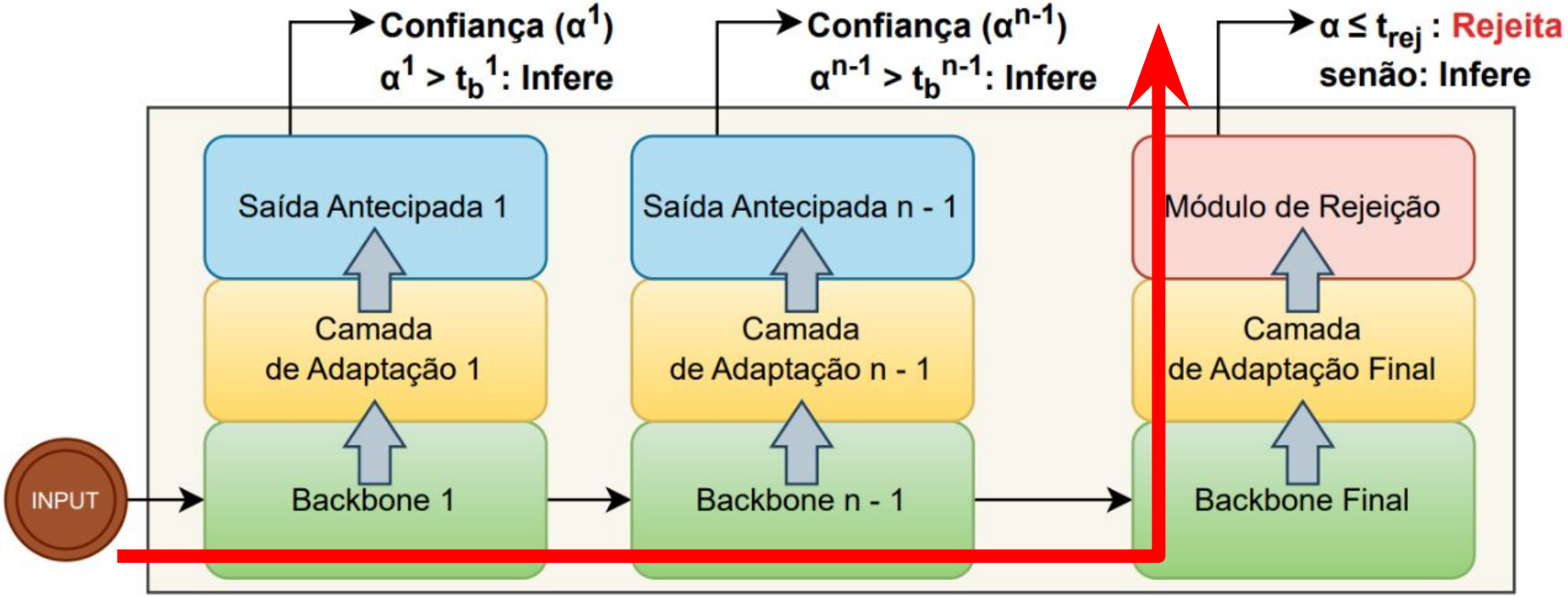
TESTANDO SAÍDA N - 1 (NÚMERO DE SAÍDAS É ESCOLHA DE PROJETO)

PUCPR

SecPLab
Disclosing your future needs for Security & Privacy

Introdução

Early Exits



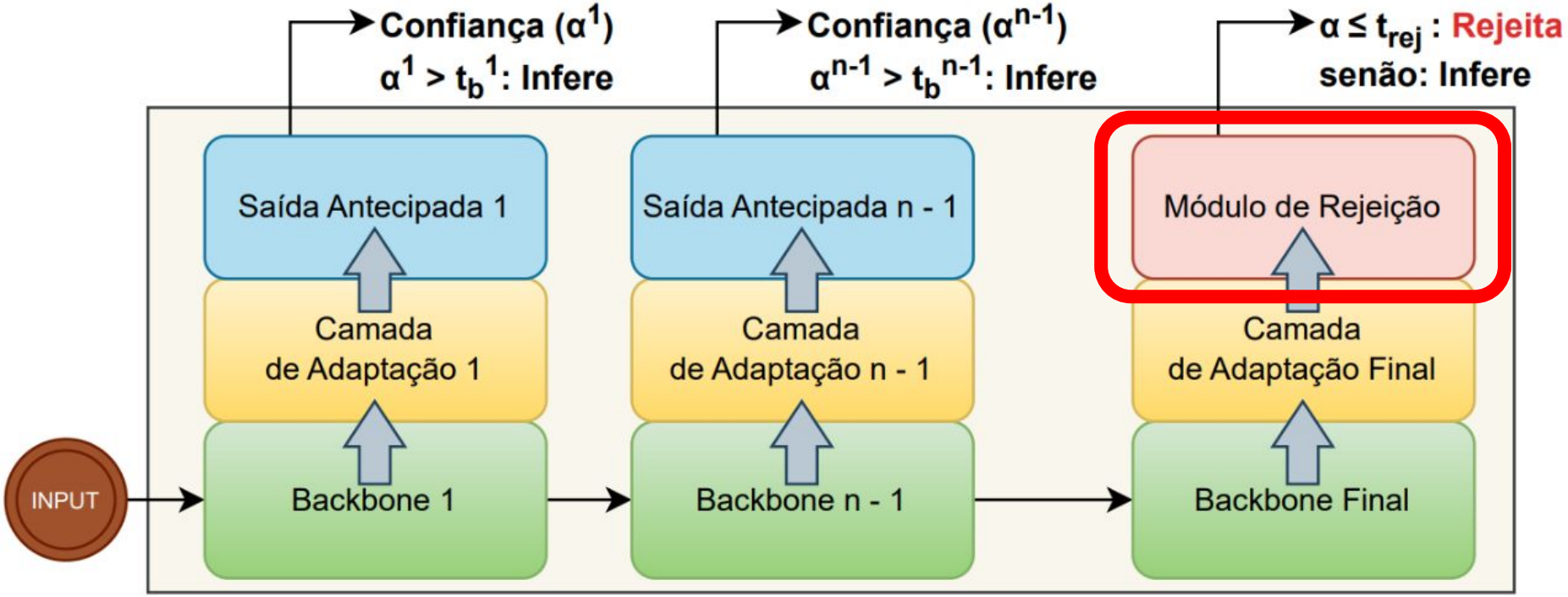
SE NENHUMA SAÍDA ACEITA, VAI PARA A ÚLTIMA

PUCPR

SecPLab
Disclosing your future needs for Security & Privacy

Introdução

Early Exits



MÓDULO DE REJEIÇÃO PODE DECIDIR NÃO CLASSIFICAR

PUCPR

SecPLab

Disclosing your future needs for Security & Privacy

Proposta

Dataset MAWIFlow

AQUISIÇÃO DE DADOS → **Samplepoint-F - MAWI**
Arquivos PCAP
Trânsito: Japão <-> EUA

EXTRAÇÃO DE CARACTERÍSTICAS → **58 Características Extraídas**
Dados Classificados

7.056.320 amostras - Jan - Dez / 2016

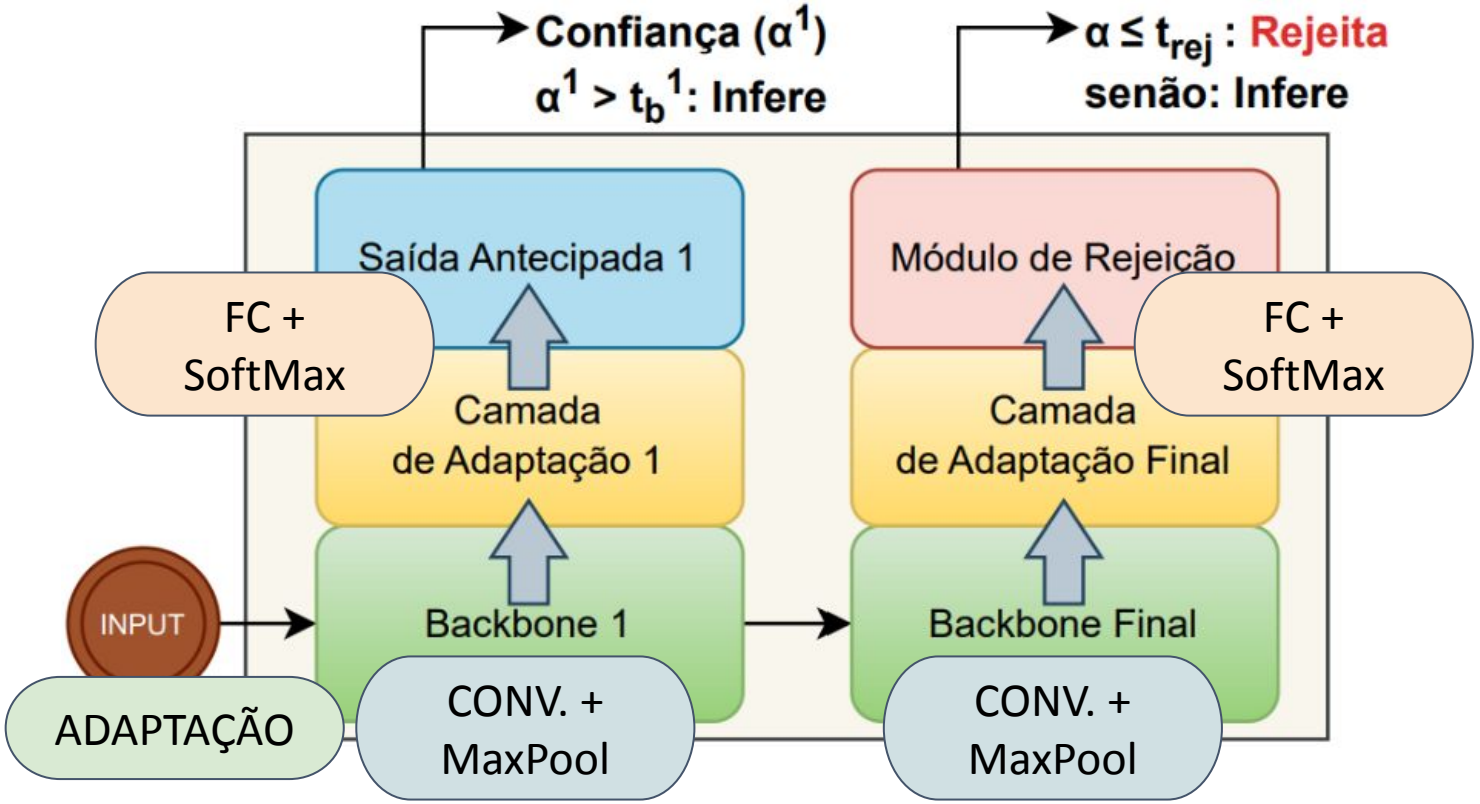
https://mawi.wide.ad.jp/mawi/

PUCPR

SecPLab
Disclosing your future needs for Security & Privacy

Proposta

AlexNet com uma saída antecipada e módulo de rejeição



PUCPR

SecPLab

Disclosing your future needs for Security & Privacy

Avaliação

Arquitetura Tradicional

EVENTOS POR SEGUNDO

RASPBERRY PI 3	DESKTOP CPU	DESKTOP GPU
7,36	247,34	17.609

PUCPR

SecPLab

Disclosing your future needs for Security & Privacy

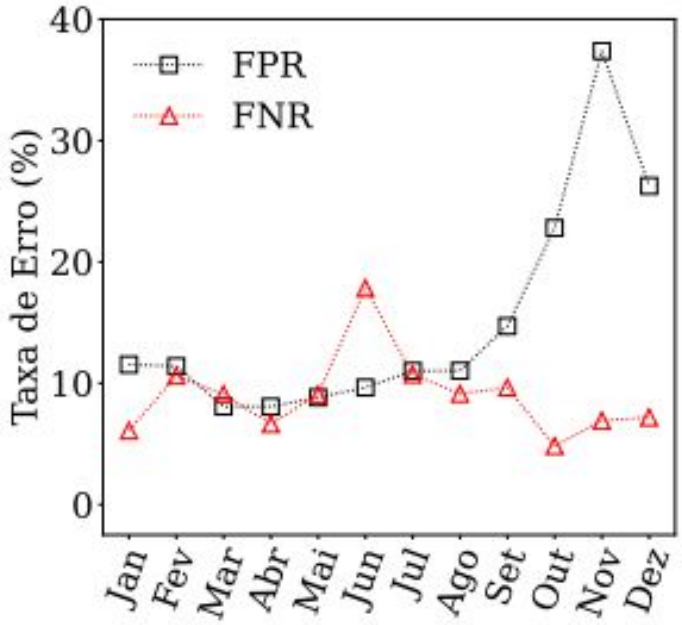
Avaliação

Arquitetura Tradicional

EVENTOS POR SEGUNDO

RASPBERRY PI 3	DESKTOP CPU	DESKTOP GPU
7,36	247,34	17.609

TAXA DE ERRO FPR / FNR MÊS A MÊS



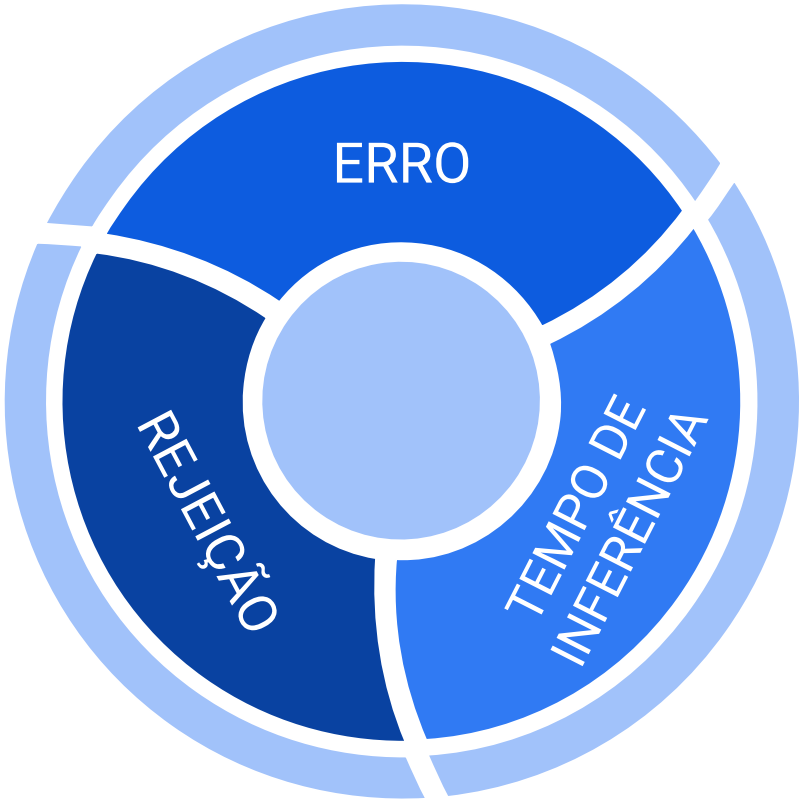
PUCPR

SecPLab

Disclosing your future needs for Security & Privacy

Implementação

Otimização multi-objetivo

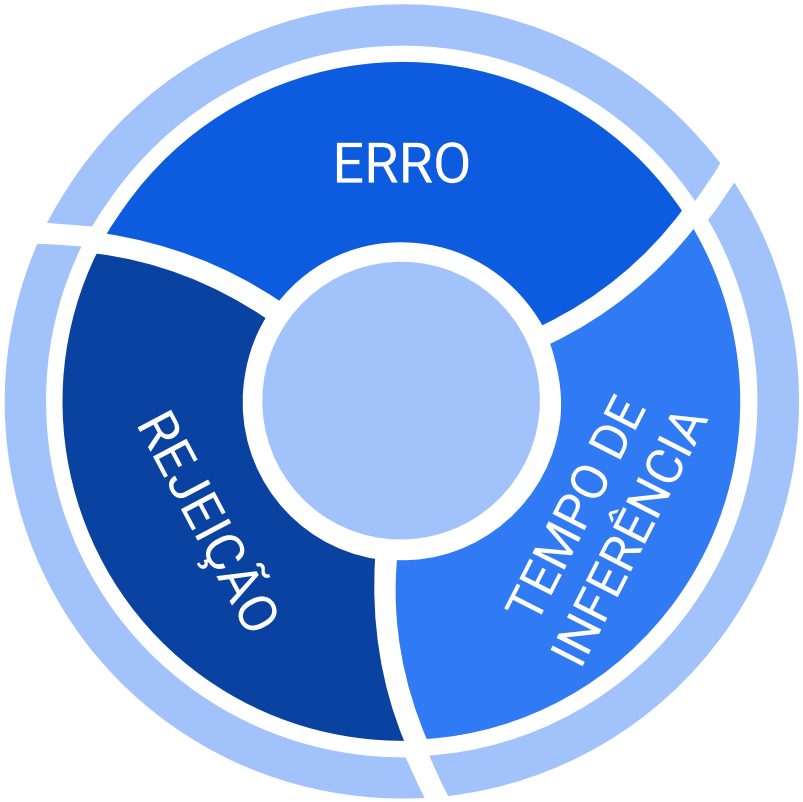


PUCPR

SecPLab
Disclosing your future needs for Security & Privacy

Implementação

Otimização multi-objetivo



SAÍDAS ANTECIPADAS

↑ ERRO ↓ TEMPO

- Threshold ataque saída 1
- Threshold normal saída 1

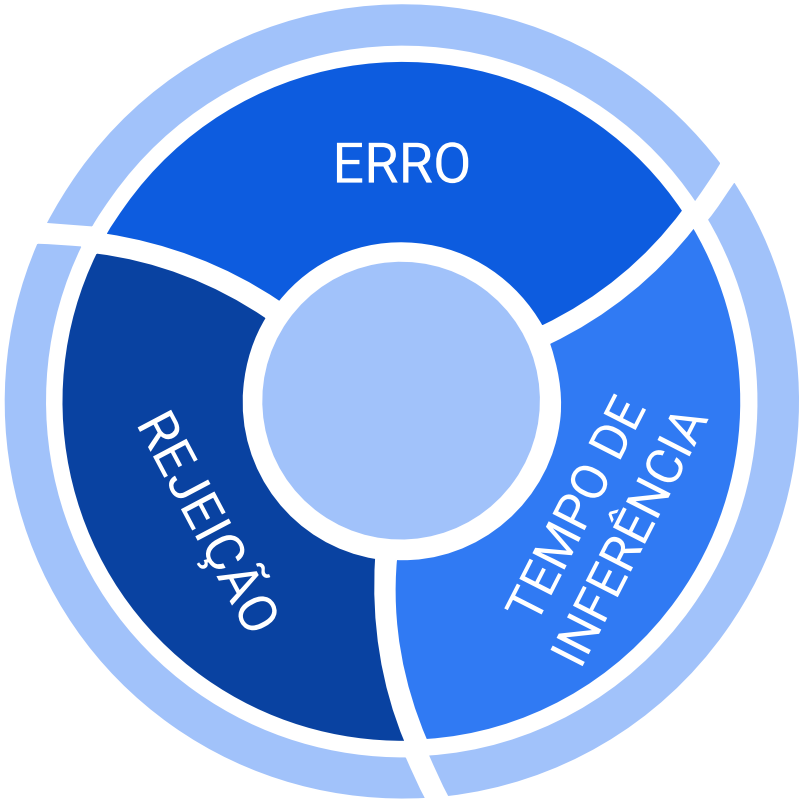
PUCPR

SecPLab

Disclosing your future needs for Security & Privacy

Implementação

Otimização multi-objetivo



SAÍDAS ANTECIPADAS
↑ ERRO ↓ TEMPO

- Threshold ataque saída 1
- Threshold normal saída 1

SAÍDA FINAL
↑ REJEIÇÃO ↓ ERRO

- Threshold ataque saída 2
- Threshold normal saída 2

PUCPR

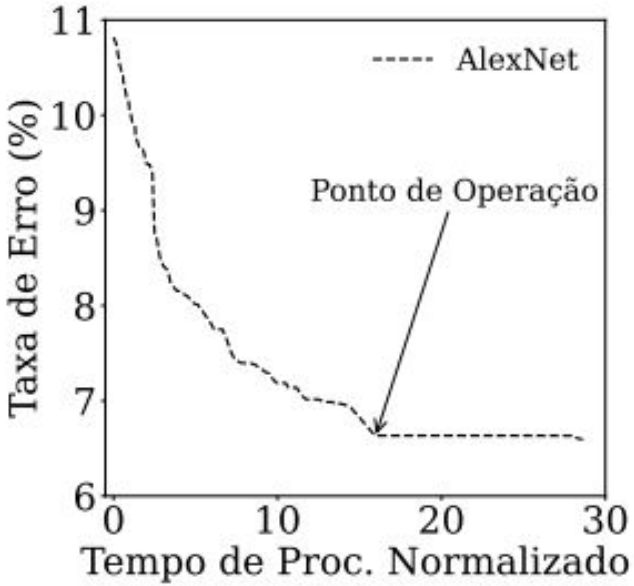
SecPLab
Disclosing your future needs for Security & Privacy

Implementação

Otimização multi-objetivo - Ponto de Operação

Rejeição Máxima: 90% (Fixo)

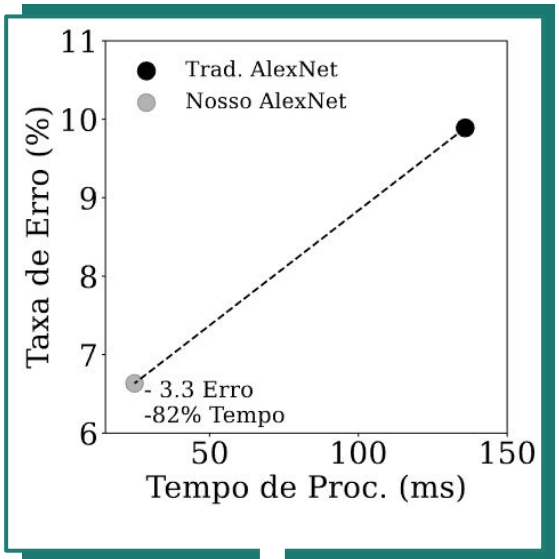
Ponto de operação:
- **Definido pelo operador**
- **Trade-off entre Erro e Tempo**



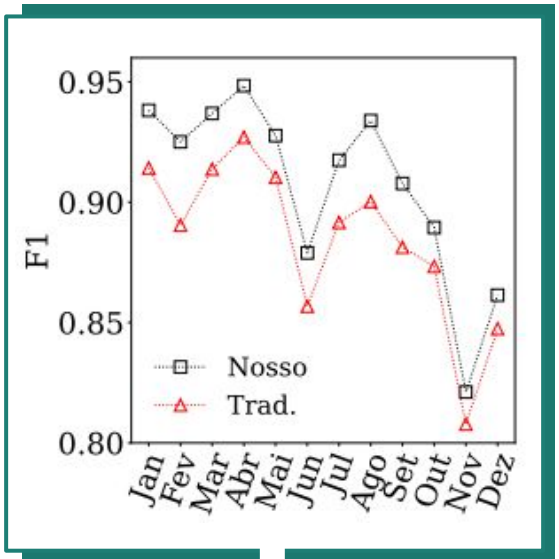
PUCPR

SecPLab
Disclosing your future needs for Security & Privacy

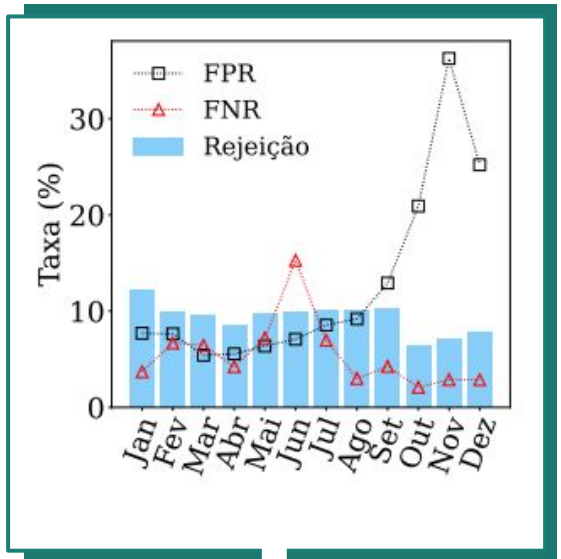
Avaliação



MELHORIAS



COMPARAÇÃO SCORE F1 NO TEMPO



TAXAS DE ERRO E REJEIÇÃO NO TEMPO

PUCPR

SecPLab
Disclosing your future needs for Security & Privacy

Conclusões

- **Desafios do NIDS em IoT**: Dificuldades em detecções confiáveis devido a altos requisitos de processamento e mudanças no comportamento do tráfego de rede.
- **Esquema proposto**: Introdução de saídas antecipadas e classificador com opção de rejeição para aumentar a eficiência.
- **Taxa de detecção aprimorada**: Saídas antecipadas permitem maior detecção de intrusão em dispositivos de IoT com recursos limitados.
- **Confiabilidade na classificação**: O classificador com rejeição garante precisão em cenários com novos comportamentos de tráfego de rede.
- **Resultados e trabalhos futuros**: Redução de custos de processamento e aumento de acurácia. Futuro foco em incorporar atualizações de modelo para eventos rejeitados.

Detecção de Intrusão Através de Redes Neurais Profundas com Saídas Antecipadas para Inferência Rápida e Confiável

Perguntas?

SBSeg 2024

Simpósio Brasileiro em Segurança da Informação (SBSeg)

PUCPR

SecPLab

Disclosing your future needs for Security & Privacy