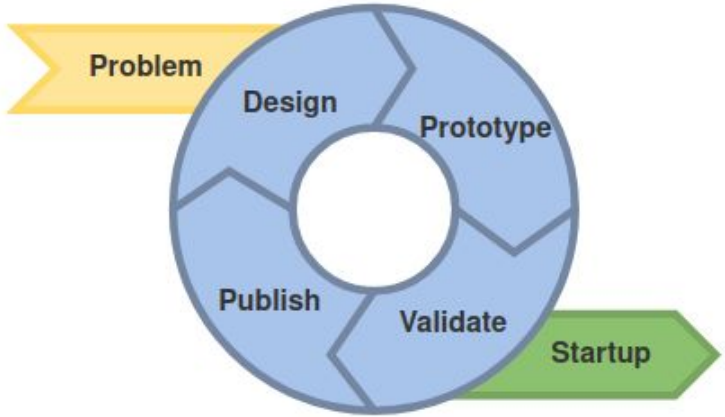
PAINEL - Segurança Cibernética na Era da IA: Desafios e Oportunidades?

Rafael Silva Guimarães
Instituto Federal do Espírito Santo - Campus Cachoeiro de Itapemirim
rafaelg@ifes.edu.br

LabNERDS: Núcleo de Estudos em Redes Definidas por SW

- **Missão:** Inovar em sistemas de rede
- **Áreas**: SDN, NFV, redes autônomas, …

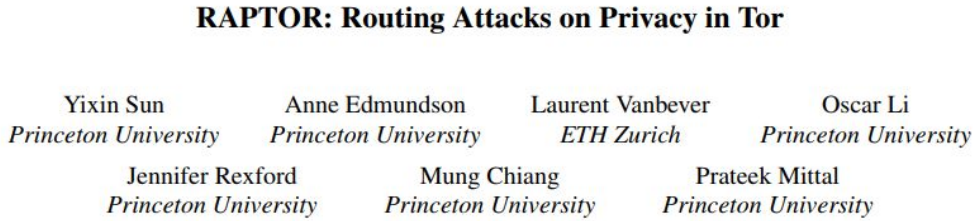


http://nerds.inf.ufes.br

Fundadores Ufes - Colaboradores Ifes

A Internet não é segura

- Além de **não atender aos requisitos das aplicações** atuais de latência, vazão, confiabilidade e conectividade…
  … Muitos **protocolos** amplamente usados na Internet **não foram** originalmente **projetados** com considerações de **segurança** em mente.



Fonte: https://www.ietf.org/proceedings/90/slides/slides-90-irtfopen-1.pdf

BGP e outros protocolos base tem falhas conhecidas

- BGP hijacking (“sequestro”): um atacante consegue redirecionar o tráfego de rede de um ou mais prefixos IP de uma rede legítima para a sua própria rede.

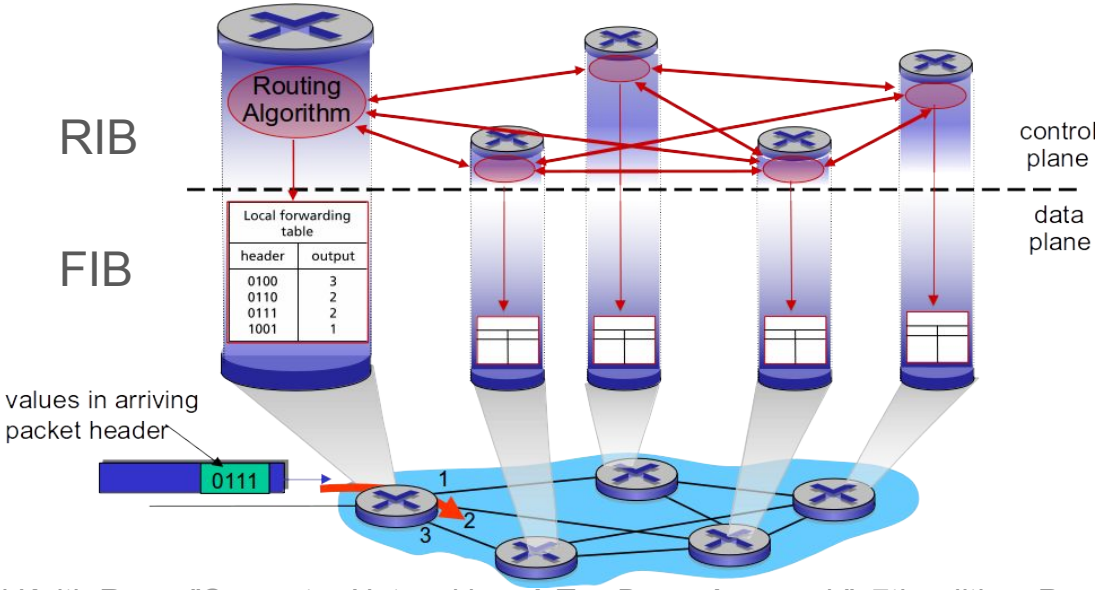
A Internet não é segura

- **Redes tradicionais:**
  - Alto custo de mudança da rede.
  - Protocolos legados com diversas vulnerabilidades de segurança.
  - Novos protocolos seguros são parcialmente implantados junto com protocolos inseguros legados.
  - Mudanças concentradas nos sistemas finais, mas não é suficiente: Focar nas extremidades da rede (e.g., sistemas finais) não resolve as fragilidades no núcleo.

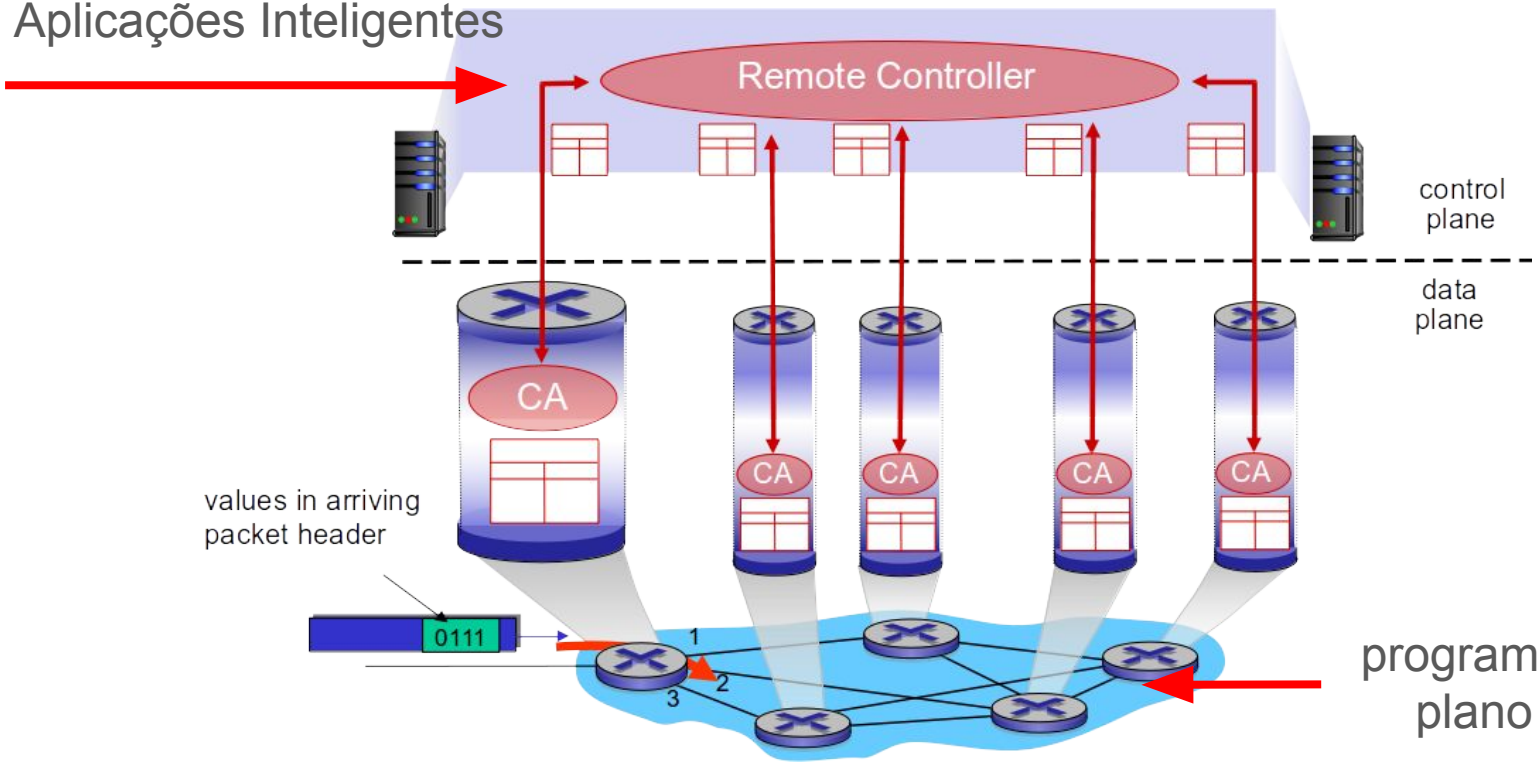
Fonte: https://www.ietf.org/proceedings/90/slides/slides-90-irtfopen-1.pdf

Redes Tradicionais

- **Distribuído**: Os algoritmos de roteamento em cada roteador interagem com os outros roteadores para calcular tabelas de encaminhamento.
- **Equipamento de rede contém tanto o plano de controle quanto o de dados.**



Redes Programáveis

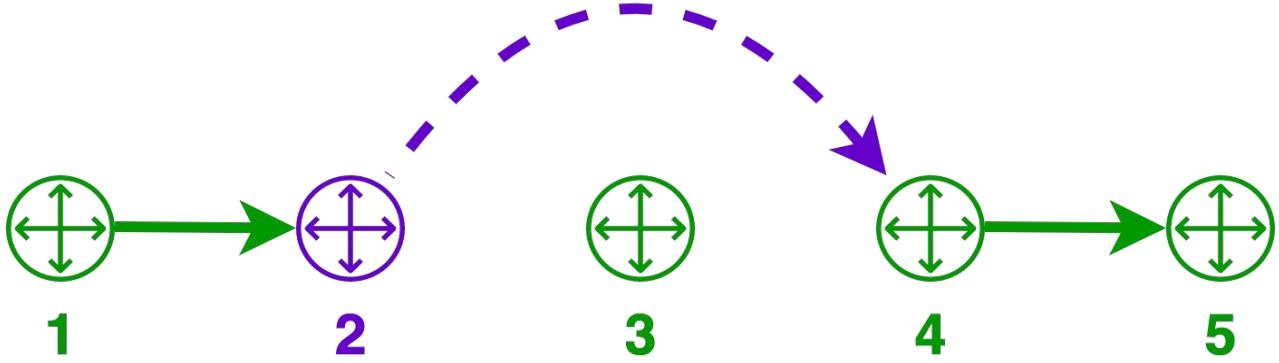


PoT-PolKA: Prova de Trânsito com PolKA

- **Proof of Transit (PoT)**: capacidade de provar que os pacotes passaram por um conjunto de nós de rede.
- **PoT-PolKA:**
  - Combina PolKA com uma solução de prova de trânsito
  - Metadados adicionados ao tráfego em cada salto com base no compartilhamento de um segredo (Shamir shared secret)
  - Verificador: testa se metadados coletados permitem recuperar segredo
  - Segredo só pode ser recuperado ao combinar todas as partes corretamente quando percorre o caminho selecionado

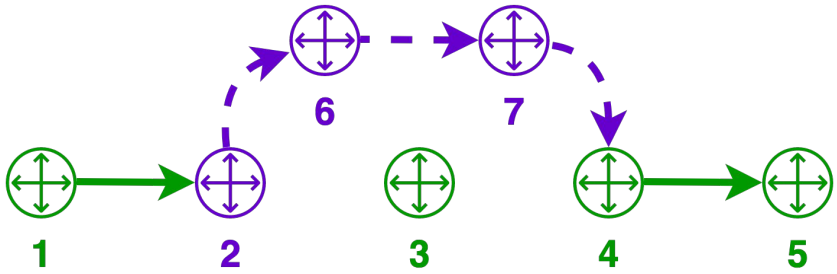
Borges, Everson Scherrer, et al. "In-situ proof-of-transit for path-aware programmable networks." 2023 IEEE 9th International Conference on Network Softwarization (NetSoft). IEEE, 2023.

Extensão de segurança: Prova de Trânsito



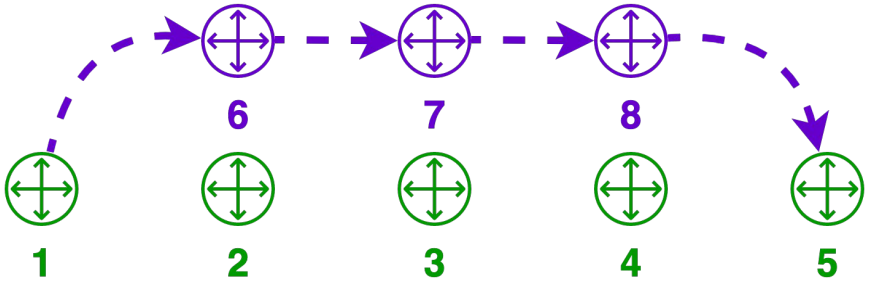
Skipping

Extensão de segurança: Prova de Trânsito



Partial Detour

Extensão de segurança: Prova de Trânsito



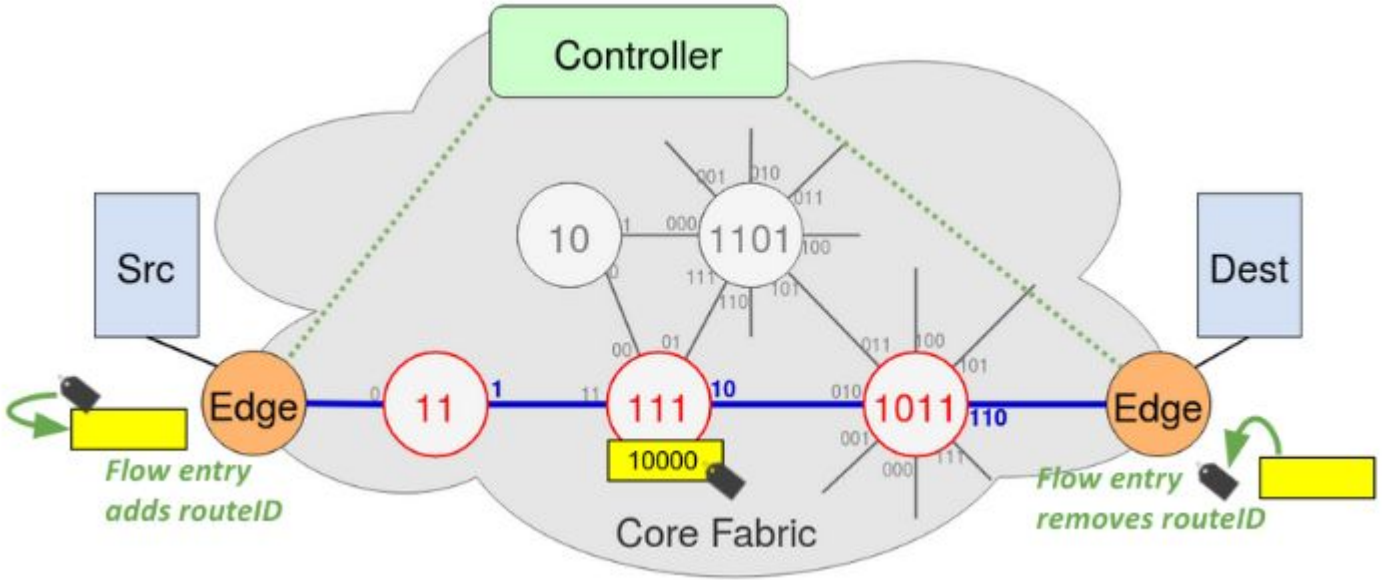
Complete Detour

PolKA: encaminhamento pela origem

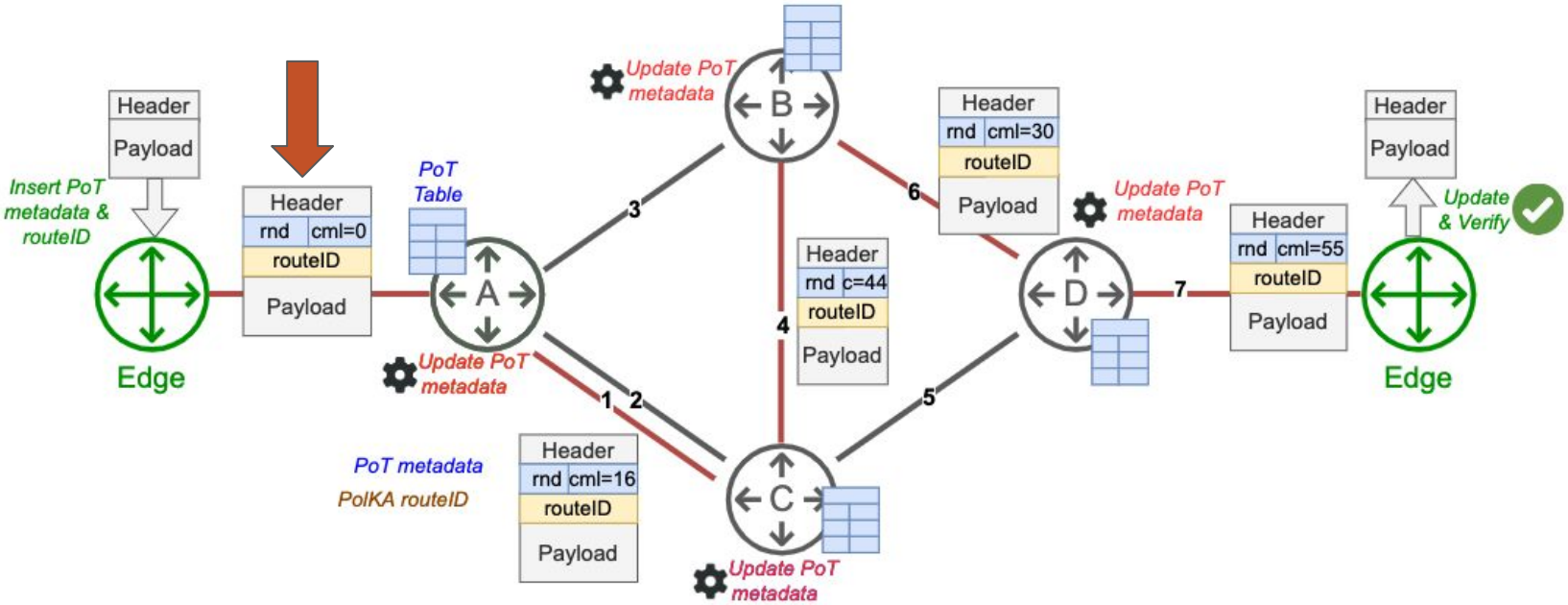
- Roteamento na fonte ou **Source Routing (SR)**
  - Uma origem determina um caminho e adiciona um rótulo de rota ao cabeçalho do pacote.
- **Proposta do grupo**:
  - Codificação da rota usando RNS (Residue Number System)
  - Aritmética usada em várias aplicações criptográficas de segurança
  - Encaminhamento através de operações aritmética de **mod** (resto da divisão):

$$\mathbf{portID} = \langle \mathbf{routeID} \rangle_{\mathbf{nodeID}}$$

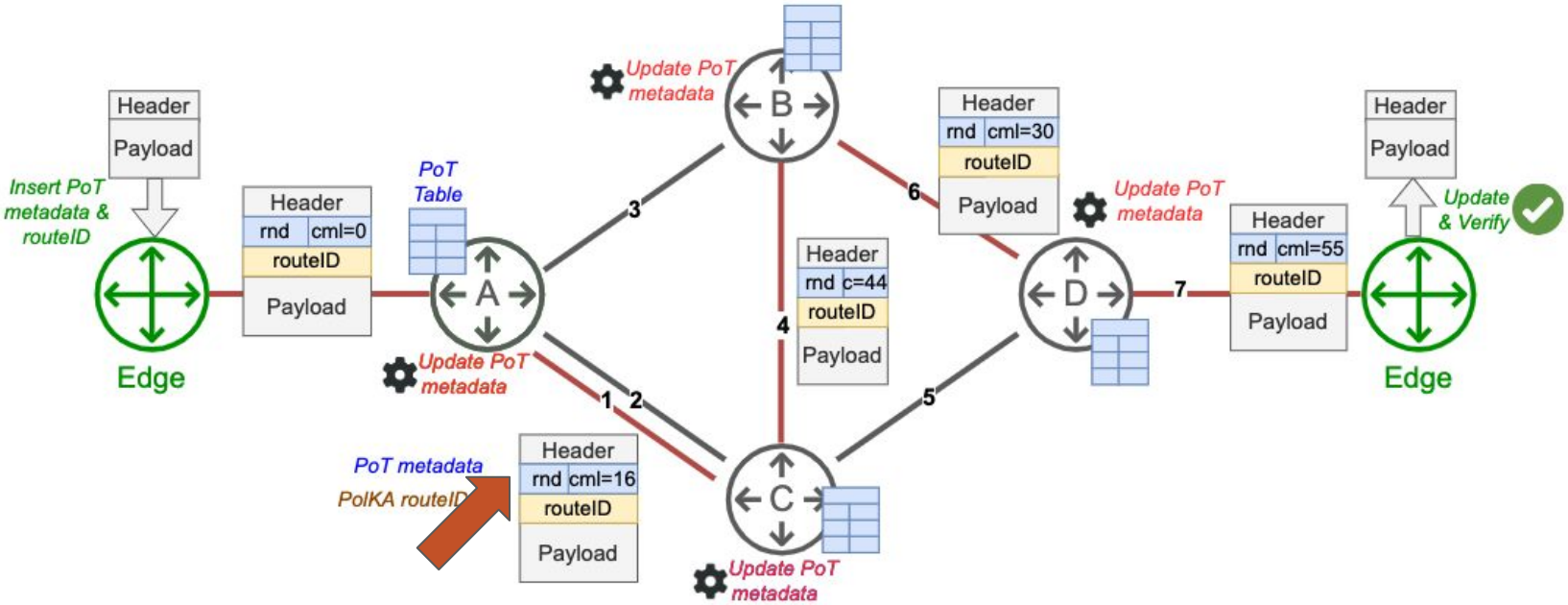
Como o PolKA funciona?



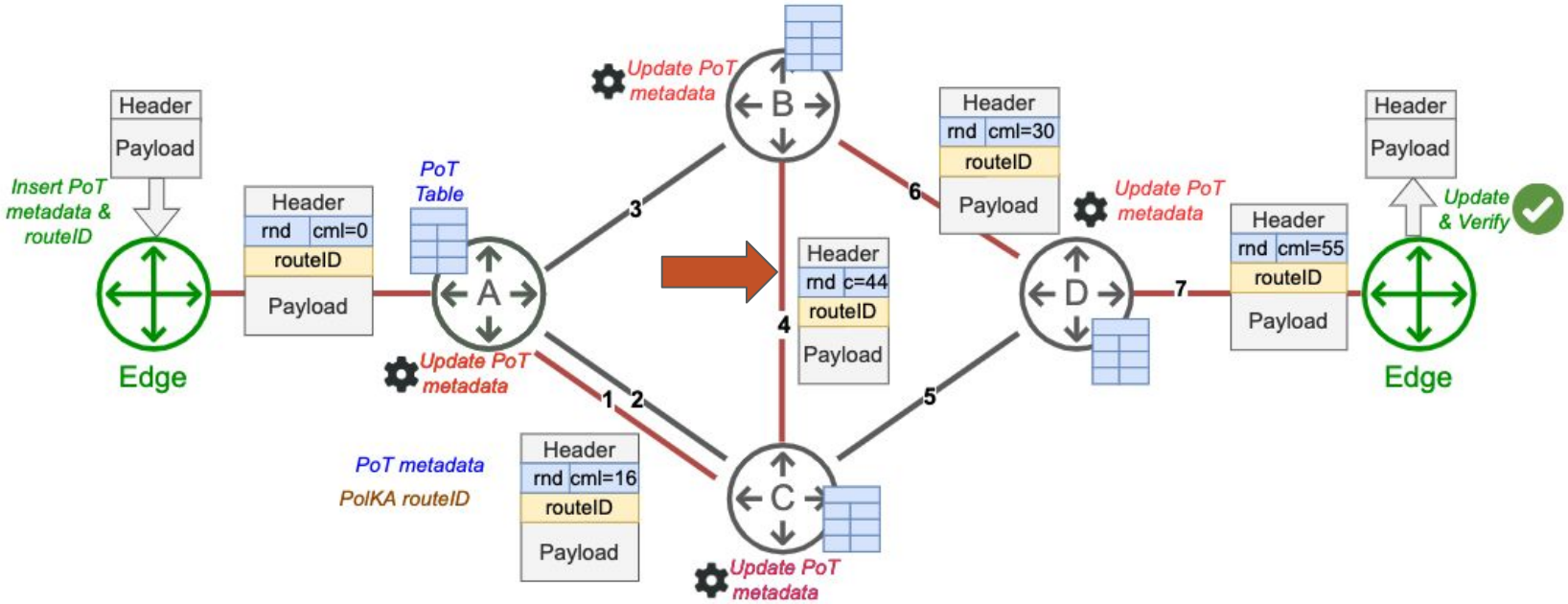
PoT-PolKA


Header
Payload
Insert PoT metadata & routeID
Edge
Header
rnd cml=0
routeID
Payload
PoT Table
A
Update PoT metadata
B
Update PoT metadata
3
4
1
2
Header
rnd c=44
routeID
Payload
PoT metadata
PolKA routeID
Header
rnd cml=16
routeID
Payload
C
Update PoT metadata
6
Header
rnd cml=30
routeID
Payload
D
Update PoT metadata
5
7
Header
rnd cml=55
routeID
Payload
Header
Payload
Update & Verify
Edge

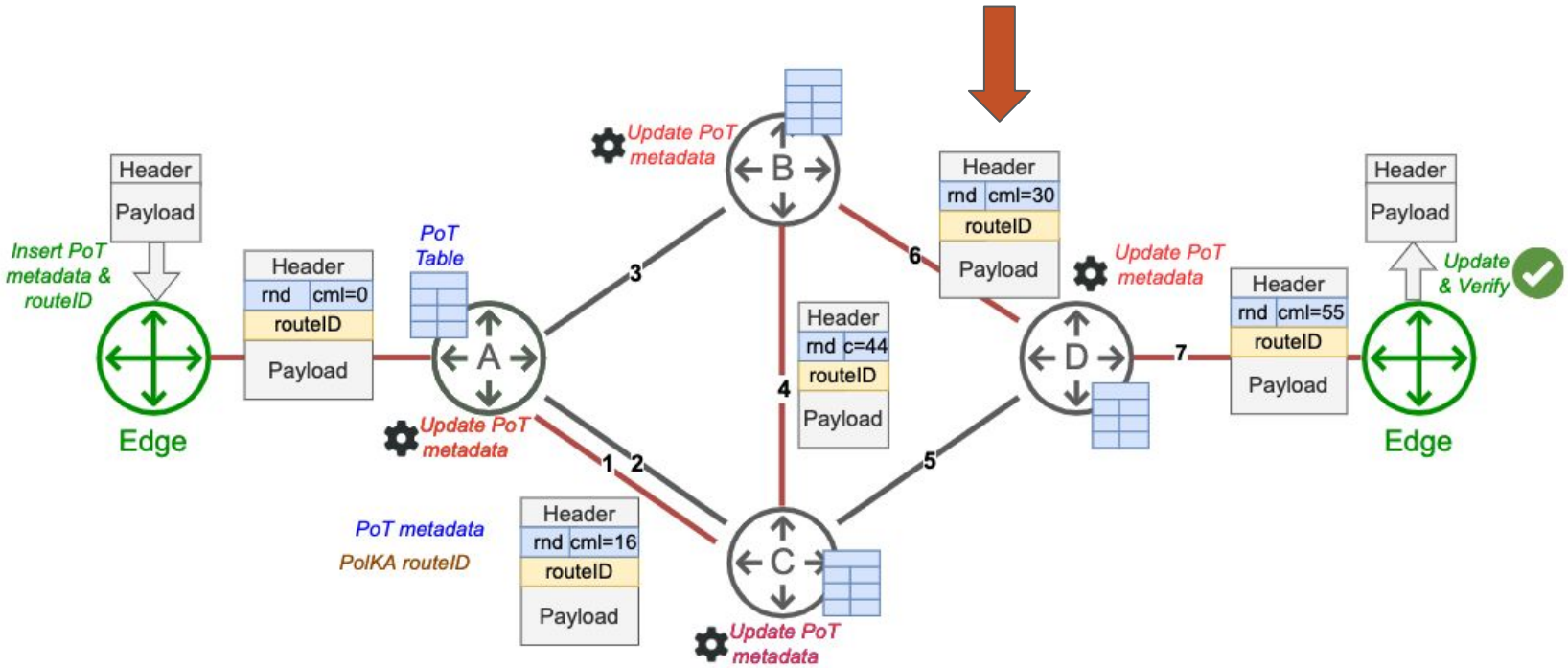
PoT-PolKA


Header
Payload
Insert PoT metadata & routeID
Edge
Header
rnd cml=0
routeID
Payload
PoT Table
A
Update PoT metadata
B
Update PoT metadata
3
4
1
2
Header
rnd c=44
routeID
Payload
PoT metadata
PolKA routeID
Header
rnd cml=16
routeID
Payload
C
Update PoT metadata
6
5
Header
rnd cml=30
routeID
Payload
D
Update PoT metadata
7
Header
rnd cml=55
routeID
Payload
Header
Payload
Update & Verify
Edge

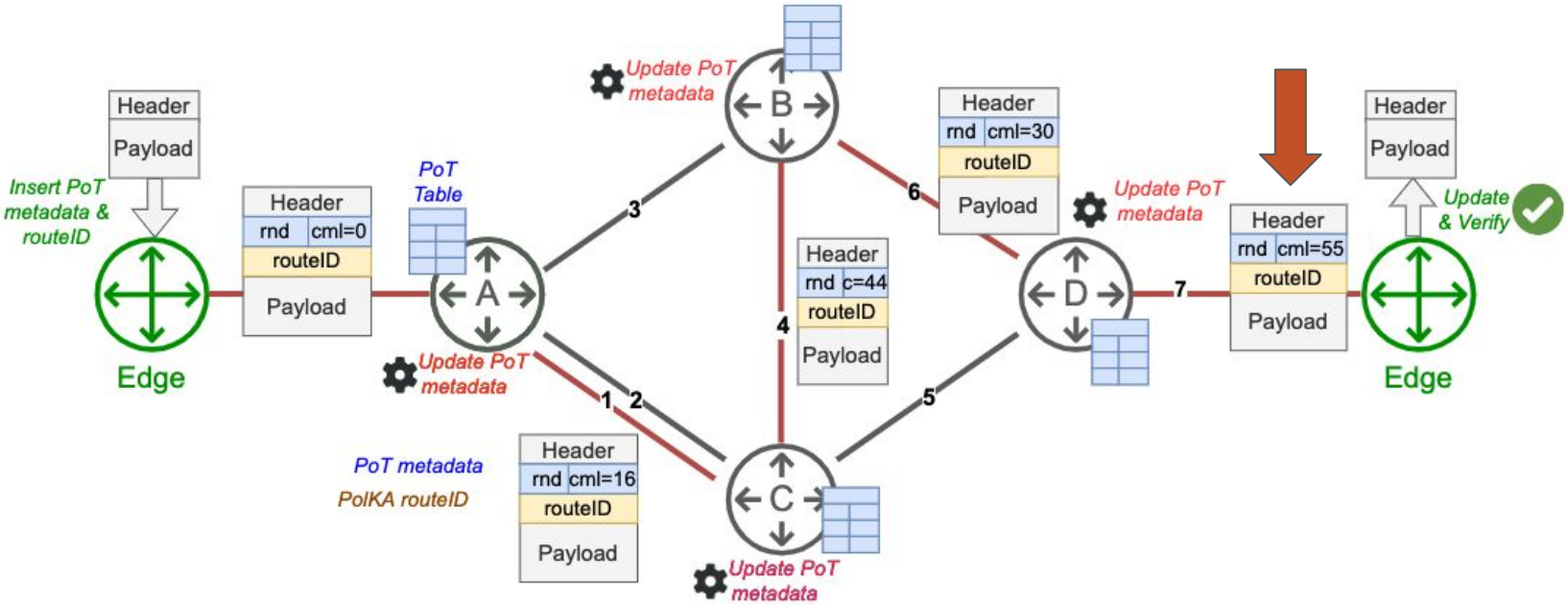
PoT-PolKA


Header
Payload
Insert PoT metadata & routeID
Edge
Header
rnd cml=0
routeID
Payload
PoT Table
A
Update PoT metadata
B
Update PoT metadata
3
4
1
2
C
Update PoT metadata
PoT metadata
PolKA routeID
Header
rnd cml=16
routeID
Payload
Header
rnd c=44
routeID
Payload
6
Header
rnd cml=30
routeID
Payload
D
Update PoT metadata
7
5
Header
rnd cml=55
routeID
Payload
Edge
Header
Payload
Update & Verify

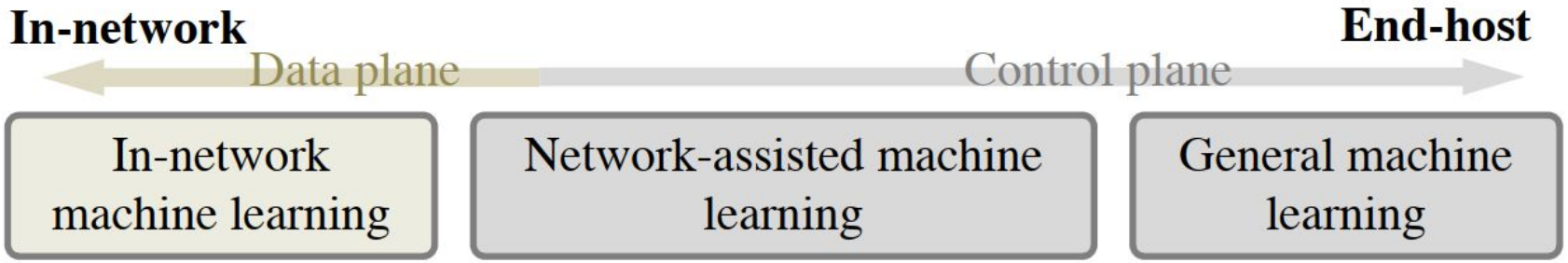
PoT-PolKA


Header
Payload
Insert PoT metadata & routeID
Edge
Header
rnd cml=0
routeID
Payload
PoT Table
A
Update PoT metadata
B
Update PoT metadata
3
4
1
2
Header
rnd c=44
routeID
Payload
PoT metadata
PolKA routeID
Header
rnd cml=16
routeID
Payload
C
Update PoT metadata
6
5
Header
rnd cml=30
routeID
Payload
D
Update PoT metadata
7
Header
rnd cml=55
routeID
Payload
Edge
Header
Payload
Update & Verify

PoT-PolKA


Header
Payload
Insert PoT metadata & routeID
Edge
Header
rnd cml=0
routeID
Payload
PoT Table
A
Update PoT metadata
B
Update PoT metadata
3
4
1
2
Header
rnd c=44
routeID
Payload
PoT metadata
PolKA routeID
Header
rnd cml=16
routeID
Payload
C
Update PoT metadata
6
5
Header
rnd cml=30
routeID
Payload
D
Update PoT metadata
7
Header
rnd cml=55
routeID
Payload
Edge
Header
Payload
Update & Verify

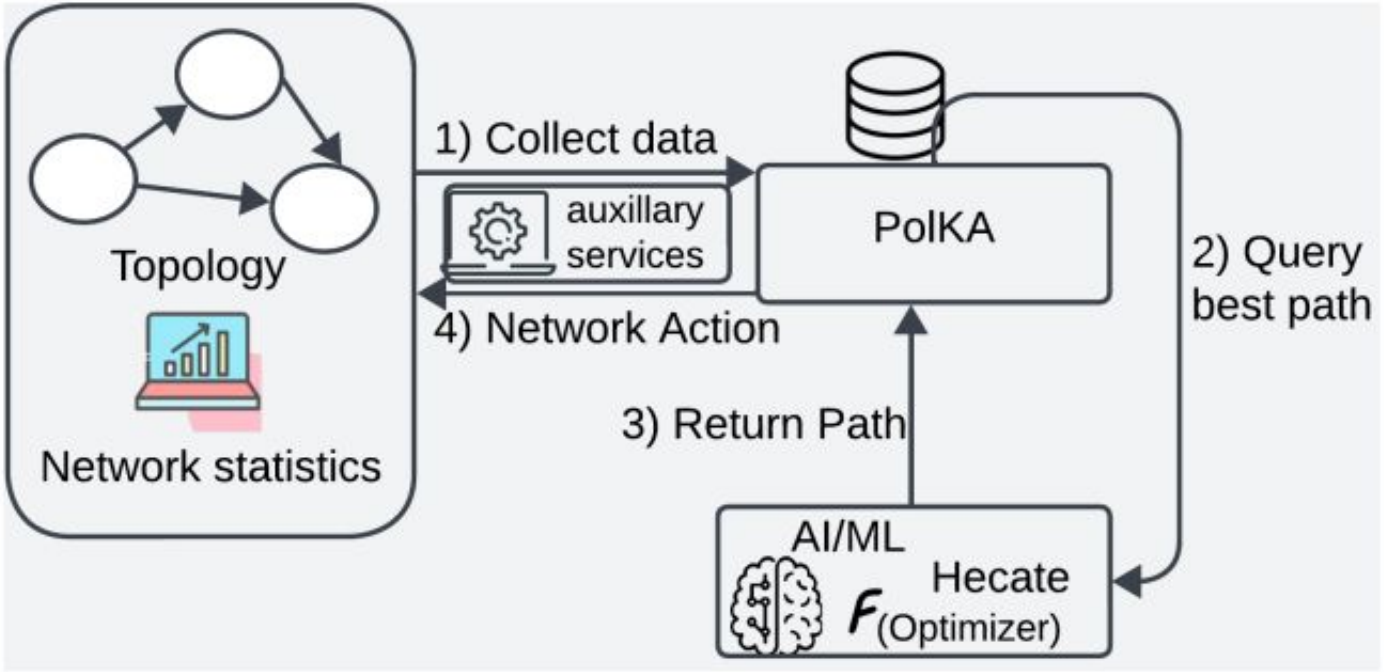
Como usar IA para redes?



Zheng, Changgang, et al. "In-network machine learning using programmable network devices: A survey." IEEE Communications Surveys & Tutorials (2023).
Parizotto, Ricardo, et al. "Offloading machine learning to programmable data planes: A systematic survey." ACM Computing Surveys 56.1 (2023): 1-34.

PolKA + Hecate: Plano de Controle com IA

- Integração de métodos de aprendizado de máquina para previsão de caminhos otimizados para os fluxos.



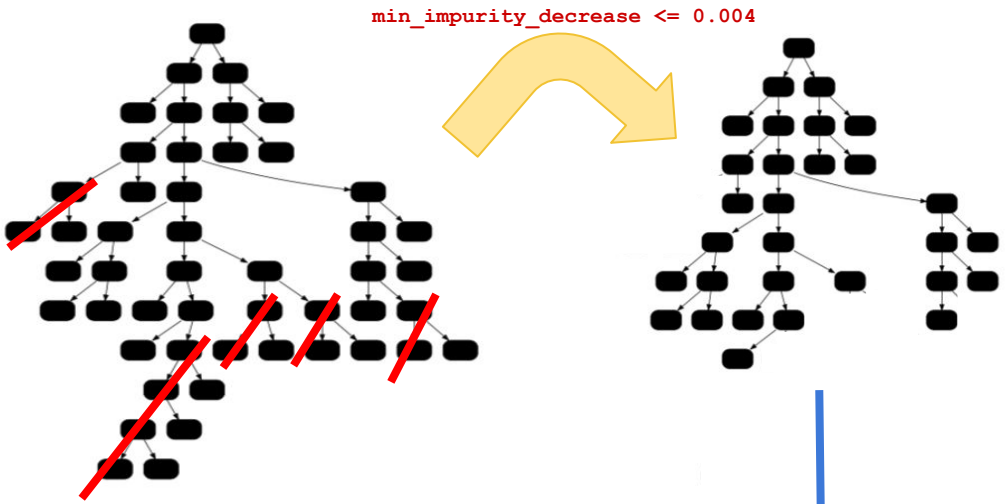
Al-Najjar, A., Paraiso, D., Kiran, M., Dominicini, C., Borges, E., Guimarães, R., Martinello, M., & Newman, H. (2024). Framework for Integrating Machine Learning Methods for Path-Aware Source Routing. Oak Ridge National Laboratory, Federal University of Espírito Santo, & California Institute of Technology.

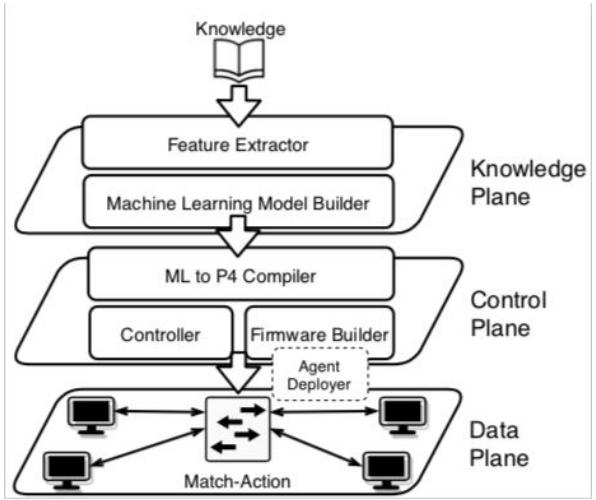
In-network ML: Árvores de decisão em SmartNICs

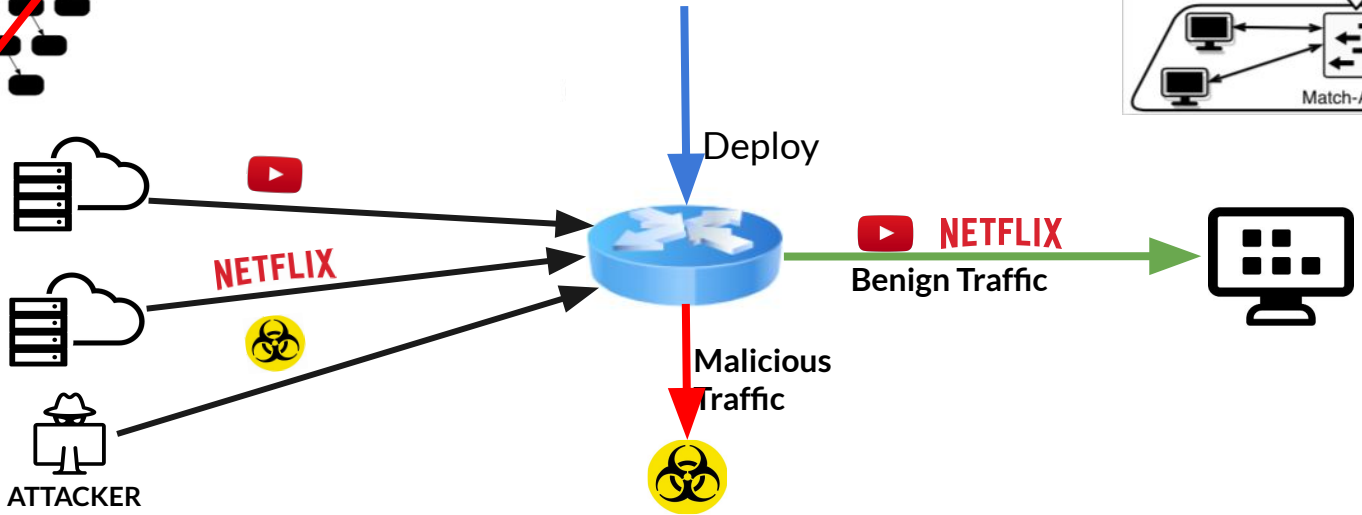
- **Tese de Doutorado Bruno Missi Xavier**
  - Título: Crossing Domains for Accuracy: In-Network Stacking of Machine Learning Classifiers, Ano de obtenção: 2024.
  - Orientador: Magnos Martinello (UFES)
  - Coorientador: Marco Ruffini (TCD, Irlanda)

Programmable Switches for in-Networking Classification (IEEE Infocom 2021)
MAP4: A Pragmatic Framework for In-Network Machine Learning Traffic Classification (IEEE TNSM 2022)

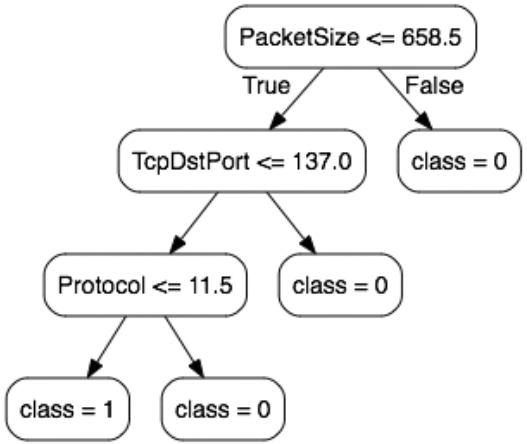
In-network ML: Árvores de decisão em SmartNICs







In-network ML: Árvores de decisão em SmartNICs




```
if (hdr.ipv4.totallen <= 658.5)
  if (hdr.tcp.dstport <= 137.0)
    if (hdr.ipv4.protocol <= 11.5)
      meta.class = 1;
    else
      meta.class = 0;
  else
    meta.class = 0;
else
  meta.class = 0;
```

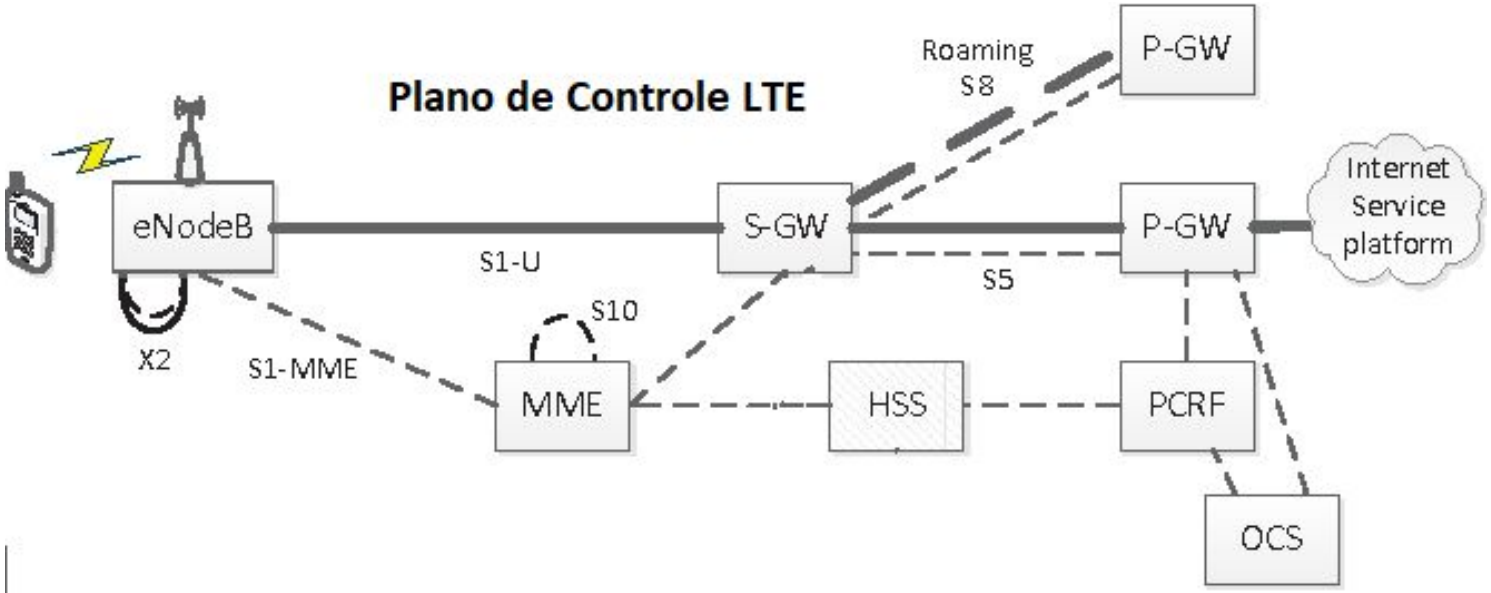
```
...
table classtable {
  key = {
    meta.class: exact;
  }
  actions = {
    forward_by_class;
    ...
  }
  size = 512;
}
...
apply {
  extract_features();
  hash();
  update_features();

  <IF-ELSE_CHAIN_HERE>

  classtable.apply();
}
...
```

Decision Tree **If-else chain** **P4 Template**

Sistema de Mitigação de Ataques de Negação de Serviços Contra o Plano de Controle do 5G (LTE)



R. S. Silva et al., "REPEL: A Strategic Approach for Defending 5G Control Plane From DDoS Signalling Attacks," in IEEE Transactions on Network and Service Management,

Problemas endereçados?

- Ataques de negação de serviços – DoS.
- Forte impacto de forma geral.
- São de difícil detecção por se misturarem ao tráfego legítimo.
- **Ao bloquear um ataque de DoS muitas vezes se bloqueia o tráfego legítimo.**
- A disponibilidade do plano de controle do 5G é ainda mais importante, por causa dos novos serviços multi-tenants/multi-slices.

Ideia

- **E se a gente, ao invés de bloquear o ataque, simplesmente aumentasse os recursos para absorver o ataque?**

- Podemos usar o ambiente virtualizado do 5G para escalonar recursos facilmente.
- Elevar a relação custo/benefício do ataque.
- Garante-se algum tempo adicional para melhorar o restante das camadas de defesa.
- Eventualmente, podemos até interromper o ataque por dissuasão.

RAVEN: Detecção e Classificação Precoce de Atores Maliciosos em uma Rede Acadêmica

Sistema inteligente para detectar e classificar varreduras de portas rapidamente, prevenindo ataques maliciosos futuros.

- Modelos de aprendizado de máquina para classificar tipos de varreduras
- Detecção em tempo real com precisão de 98,8%

Inovações:

- 2 conjuntos de dados gerados usando tráfego real da rede eduroam no Ifes
- Foco na privacidade: sem inspeção de pacotes, apenas análise de fluxo
- Detecção eficaz de 8 tipos de varreduras de portas

Coelho, W. B., Zanotelli, V. F., Comarela, G., & Villaça, R. S. (2024). RAVEN: Detecção e Classificação Precoce de Atores Maliciosos em Redes Acadêmicas. Instituto Federal do Espírito Santo (Ifes) e Universidade Federal do Espírito Santo (Ufes).

UFES criES Escola Regional de Informática ES

INSTITUTO FEDERAL
Espírito Santo
Campus
Cachoeiro de Itapemirim

Obrigado!

Rafael S. Guimarães
rafaelg@ifes.edu.br