IX Escola Regional de Informática do Espírito Santo (ERI-ES 2024)
17 a 19 de outubro de 2024 - UFES

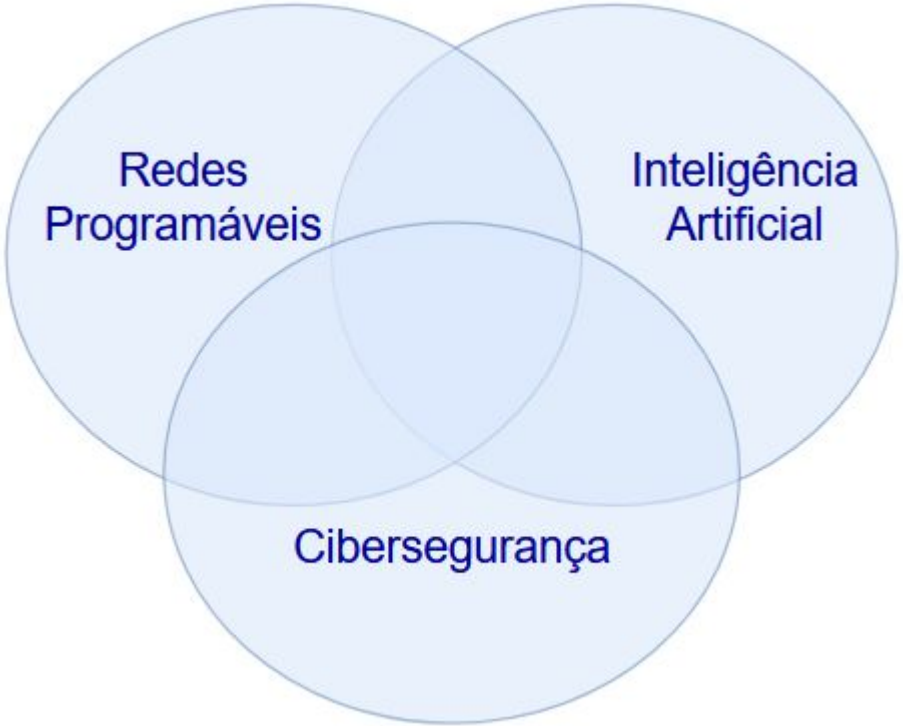
Programabilidade de redes para endereçar os Desafios da Segurança da Informação na era da IA

Cristina Klippel Dominicini
Instituto Federal do Espírito Santo - Campus Serra
cristina.dominicini@ifes.edu.br

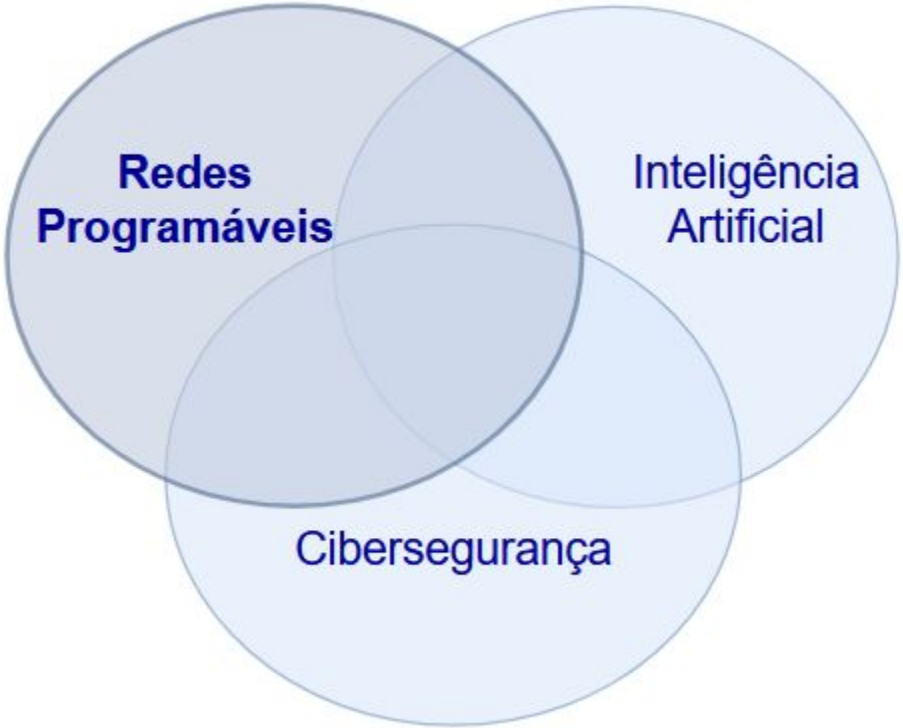
INSTITUTO FEDERAL
Espírito Santo

UFES

Palestra: Áreas de Conhecimento



Palestra: Áreas de Conhecimento



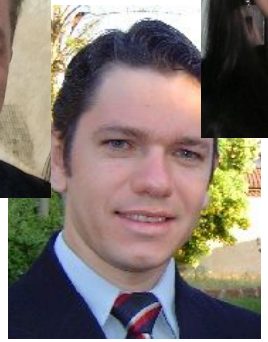
PPCOMP Ifes - Campus Serra

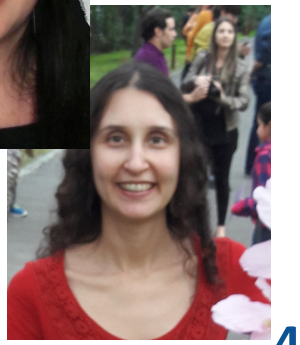
- Mestrado Profissional do Programa de Pós-Graduação em Computação Aplicada (PPComp)
- **Linhas: IA e Redes de computadores**

https://ppcomp.serra.ifes.edu.br

PPComp

Mestrado Profissional em Computação Aplicada

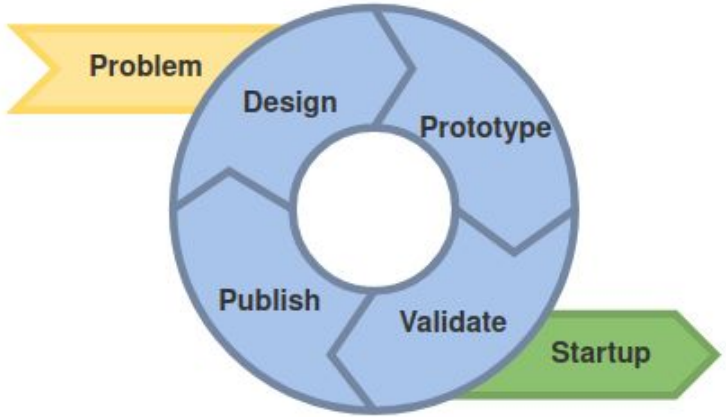




LabNERDS: Núcleo de Estudos em Redes Definidas por SW

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

Nerds http://nerds.inf.ufes.br



Fundadores Ufes - Colaboradores Ifes

Agenda

- Por que os desafios atuais de cibersegurança não conseguem ser resolvidos pelas redes atuais?
- O que são redes programáveis?
- Como IA e redes programáveis podem ser combinadas para resolver problemas de segurança?
- A nossa experiência no LabNERDS :-)
  - Como prototipar soluções com redes programáveis?
  - Aplicações

Agenda

- Por que os desafios atuais de cibersegurança não conseguem ser resolvidos pelas redes atuais?
- O que são redes programáveis?
- Como IA e redes programáveis podem ser combinadas para resolver problemas de segurança?
- A nossa experiência no LabNERDS :-)

Aplicações emergentes em telecomunicações...

- Indústria 4.0
- Cidades Inteligentes
- Saúde Móvel
- Realidade Aumentada

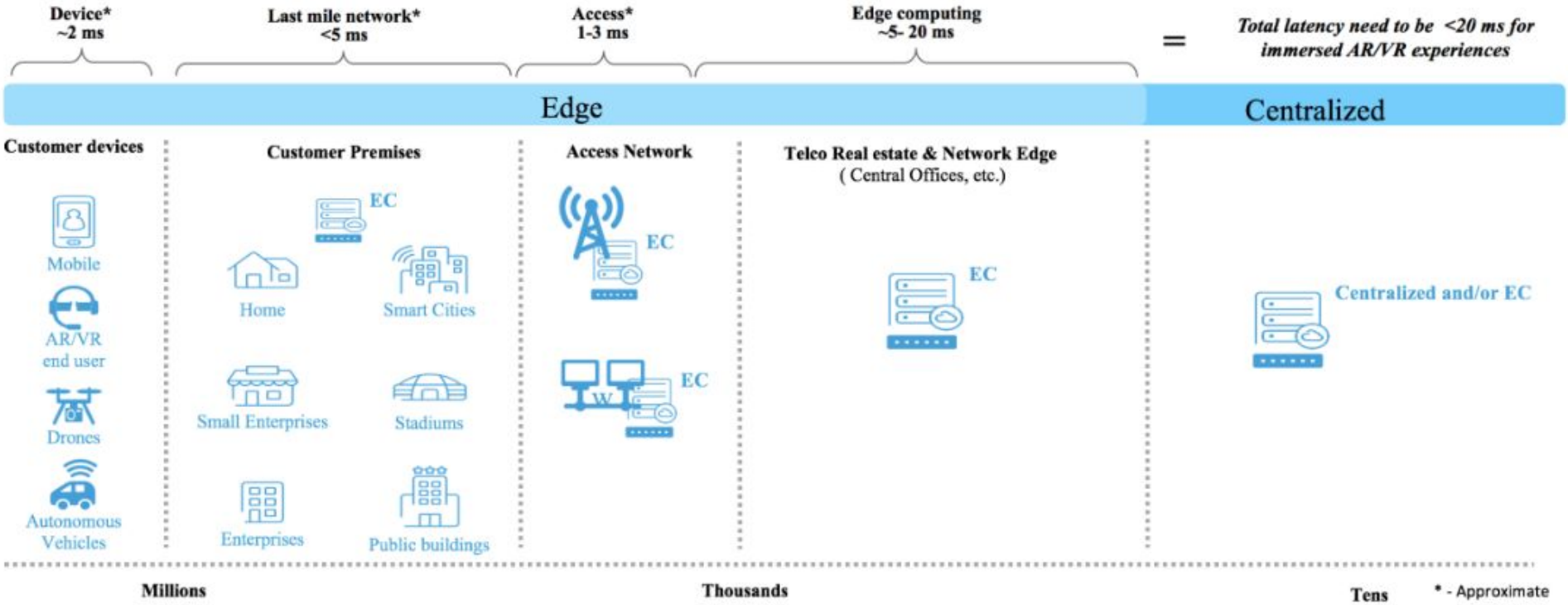
...

Fonte: Intel's Vision for 5G: https://www.intel.com/content/www/us/en/wireless-network/5g-vision-document.html

...demandam processamento dinâmico de um grande volume de dados

Fonte: Intel's Vision for 5G: https://www.intel.com/content/www/us/en/wireless-network/5g-vision-document.html

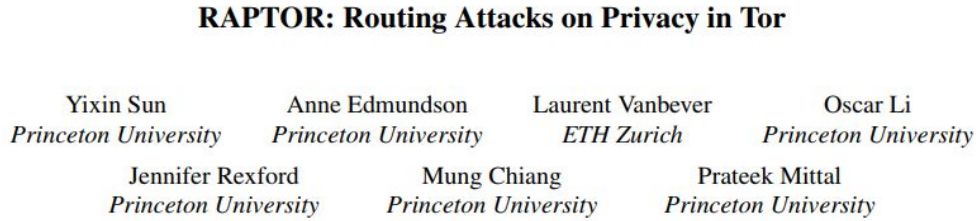
Dispositivos heterogêneos distribuídos desde a borda até o núcleo da rede



Fonte: AT&T Edge Cloud (AEC) White Paper, 2017

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.

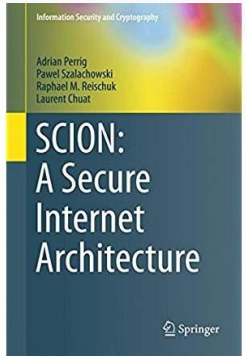
A Internet não é segura

- **Redes tradicionais: black boxes!**
  - Alto custo de mudança no núcleo da rede.
  - **Raciocínio**: Fornecer proteção suficiente sem introduzir complicações.
  - Novos protocolos seguros são parcialmente implantados junto com protocolos inseguros legados.
  - Mudanças concentradas nos sistemas finais, mas não é suficiente.
- **Solução: Mudar as redes!**
  - Escopo: Internet ou domínios administrativos específicos

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

Propostas para Internet Segura

- ETH Zurich
- SCION: A Global Next-Generation Public Internet
  - Alta segurança e eficiência
  - Comunicação multicaminho
  - Path-aware networking
- Maturidade
  - 11 anos de desenvolvimento
  - Código aberto
  - Rede de produção global (60 locais, sem BGP)
  - Rede de pesquisa global



Agenda

- Por que os desafios atuais de cibersegurança não conseguem ser resolvidos pelas redes atuais?
- O que são redes programáveis?
- Como IA e redes programáveis podem ser combinadas para resolver problemas de segurança?
- A nossa experiência no LabNERDS :-)

Conceitos Básicos

- **Encaminhamento:** como os pacotes que chegam na **porta de entrada** de um roteador são movidos para a **porta de saída** apropriada.

  → **Plano de dados**

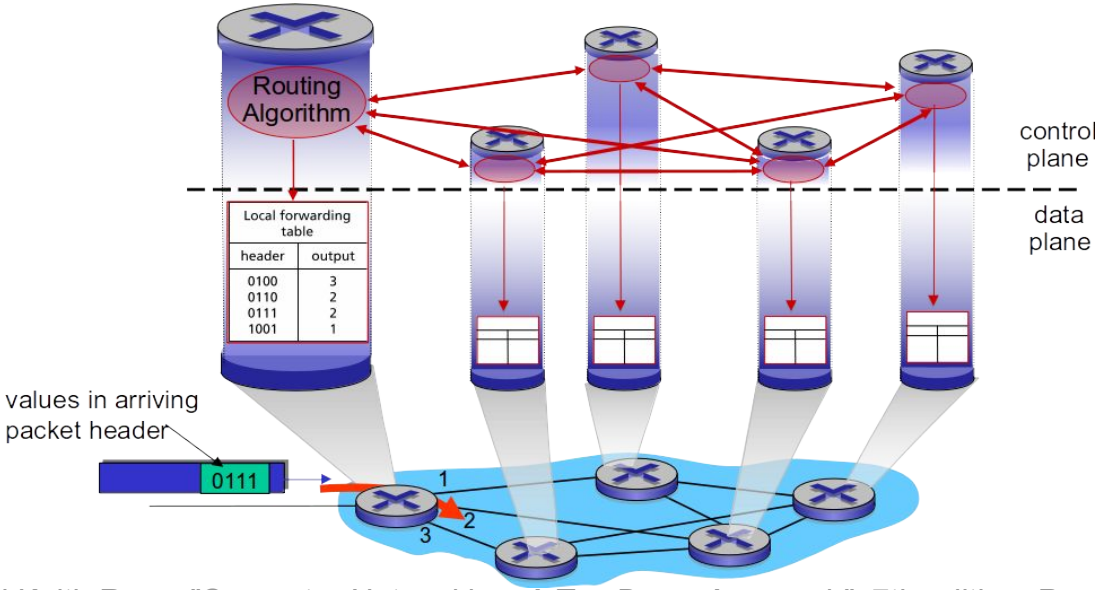
- **Roteamento:** determina o **caminho fim-a-fim** percorrido pelos pacotes da origem ao destino.

  → **Plano de Controle**

  - E mais… balanceamento de carga, controle de acesso, economia de energia....

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.**



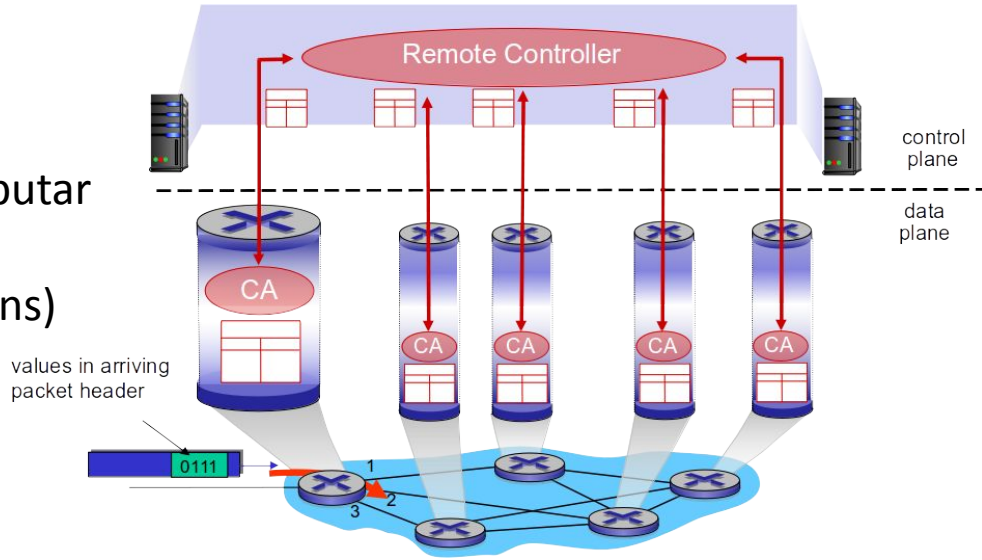
Redes Tradicionais

- **Equipamento de rede: black box**
  - Hardware com protocolos pré-determinados
  - Interfaces e funcionalidades específicas do fabricante
  - Configuração de muitos dispositivos distribuídos
  - Difícil inovar e adicionar novos recursos

1ª onda SDN: Programabilidade do Plano de Controle

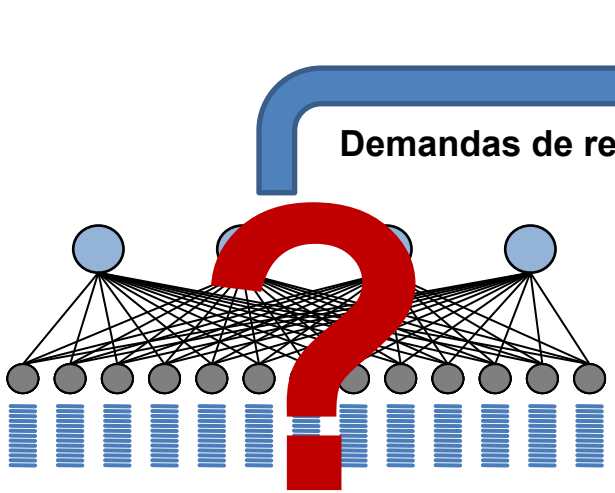
- **Software-defined networking (SDN): Redes definidas por software**
  - Separa planos de controle e dados.
  - Um controlador (logicamente) centralizado interage com agentes locais nos roteadores.
  - O protocolo OpenFlow permite "programar" roteadores para computar tabelas de encaminhamento.
  - Plano de dados fixo (match & actions)

wildcards		
in_port		dl_src
dl_dst		
		dl_vlan
dl_pcp	pad	dl_type
nw_tos	nw_prot	pad
nw_src		
nw_dst		
tp_src		tp_dst

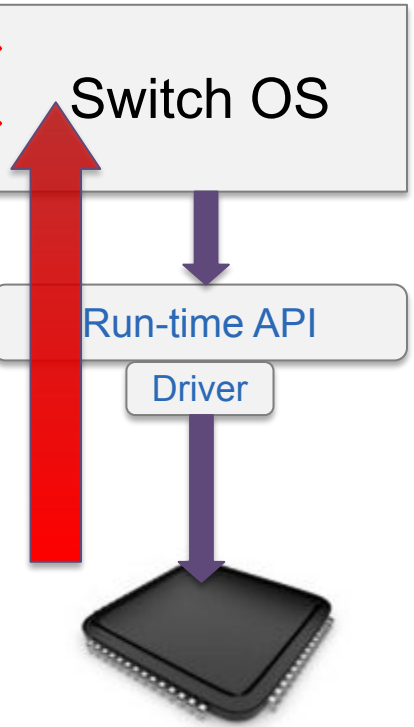


Source: Jim Kurose and Keith Ross, "Computer Networking: A Top Down Approach", 7th edition, Pearson/Addison Wesley, 2016

Plano de dados fixo: Bottom-up design



Demandas de redes

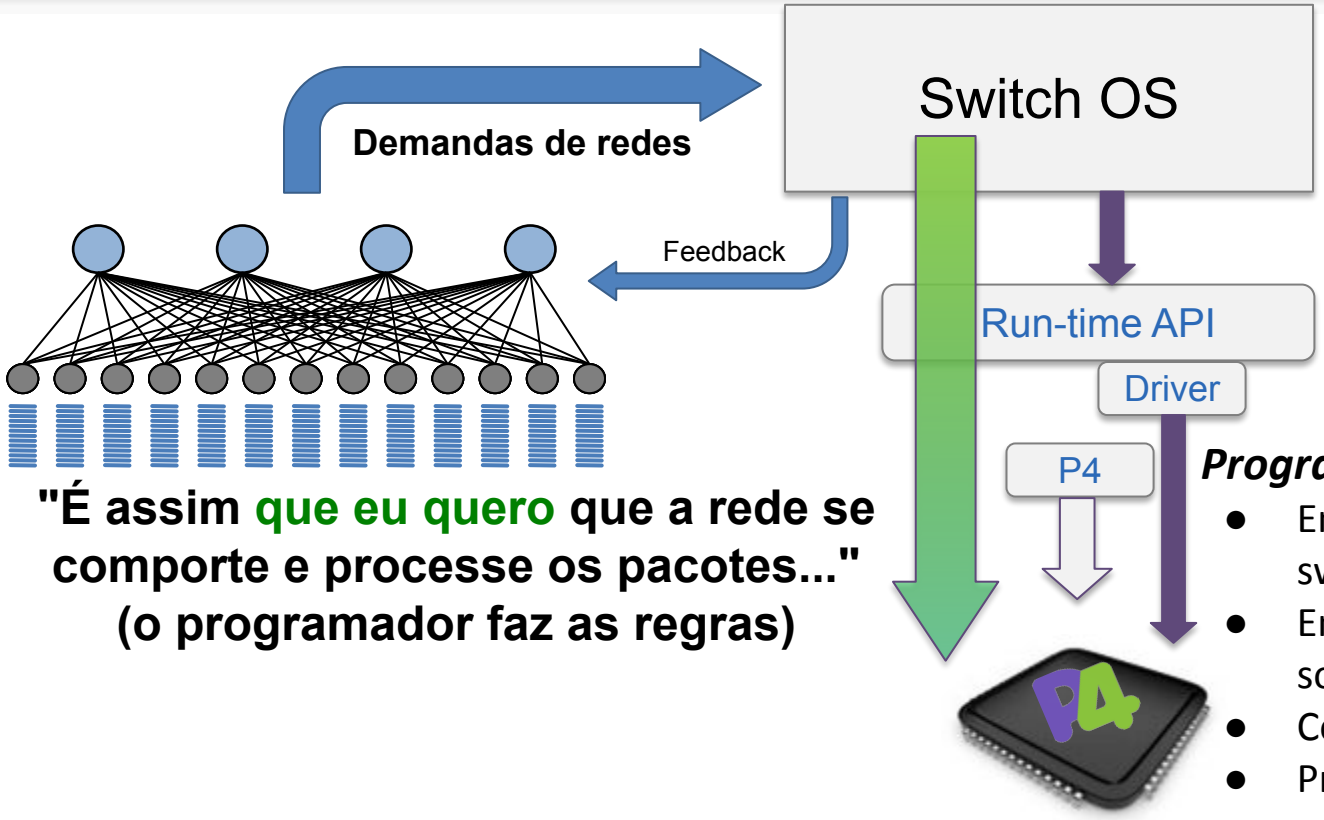


“É assim que eu sei processar pacotes”
(O ASIC faz as regras)

Fixed-function ASIC
(*Application-Specific Integrated Circuit*)

Source: https://github.com/p4lang/tutorials/blob/sigcomm19/P4_tutorial_SIGCOMM19.pdf

2ª onda SDN: Programabilidade do Plano de Dados



"É assim que eu quero que a rede se comporte e processe os pacotes..."
(o programador faz as regras)

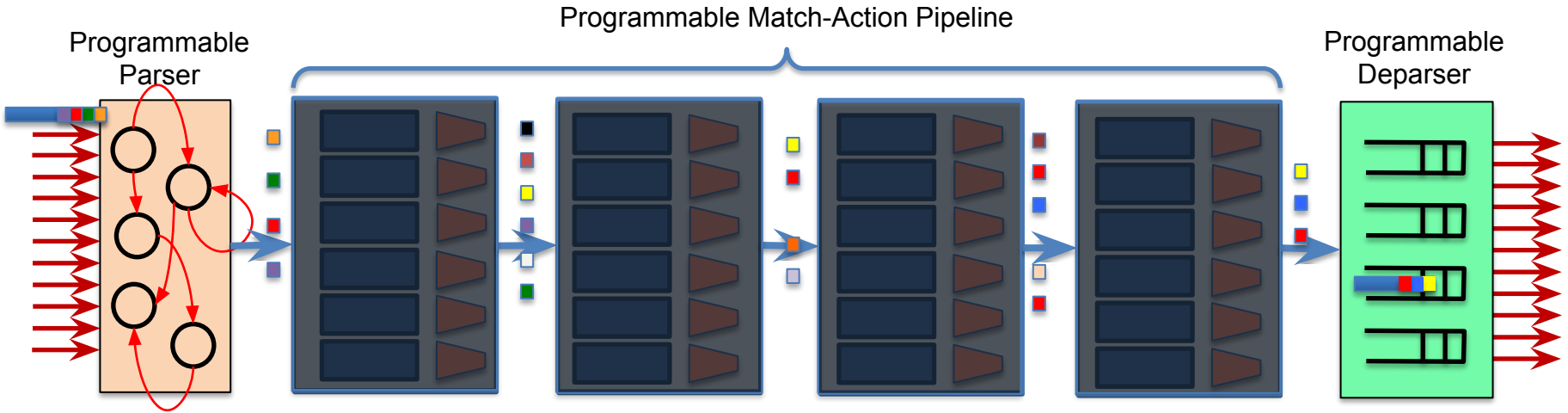
Programmable Switch ASIC

- Energia, custo e desempenho = switches de função fixa
- Encaminhamento definido em software (**linguagem P4**)
- Compila o programa para o chip
- Programas rodam em taxa de linha

Source: https://github.com/p4lang/tutorials/blob/sigcomm19/P4_tutorial_SIGCOMM19.pdf

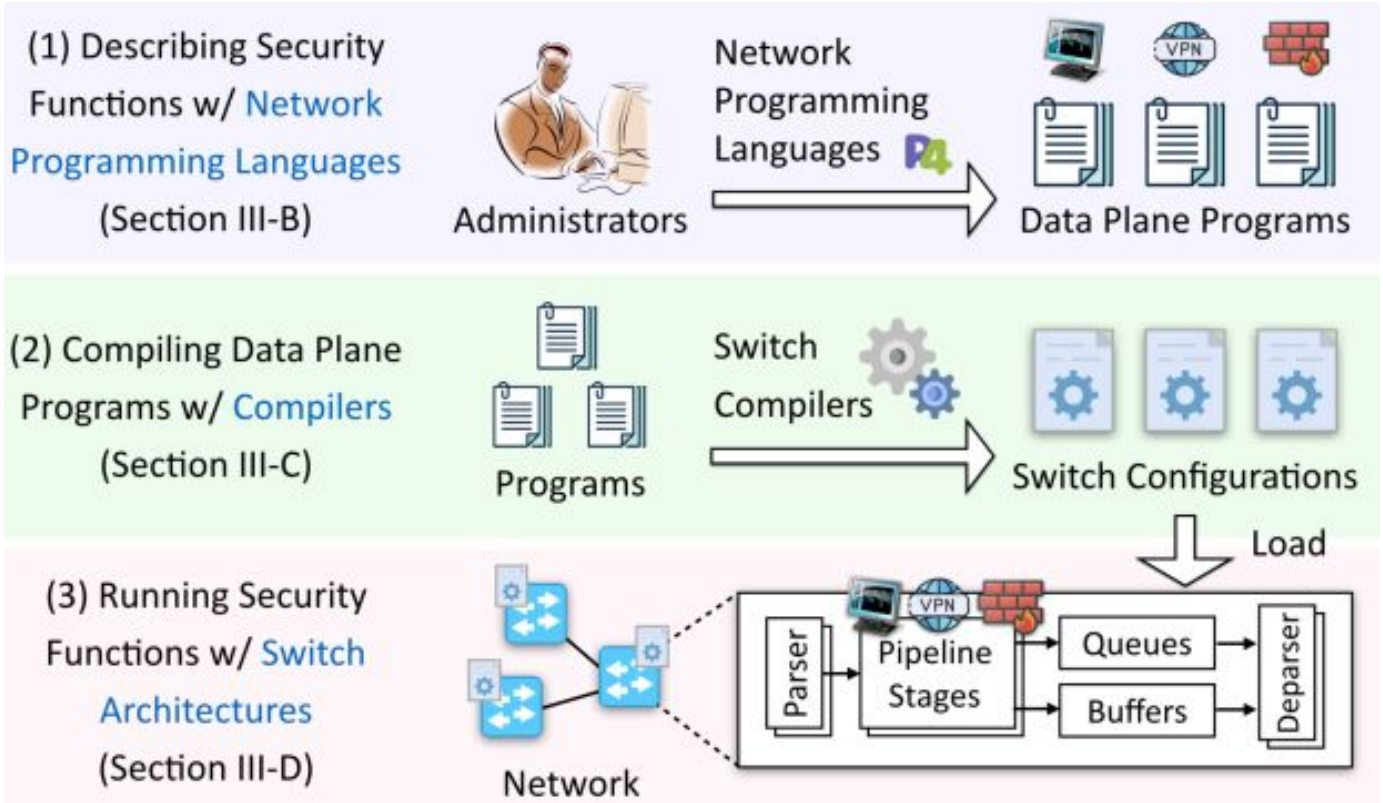
Protocol Independent Switch Architecture (PISA)

- Programa em **linguagem de alto nível P4** define:
  - Como cabeçalhos são lidos (parser)
  - Como cabeçalhos são modificados, adicionados ou removidos por meio de tabelas e o algoritmos de processamento (match-action pipeline)
  - Como pacotes são serializados para envio (deparser)



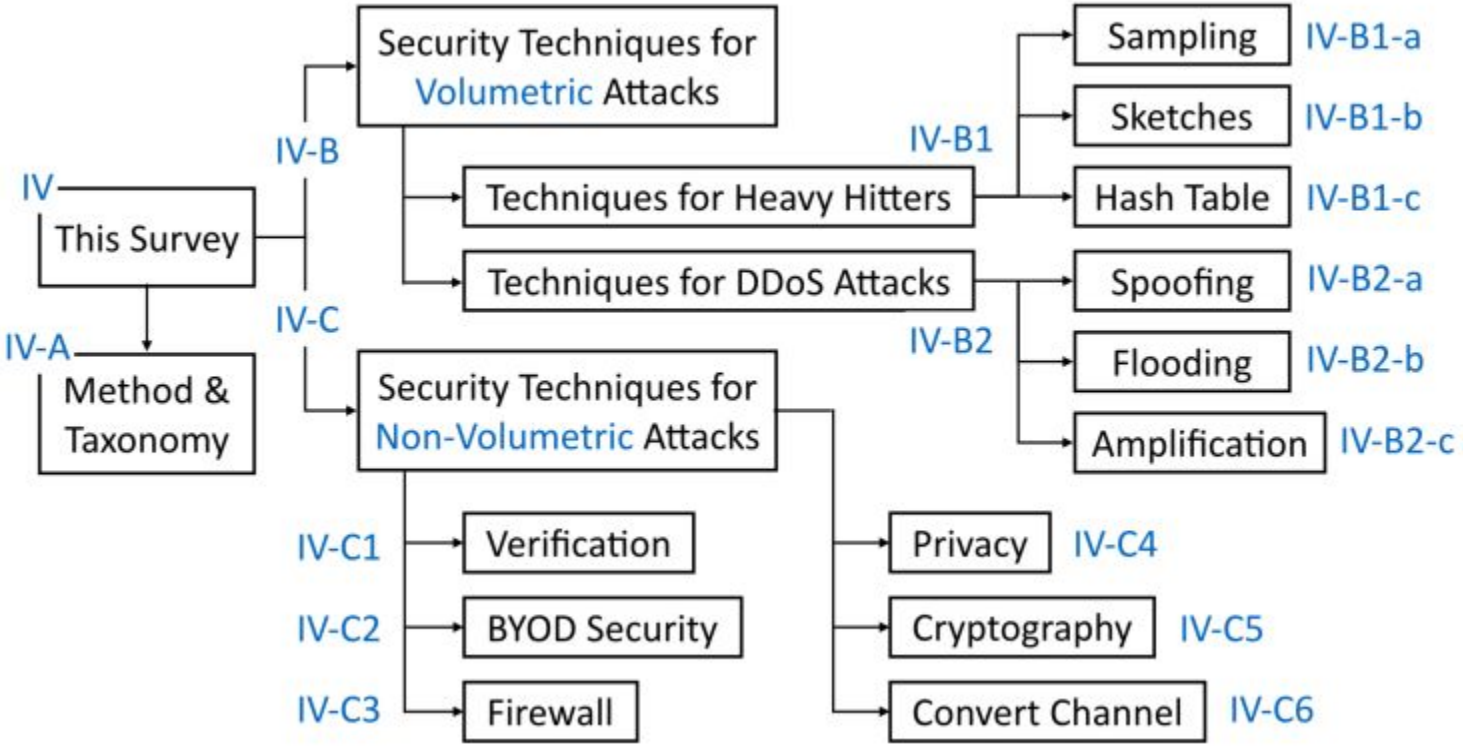
Source: https://github.com/p4lang/tutorials/blob/sigcomm19/P4_tutorial_SIGCOMM19.pdf

Fortalecendo a segurança de rede com switches programáveis



X. Chen et al., "Empowering Network Security With Programmable Switches: A Comprehensive Survey," in IEEE Communications Surveys & Tutorials, vol. 25, no. 3, pp. 1653-1704, thirdquarter 2023

Fortalecendo a segurança de rede com switches programáveis



X. Chen et al., "Empowering Network Security With Programmable Switches: A Comprehensive Survey," in IEEE Communications Surveys & Tutorials, vol. 25, no. 3, pp. 1653-1704, thirdquarter 2023

Benefícios: Programabilidade do Plano de Dados

- Adicionar novos protocolos
- Remover protocolos não utilizados
- Uso eficiente de recursos de hardware
- Novas técnicas de diagnóstico e telemetria
- Desenvolvimento rápido e inovação
- Agora podemos implementar nossas próprias ideias no plano de dados!!

Source: https://github.com/p4lang/tutorials/blob/sigcomm19/P4_tutorial_SIGCOMM19.pdf

Agenda

- Por que os desafios atuais de cibersegurança não conseguem ser resolvidos pelas redes atuais?
- O que são redes programáveis?
- Como IA e redes programáveis podem ser combinadas para resolver problemas de segurança?*
- A nossa experiência no LabNERDS :-)
  - Como prototipar soluções com redes programáveis?
  - Aplicações

**Discussão baseada na apresentação: Desvendando o Potencial e os Limites de IA/ML em Redes de Comunicação, Prof. Prof. Luciano Paschoal Gaspary, INF-UFRGS, 27 de setembro de 2024 : https://www.youtube.com/watch?v=Wqk8_JTuad0*

Escopo da Palestra

- **AI for Networking or**

… Networking for AI

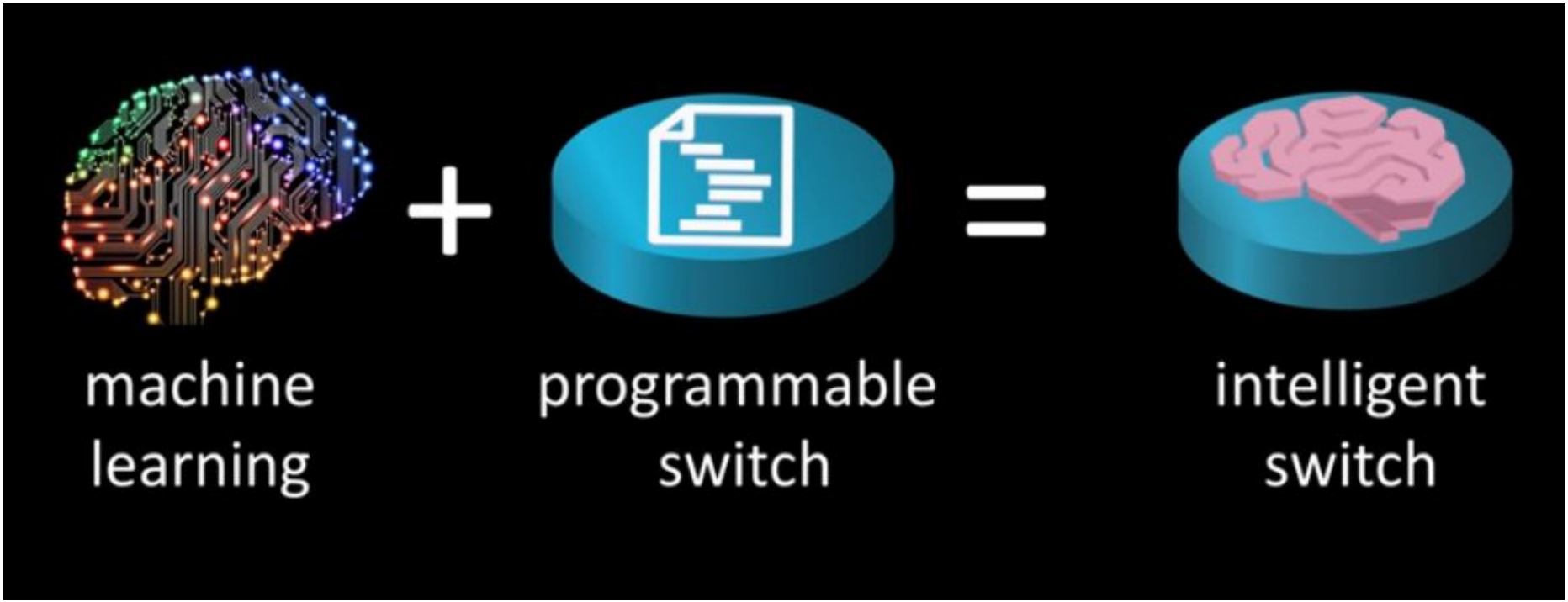
  - Técnicas de IA para apoiar problemas de redes

- **Plano de Dados ou**

… Plano de Controle

  - Foco no encaminhamento dos dispositivos de redes

IA + Redes Programáveis



**Slides cedidos pelo Prof Magnos Martinello (UFES) em apresentação para UFF em 2020: Programabilidade do sistema numérico de resíduos e seus genes inovadores na área de redes*

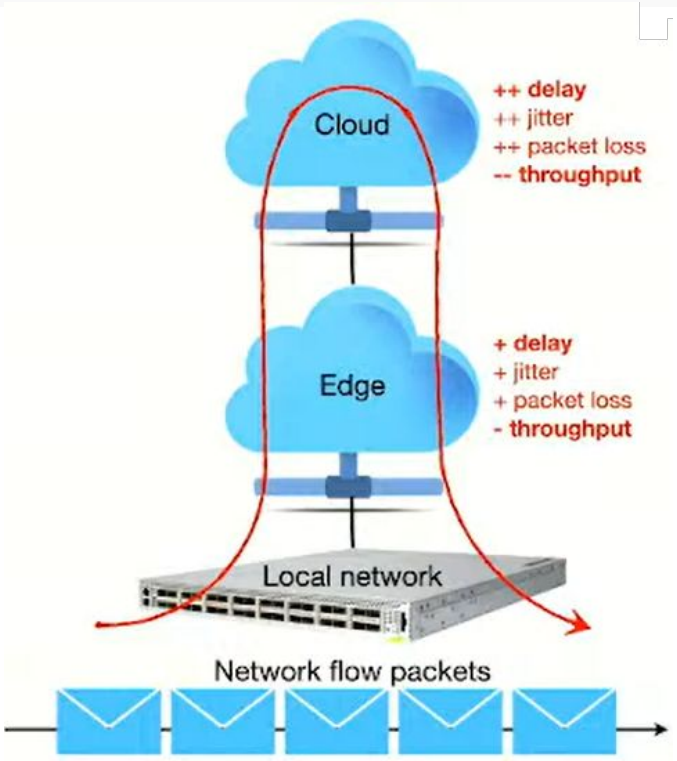
Como usar IA para redes?

- **Exemplos de Problemas:**
  - Detecção de intrusão observando eventos não esperados
  - Classificação de tráfego baseado em padrões nos pacotes de rede
  - Engenharia de tráfego baseada em predição de demandas e gargalos

- **Como a IA pode ajudar as redes:**
  - **Maior qualidade da resposta**
  - **Respostas mais rápidas**

Como usar IA para redes?

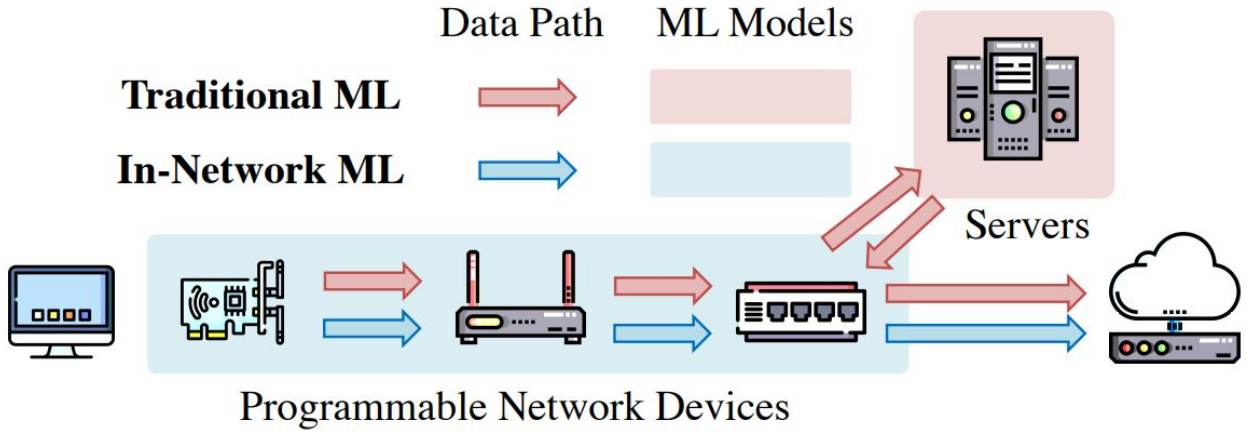
- **Locais**
  - Nuvem
  - Borda
  - **Dispositivos de rede**
    - Alto poder de processamento
    - Onde os dados trafegam
    - Maiores taxas de transmissão
    - Menor latência



Jonatas Marques, Kirill Levchenko, and Luciano Gaspary. 2020. IntSight: diagnosing SLO violations with in-band network telemetry. CoNEXT '20. https://doi.org/10.1145/3386367.3431306

Como usar IA para redes?

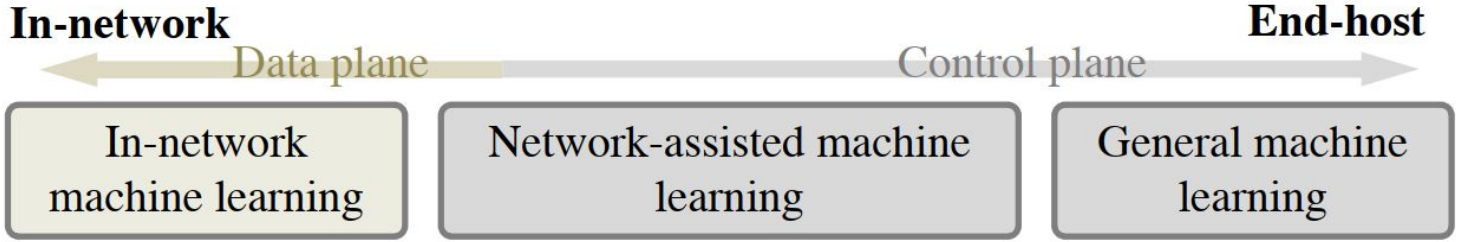
- **In-network Machine Learning:**
  - Offloading parcial ou total (implantação) de algoritmos de ML executados em dispositivos de rede



Malkan Jenil Manojkumar, Trivedi Aastha Kunalkumar, Network Automation using Machine Learning, International Journal of Research Publication and Reviews, Vol (5), Issue (8), August (2024), Page – 930-945

Como usar IA para redes?

- **Fases IA**
  - **Treinamento** (Aprendizado)
    - Estratégia no **plano de controle**
    - Offload mais eficiente (nuvem, por exemplo)
  - **Inferência** (Aplicação do modelo treinado para previsões)
    - Tática no **plano de dados**
    - Implantar modelos de ML nos dispositivos de rede



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.

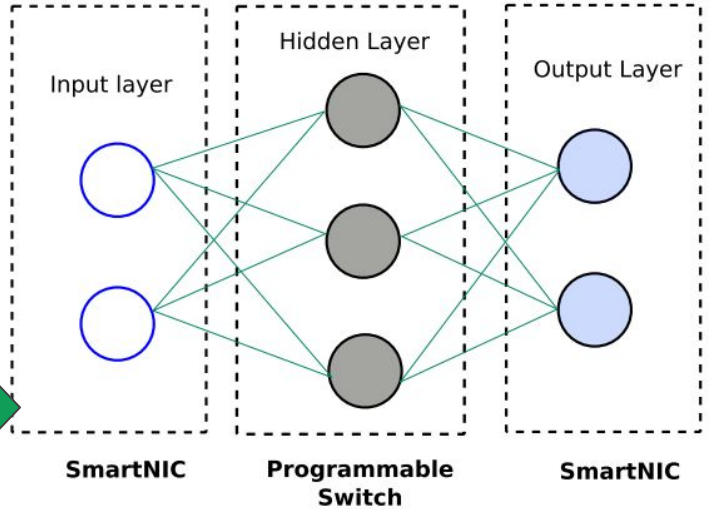
Limitações de programação do plano de dados

- Sem suporte:
  - **Loops**: devem ser decompostos em um pequeno conjunto de passos tratáveis
  - **Operações matemáticas não elementares e ponto flutuante**
  - **Alocação dinâmica de memória**
- Necessário adaptar algoritmos de IA (vários trabalhos existentes)

1. Yifan Yuan, Omar Alama, Jiawei Fei, *et al*. **Unlocking the Power of Inline Floating-Point Operations on Programmable Switches**. NSDI 2022.
2. Penglai Cui, Heng Pan, Zhenyu Li, *et al*. **Enabling In-Network Floating-Point Arithmetic for Efficient Computation Offloading**. IEEE Transactions on Parallel and Distributed Systems, vol. 33, no. 12, pp. 4918-4934, 2022.
3. Matthews Jose, Kahina Lazri, Jérôme François and Olivier Festor. **InREC: In-network REal Number Computation**. IM 2021.
4. Damu Ding, Marco Savi and Domenico Siracusa. **Estimating Logarithmic and Exponential Functions to Track Network Traffic Entropy in P4**. NOMS 2020.

Como contornar as limitações do hardware de rede?

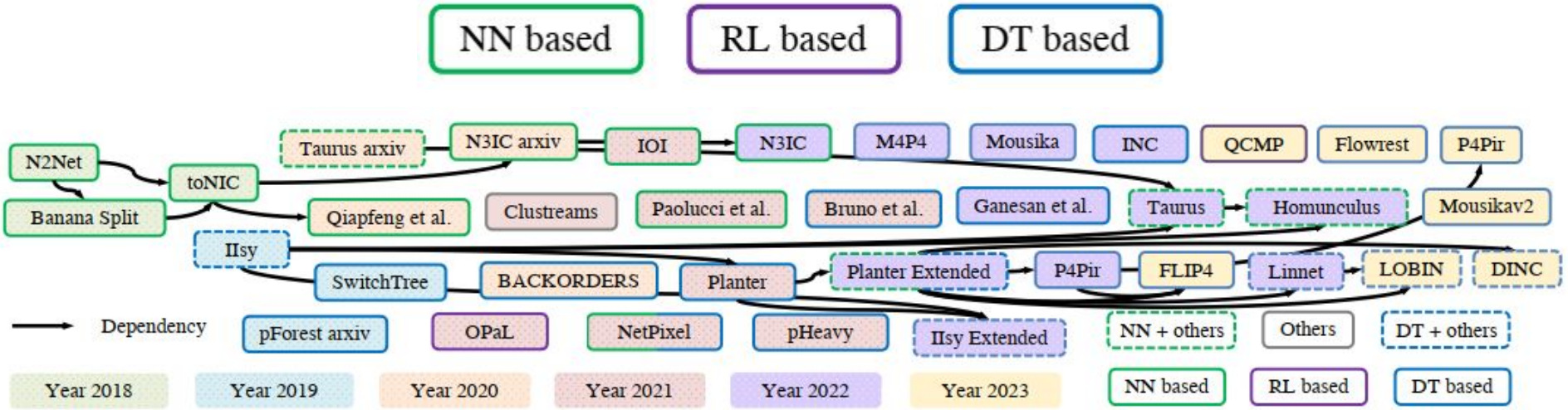
- Redução de modelo
  - **Perda de acurácia**
- Particionamento de modelo em diferentes camadas nos dispositivos de rede
  - **Complexidade**
- Paralelismo de dados com múltiplas instâncias nos dispositivos de rede
  - **Uso de recursos**



Parizotto, Ricardo, et al. "Offloading machine learning to programmable data planes: A systematic survey." ACM Computing Surveys 56.1 (2023): 1-34.

Trabalhos da Literatura (últimos 5 anos)

- NN: Neural Networks | RL: Reinforcement Learning| DT: Decision Tree
- Implementações abrangem todas as principais áreas
- Diferentes níveis de maturidade e baixa reprodutibilidade



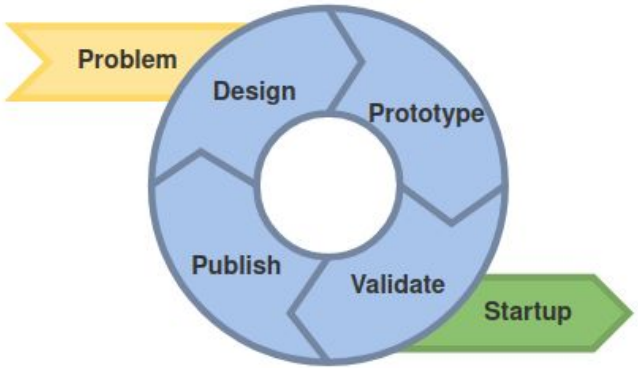
Zheng, Changgang, et al. "In-network machine learning using programmable network devices: A survey." IEEE Communications Surveys & Tutorials (2023).

Agenda

- Por que os desafios atuais de cibersegurança não conseguem ser resolvidos pelas redes atuais?
- O que são redes programáveis?
- Como IA e redes programáveis podem ser combinadas para resolver problemas de segurança?
- A nossa experiência no LabNERDS :-)
  - Como prototipar soluções com redes programáveis?
  - Aplicações

DNA do Grupo de Pesquisa LabNERDS

- Laboratório nasce da demanda por redes programáveis
- Prototipação como prova de princípio
- Participação na criação de infraestrutura de testbeds nacionais internacionais de pesquisa em redes
- Desenvolvimento de software de código aberto
- Amadurecimento para inovação



Como prototipar soluções com redes programáveis?

Plataformas para a realização de testes exaustivos, transparentes e replicáveis de novas técnicas: ***Testbeds***

Simulados

→ Resultados com baixa representatividade, mas permitem testes em larga escala (ex. NS3, OMINET++)

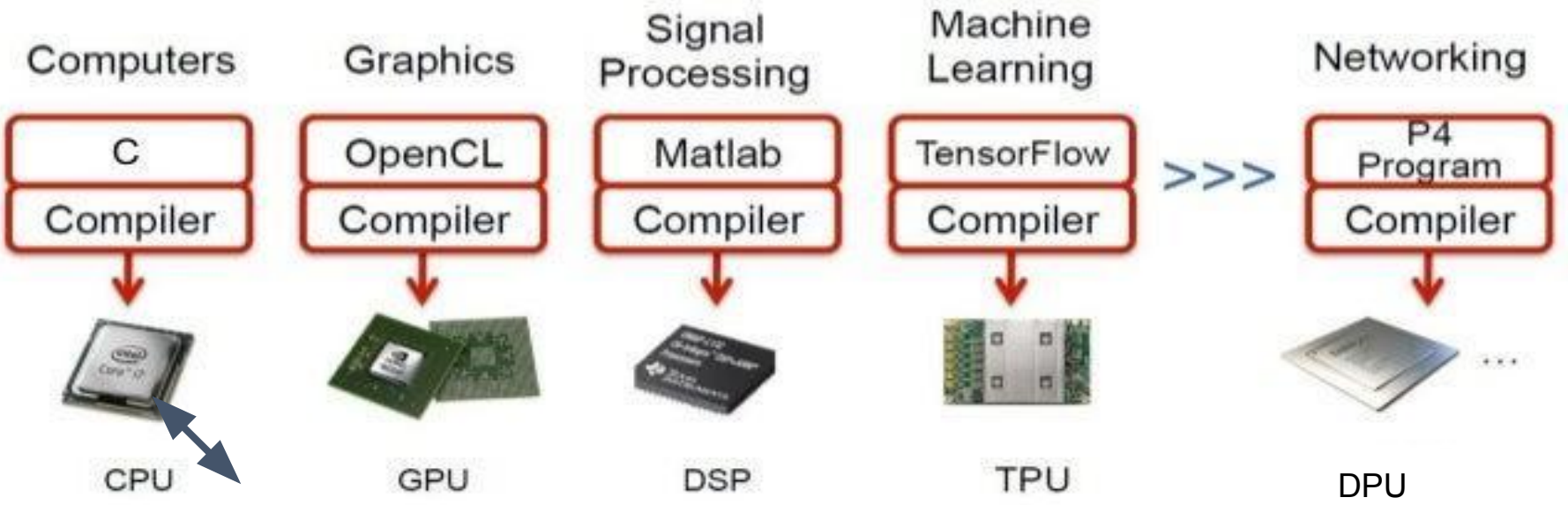
Emulados

→Resultados representativos (em alguns aspectos), mas não permitem testes em escalas sem demandarem custo excessivo em computação (ex. Mininet).

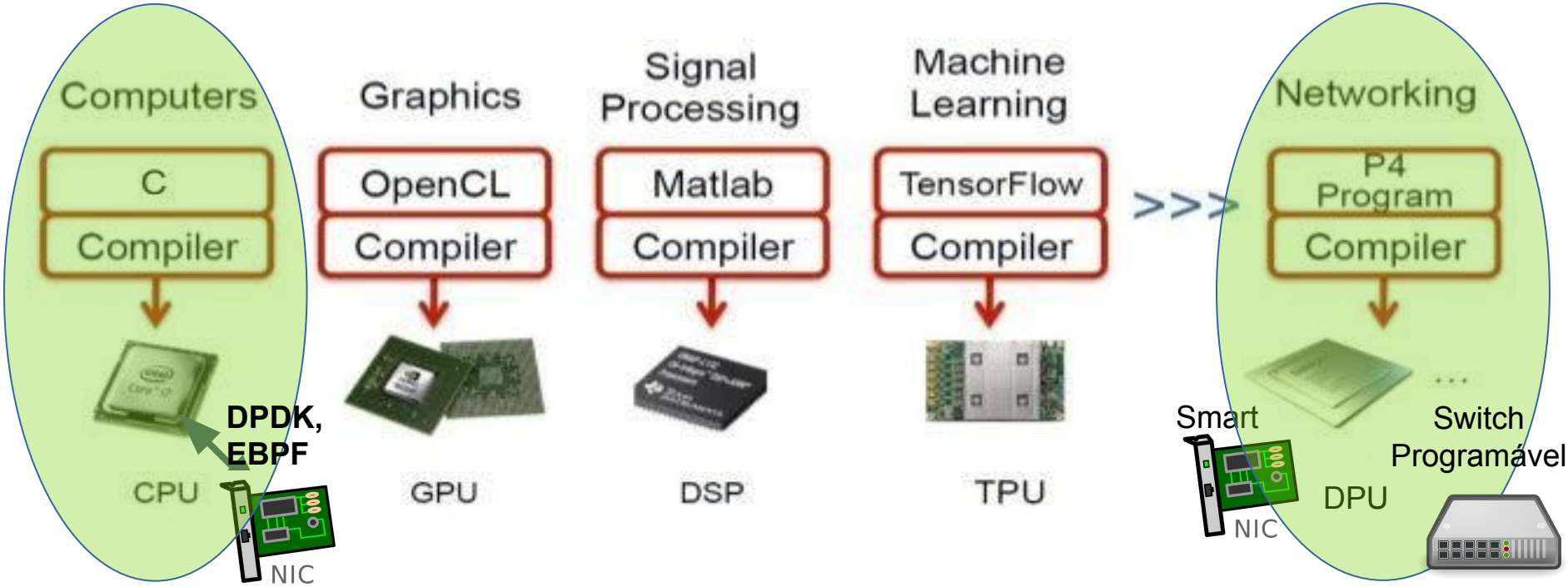
Físicos

→ Realismo garantido, todavia custo elevado e baixa escala se restrito à infra de uma instituição

Programabilidade de Dispositivos



Programabilidade de Dispositivos



Exemplo de Aplicações

- Proposta com maior impacto e maturidade:
  - PolKA: Polynomial Key-based Architecture for Source Routing
  - Extensão para prova de trânsito
- Proposta de pesquisa com foco IA e segurança:
  - In-network ML
  - Implantação de árvores de decisão em SmartNICs
  - Aplicação: Classificação de tráfego para mitigação de ataques

PolKA: Highlights

Networking

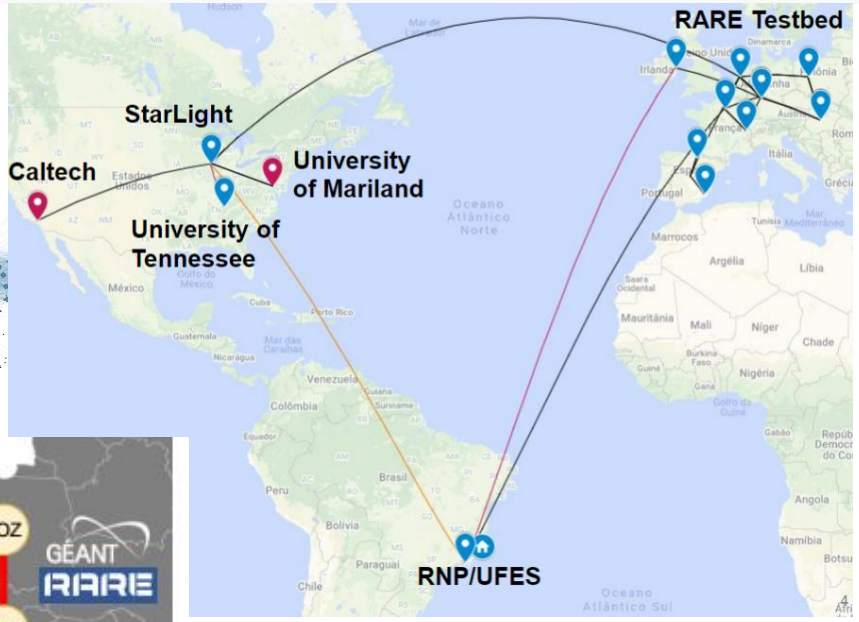
Google

Aurojit Panda, New York University
Bertha: Network APIs for the Programmable Network Era

Cristina Klippel Dominicini, Instituto Federal do Espirito Santo
Polynomial Key-based Architecture for Source Routing in Network Fabrics

Noa Zilberman, University of Oxford
Exposing Vulnerabilities in Programmable Network Devices

Rachit Agarwal, Cornell University
Designing Datacenter Transport for Terabit Ethernet



freeRtr

PolKA: motivação

- **Métodos de encaminhamento tradicionais baseados em tabela:**
  - Conjunto de caminhos mais curtos → Engenharia de tráfego 😕
  - Grande número de estados → Escalabilidade 😕
  - Latência para configuração de caminho → Agilidade 😕
  - Pouco controle na configuração de rotas → Segurança 😕

PolKA: motivação

- **Métodos de encaminhamento tradicionais baseados em tabela:**
  - Conjunto de caminhos mais curtos → Engenharia de tráfego
  - Grande número de estados → Escalabilidade
  - Latência para configuração de caminho → Agilidade
  - Pouco controle na configuração de rotas → Segurança

Subutilização

Ossificação

Pouco controle dos caminhos

Controle de congestionamento ruim

PolKA: motivação

- Alternativa: 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: Substituir tabelas por uma operação aritmética de **mod** (resto da divisão):

$$portID = < routeID >_{nodeID}$$

PolKA: Histórico

- **RNS inteiro: protótipo de software ou dispositivos NetFPGA especializados**
  - *M. Martinello et al., "Keyflow: a prototype for evolving SDN toward core network fabrics," in IEEE Network, 2014. (**RNS SR applied to core networks with SDN**)*
  - *R. R. Gomes et al., "KAR: Key-for-any-route, a resilient routing system," in 2016 IEEE/IFIP DSN. (**Fast-failure reaction with RNS SR**)*
  - *A. Liberato et al., "RDNA: Residue-Defined Networking Architecture Enabling Ultra-Reliable Low-Latency Datacenters," IEEE TNSM 2018. (**RNS SR applied to multicast in DC networks**)*

- C. K. Dominicini et al., "**PolKA: Polynomial Key-based Architecture for Source Routing in Network Fabrics**," IEEE NetSoft 2020.
  - RNS polinomial é mais aderente aos switches modernos com P4.
  - O P4 não suporta nativamente a operação de mod.
  - Solução: reuso do hardware CRC (Cyclic Redundancy Check) para mod polinomial.

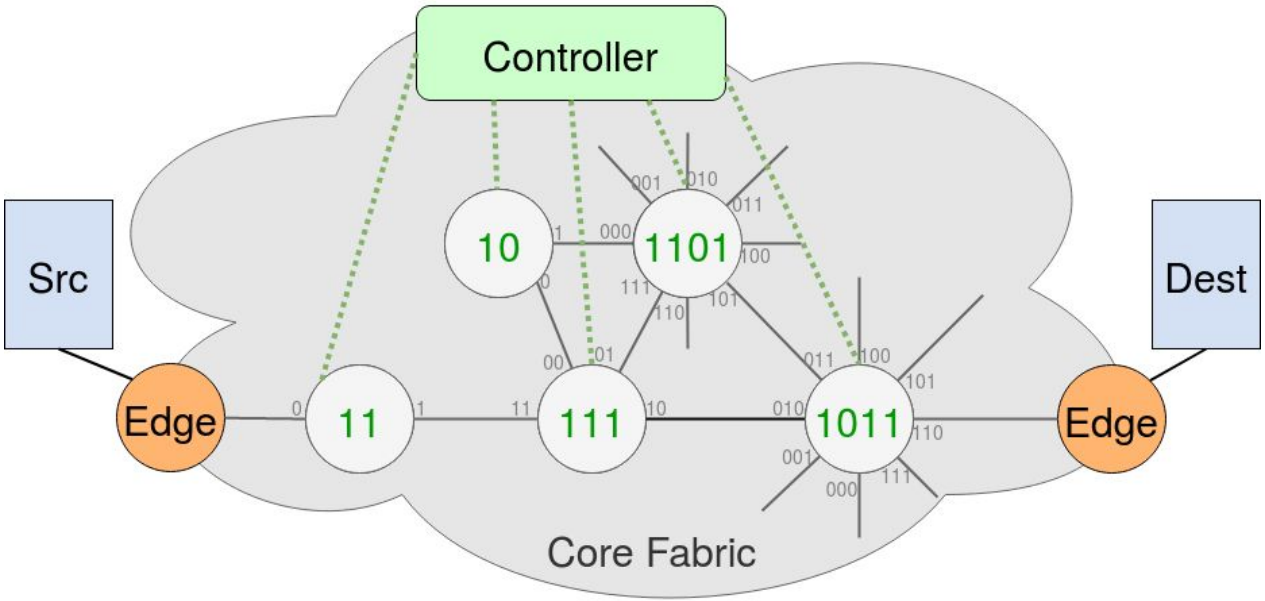
Como o PolKA funciona?

- Codificação de três identificadores polinomiais usando RNS:
  - **routeID**
  - **nodeID**
  - **portID**
- O encaminhamento usa uma operação de **mod** (resto da divisão):

$$portID = < routeID >_{nodeID}$$

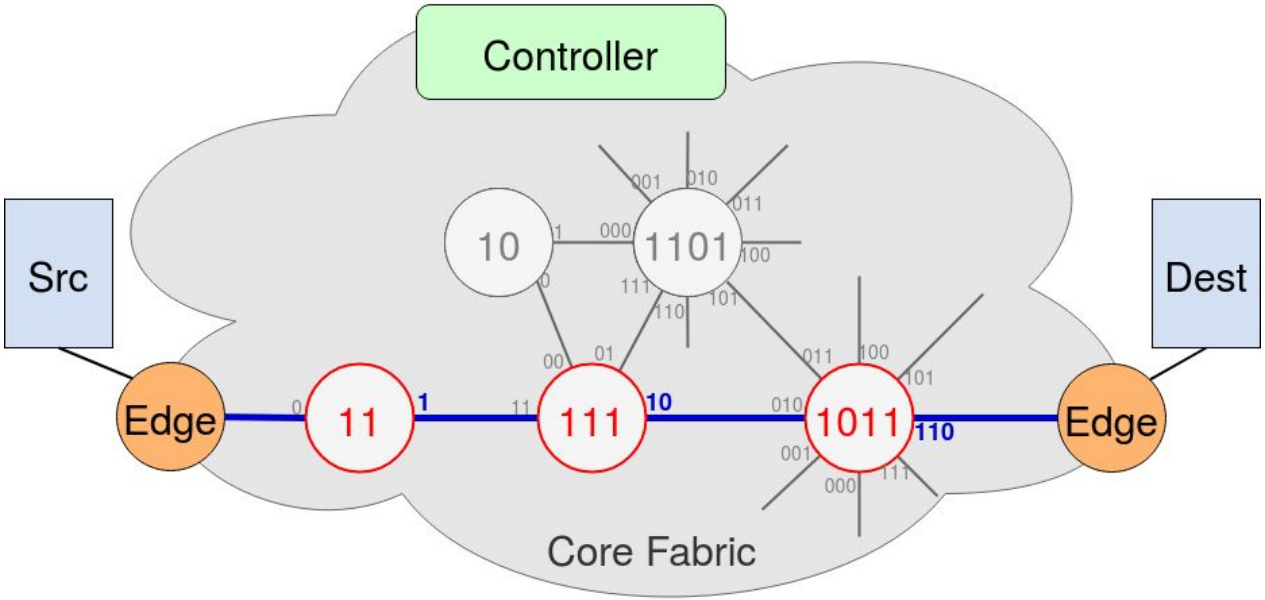
Como o PolKA funciona?

- O controlador configura polinômios para switches (**nodeIDs**) e portas (**portIDs**).



Como o PolKA funciona?

- O controlador escolhe o caminho para um fluxo:
  - Switches: {0011,0111,1011}
  - e portas de saída: {1 , 10, 110}



nodeIDs

$$s_1(t) = t + 1 = 11$$

$$s_2(t) = t^2 + t + 1 = 111$$

$$s_3(t) = t^3 + t + 1 = 1011$$

portIDs

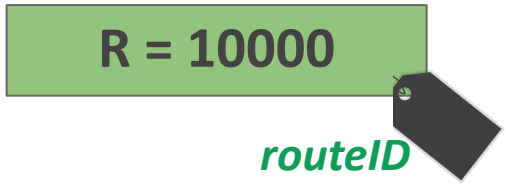
$$o_1(t) = 1$$

$$o_2(t) = t = 10$$

$$o_3(t) = t^2 + t = 110$$

Como o PolKA funciona?

- o **Controlador** calcula o ***routeID*** usando RNS:



- Encaminhamento:

portID = < routeID >$_{nodeID}$

1	=	$<10000>_{0011}$	: s_1
10	=	$<10000>_{0111}$	: s_2
110	=	$<10000>_{1011}$	: s_3

nodeIDs

$s_1(t) = t + 1 = 11$

$s_2(t) = t^2 + t + 1 = 111$

$s_3(t) = t^3 + t + 1 = 1011$

portIDs

$o_1(t) = 1$

$o_2(t) = t = 10$

$o_3(t) = t^2 + t = 110$

Cálculo routeID com RNS

$t^4 \equiv 1 \mod (t+1)$

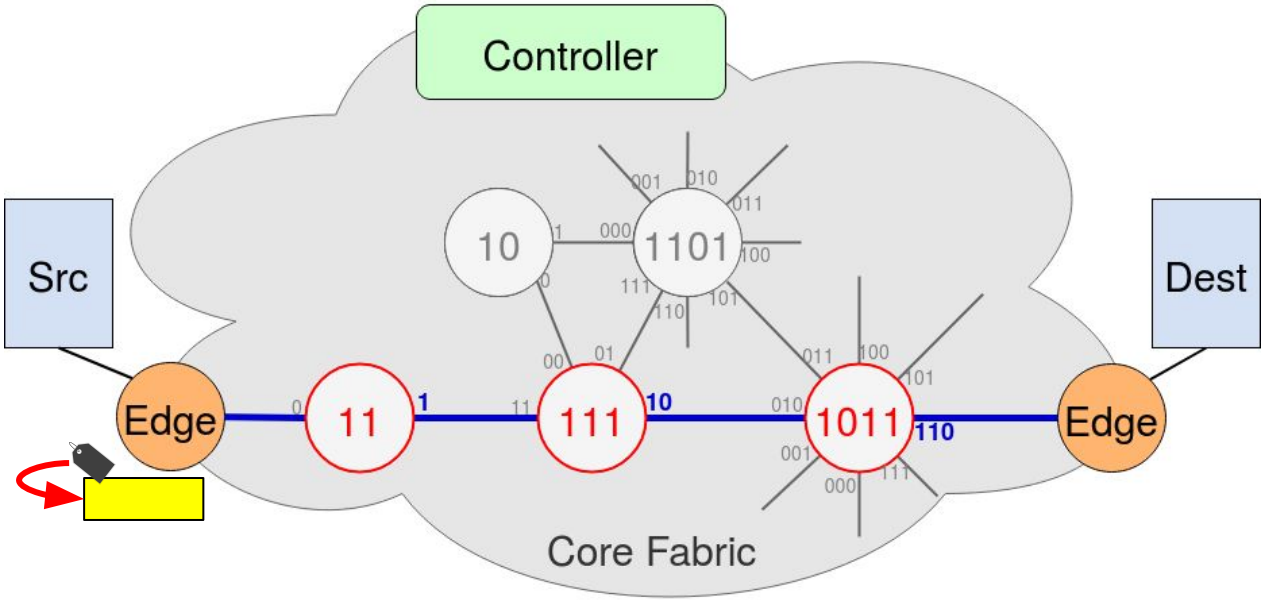
$t^4 \equiv t \mod (t^2+t+1)$

$t^4 \equiv (t^2+t) \mod (t^3+t+1)$

$t^4 = 10000$

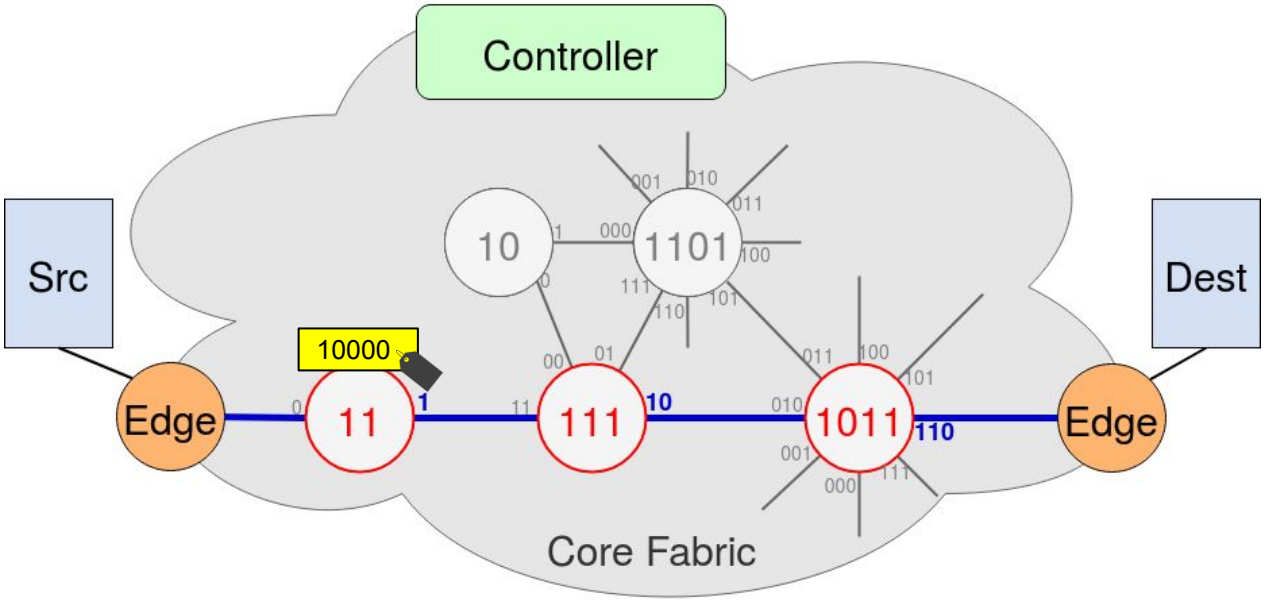
Como o PolKA funciona?

- Quando os pacotes chegam, o nó de entrada adiciona o routeID nos pacotes.



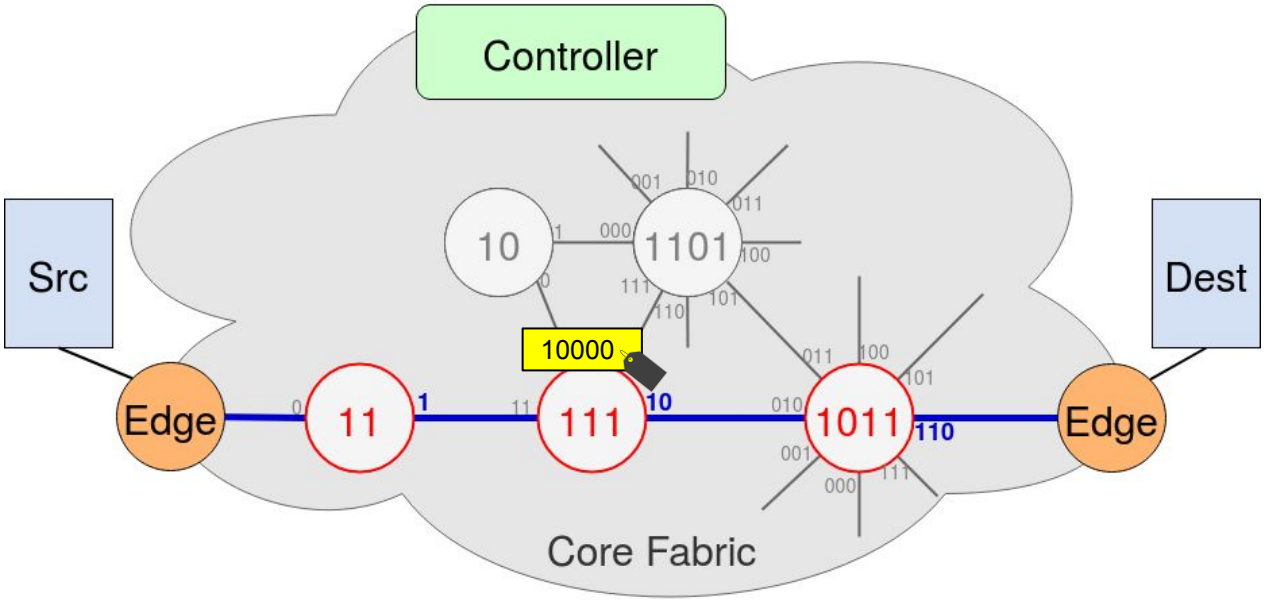
Como o PolKA funciona?

- Encaminhamento usando **mod**: $\langle 10000 \rangle_{0011}$ = 1 → porta de saída
- O *routeID* não muda! Sem tabelas!



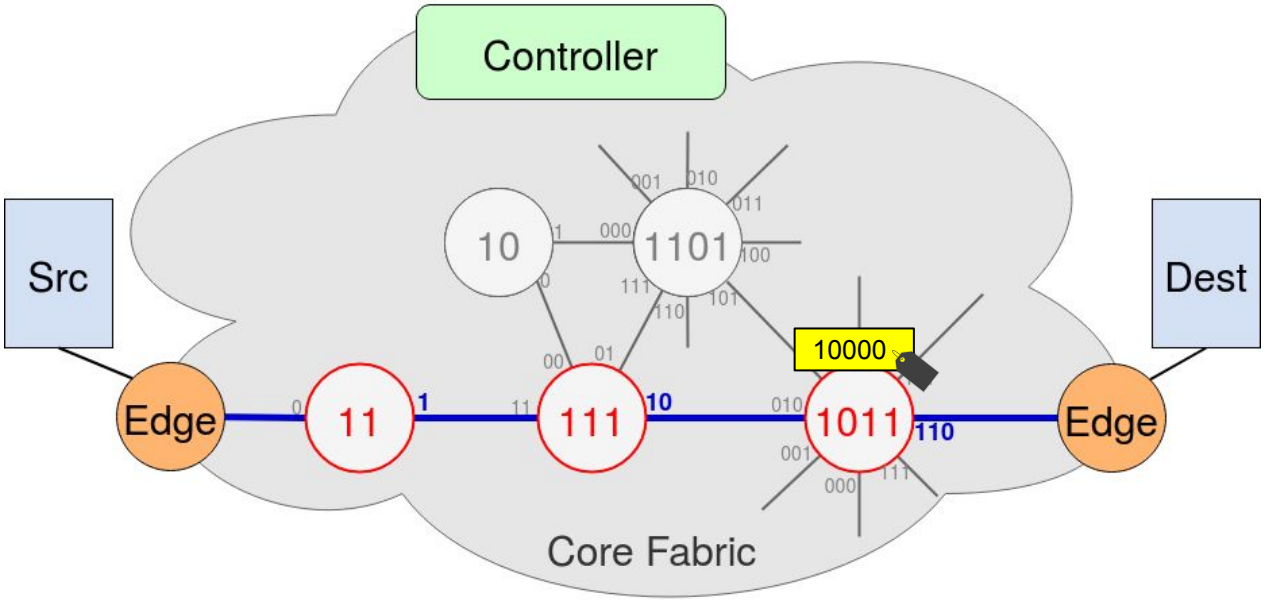
Como o PolKA funciona?

- Encaminhamento usando **mod**: $\langle 10000 \rangle_{0111}$ = 10 → porta de saída
- O *routeID* não muda! Sem tabelas!



Como o PolKA funciona?

- Encaminhamento usando **mod**: $\langle 10000 \rangle_{1011}$ = 110 → porta de saída
- O *routeID* não muda! Sem tabelas!



Timeline

O projeto PolKA recebeu o prêmio 2021 Google Research Scholar Award

O projeto M-PolKA recebeu o prêmio Intel Connectivity Research Grant (Fast Forward Initiative)

2020

PolKA paper IEEE NetSoft

Novel Polynomial RNS-based SR and reuse of CRC hardware

Emulated prototype in Mininet

2021

ONDM paper Deploy @RARE

Hardware prototype in Tofino

Integration RARE+FreeRtr

PolKA data & control plane implementation + integration

Emulated prototype in FreeRtr &

Hardware prototype in Tofino w/ FreeRtr control plane

2022

M-PolKA paper IEEE TNSM

Extension to multipath SR for reliable communications

PolKA@pangr IETF 113

Lightning Talk Path Aware Networking RG

PolKA@Global P4 Lab

PolKA deployment @Caltech SDN Lab

PolKA Demo at SC-22

2023/2024

INT-PolKA paper AINA

Extension to inband network telemetry

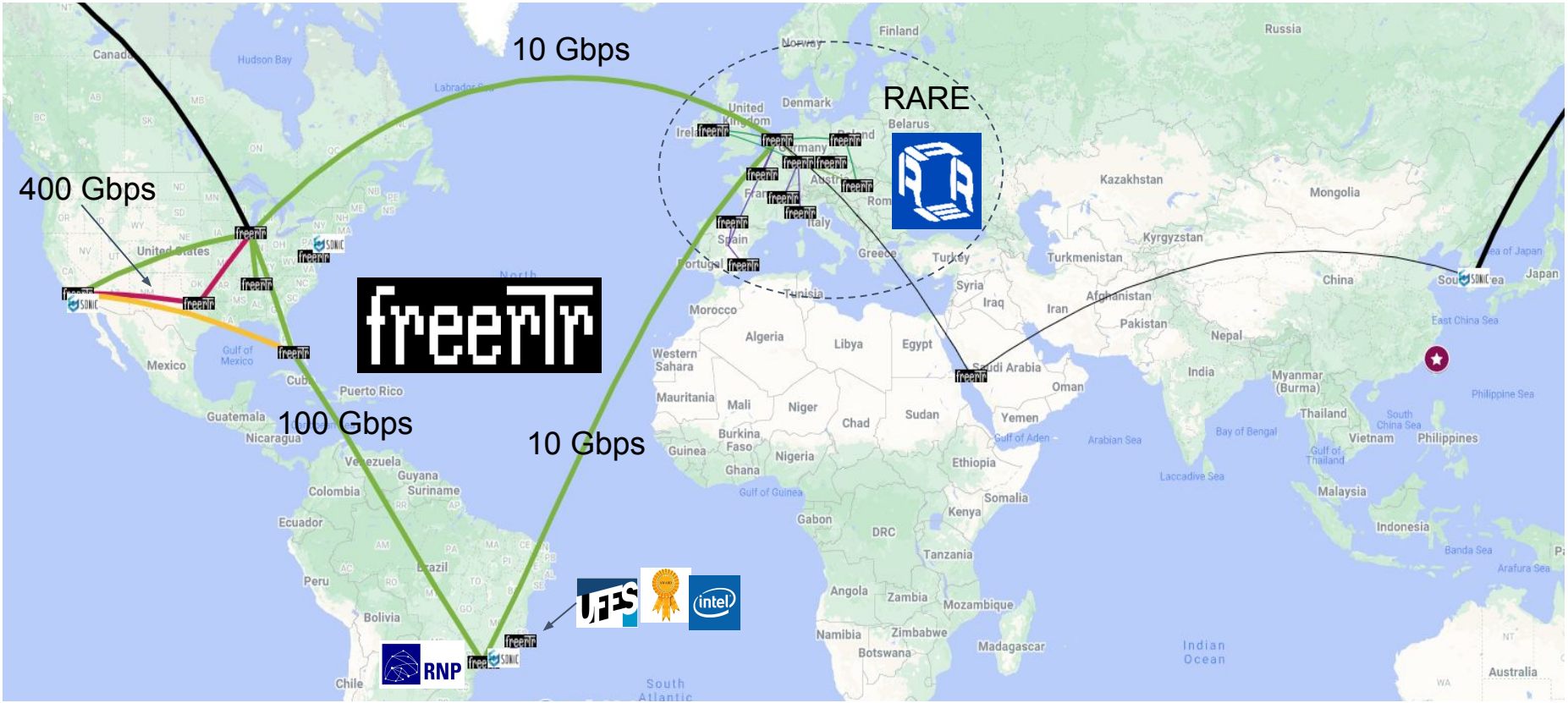
PoT-PolKA paper IEEE NetSoft/TNSM

Extension to proof-of-transit

PolKA AI paper Indis

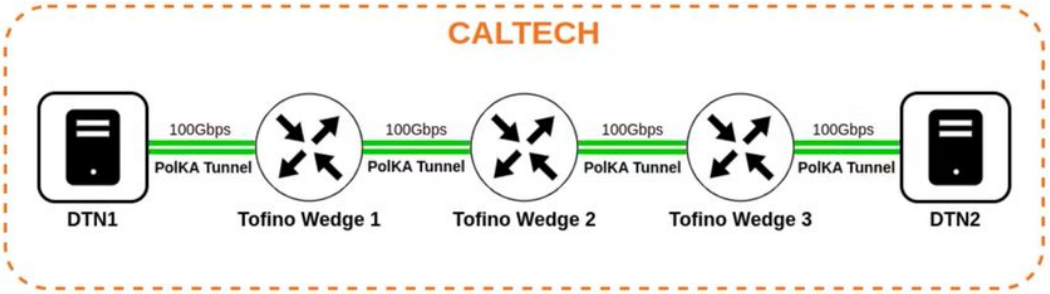
Extension to data science scenario with AI control plane

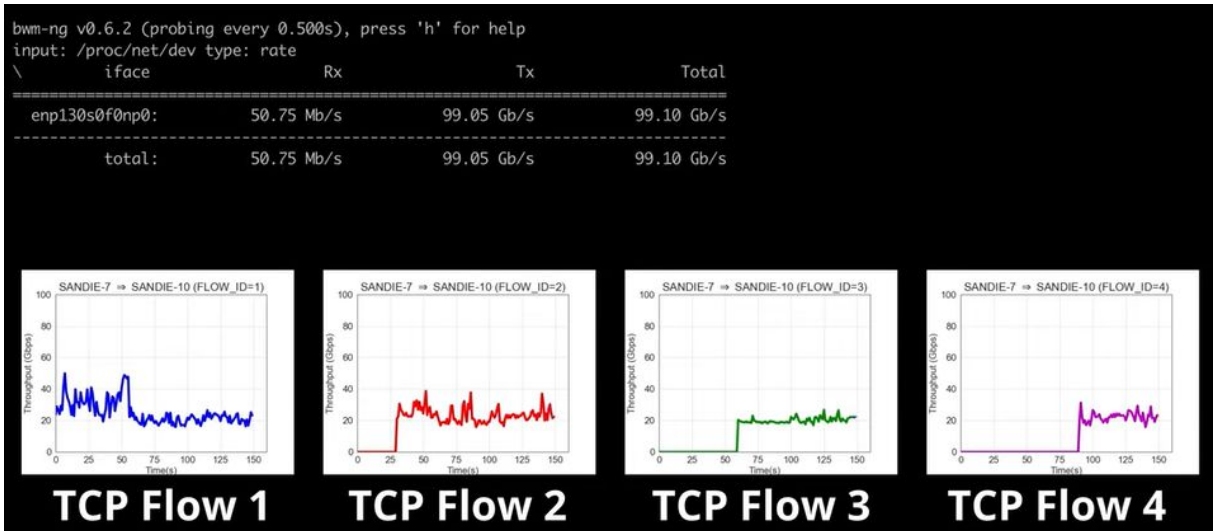
PolKA integrado no freerTr OS + UFES parte do Global P4 Testbed



Data Science Group - PolKA Demo @SC23

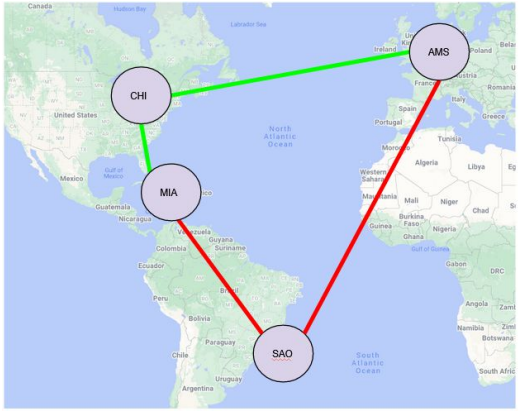
- **Grandes streams de dados com vazão de 100 Gbps**
  - Caltech P4 lab testbed
  - Vários fluxos TCP agregados direcionados para túneis pré-configurados

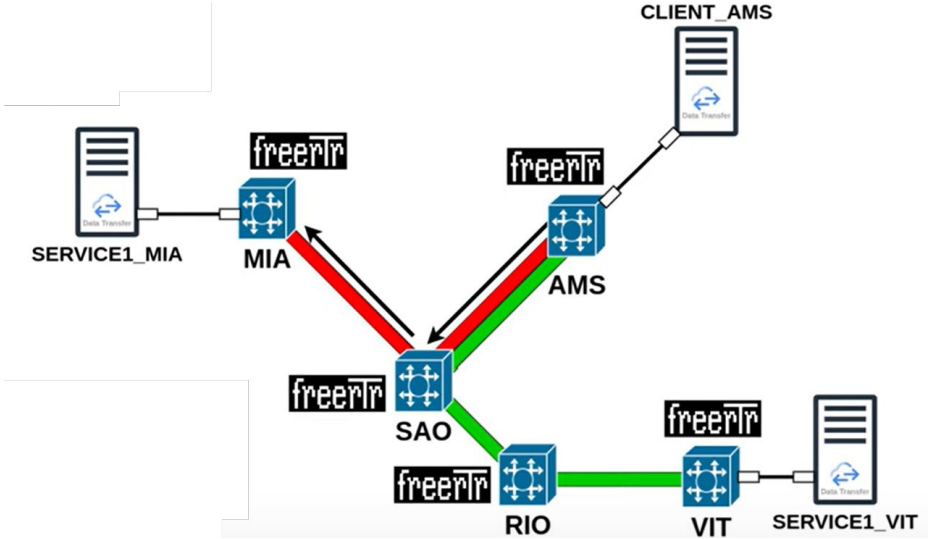


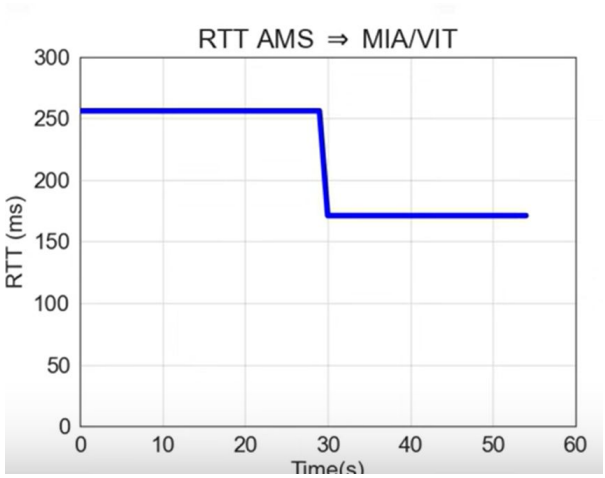


Data Science Group - PolKA Demo @SC23

- **Migração ágil de caminhos em Testbed Intercontinental**
  - Global P4 lab testbed
  - Configuração de túnel para engenharia de tráfego
  - Define um caminho explícito (routeID)
  - A migração para outro túnel requer uma única atualização na origem do tráfego

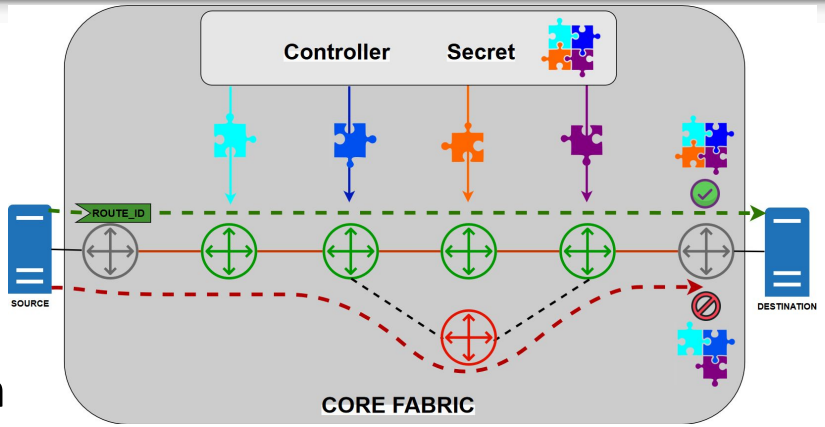






Extensão de segurança: Prova de Trânsito

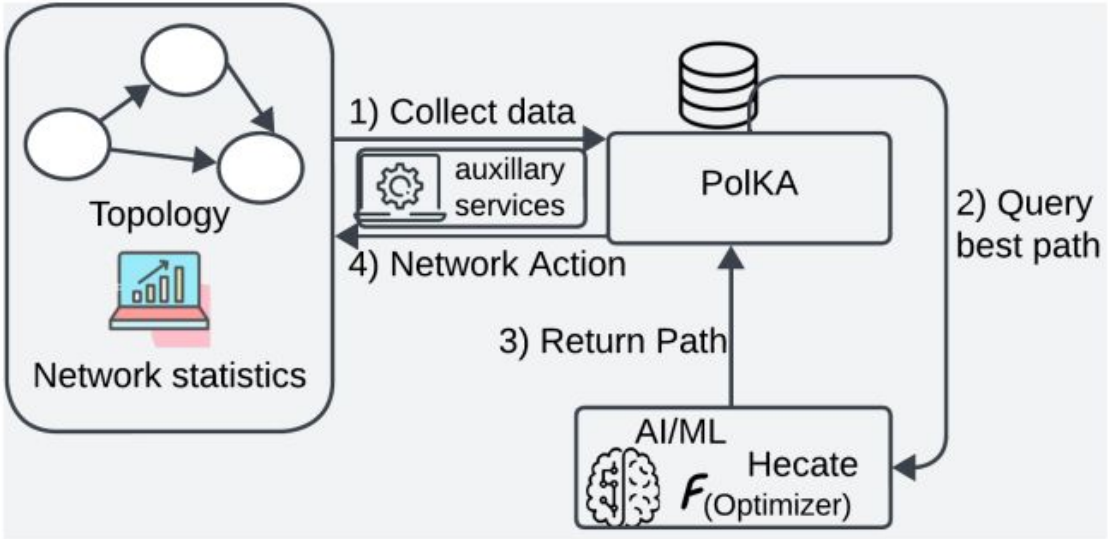
- **Proof of Transit (PoT)**: capacidade de provar que os pacotes passaram por um conjunto de nós de rede.



- **PoT-PolKA:**
  - 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
- **Trabalhos em andamento: autenticidade de rota**

PolKA: Plano de Controle com IA

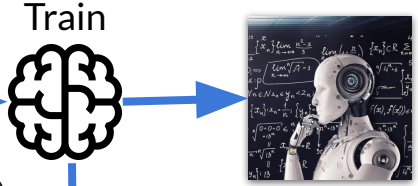
- Integração de métodos de aprendizado de máquina para previsão de caminhos otimizados para os fluxos.



Exemplo de Aplicações

- Proposta com maior impacto e maturidade:
  - PolKA: Polynomial Key-based Architecture for Source Routing
  - Extensão para prova de trânsito
- Proposta de pesquisa com foco IA e segurança:
  - In-network ML
  - Implantação de árvores de decisão em SmartNICs
  - Aplicação: Classificação de tráfego para mitigação de ataques

Aplicação: Classificação de tráfego para mitigação de ataques



Train

Feedback

Machine Learning

Closed Control Loop

Deploy

NETFLIX

NETFLIX

Benign Traffic

Malicious Traffic

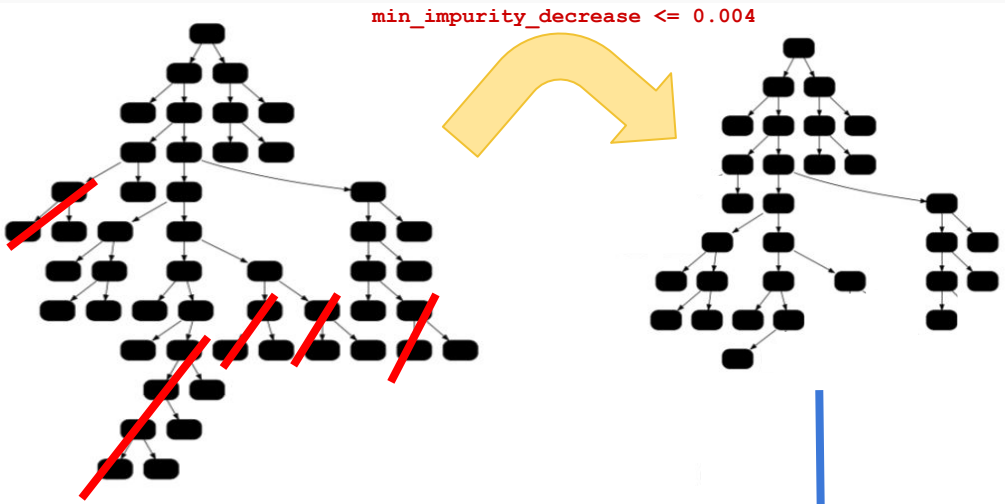
ATTACKER

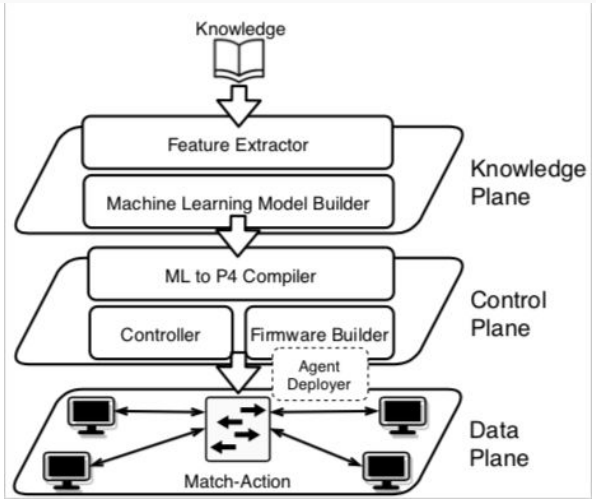
In-network ML: Árvores de decisão em SmartNICs

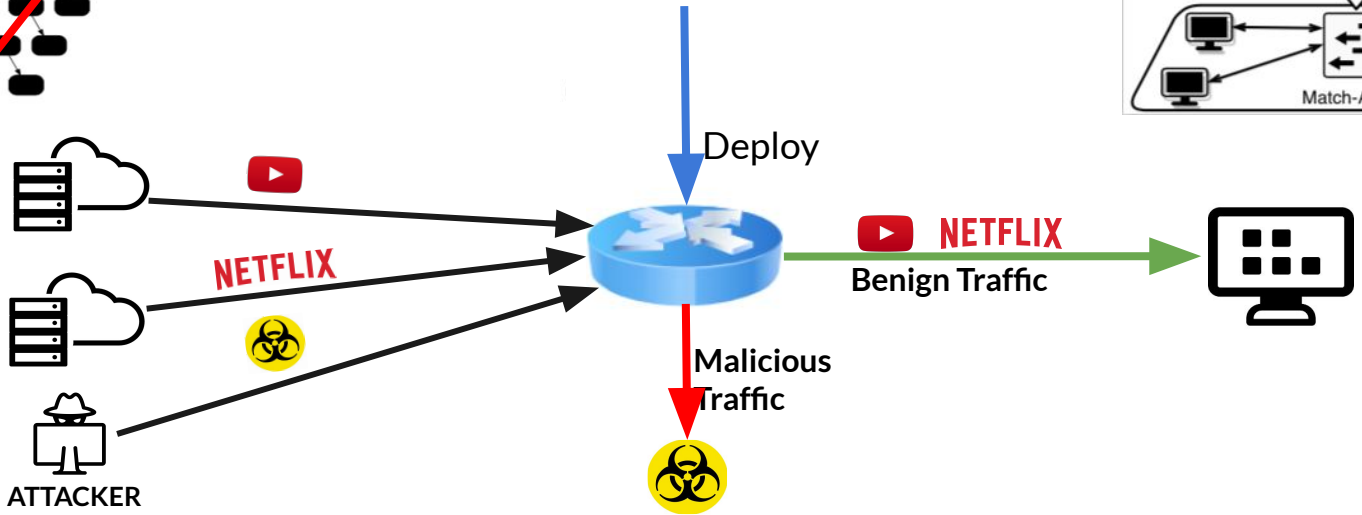
- **Tese de Doutorado Bruno Missi Xavier**
  - Título: Crossing Domains for Accuracy: In-Network Stacking of Machine Learning Classifiers, Ano de obtenção: 2024.
  - Orientador: Magnos Martinello (UFES)
  - Coorientador: Marco Ruffini (TCD, Irlanda)

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

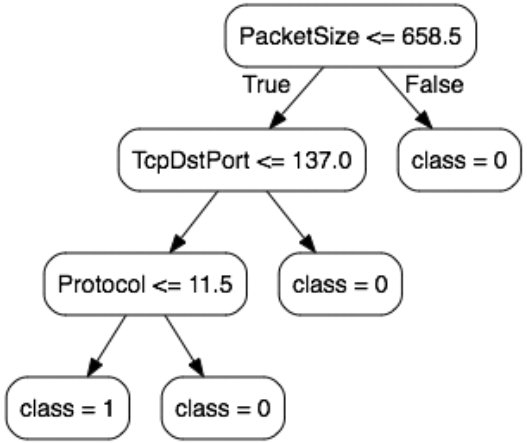
In-network ML: Árvores de decisão em SmartNICs







In-network ML: Árvores de decisão em SmartNICs



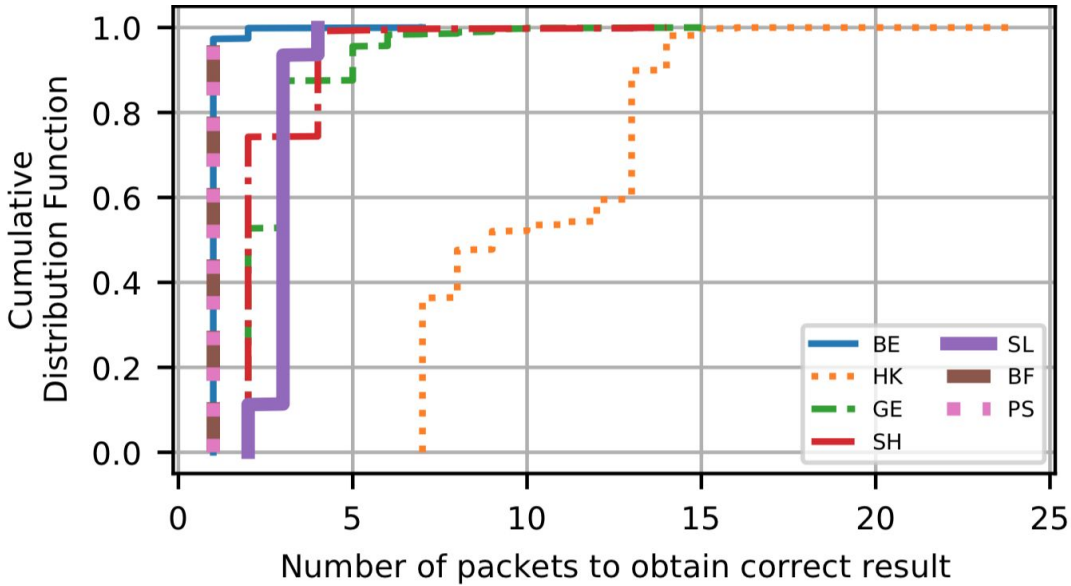

```
if (hdr.ipv4.totallen <= 658.5)
  if (hdr.tcp.dstport <= 137.0)
    if (hdr.ipv4.protocol <= 11.5)
      meta.class = 1;
    else
      meta.class = 0;
  else
    meta.class = 0;
else
  meta.class = 0;
```

```
...
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**

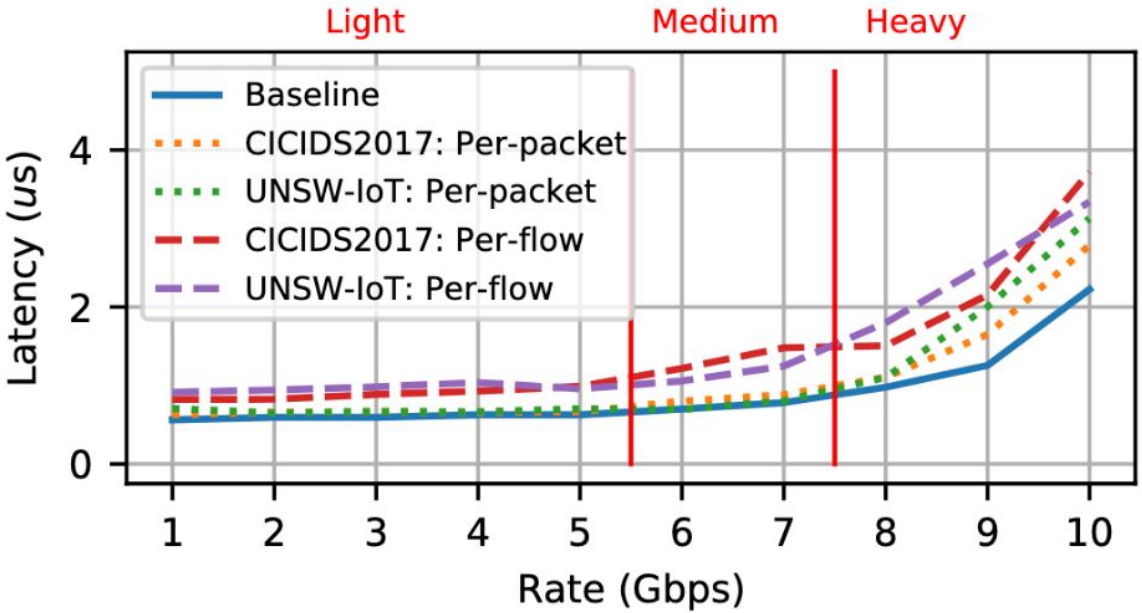
DTs em SmartNICs: Classificação de tráfego para mitigação de ataques

- A maioria dos trabalhos recentes ignoram a natureza dinâmica de um ataque.
- Mostramos em uma smartNIC que com um pequeno número de pacotes é possível classificar o tráfego com precisão.



DTs em SmartNICs: Classificação de tráfego para mitigação de ataques

- O classificador não é um gargalo, operando em taxa de linha.
- Mesmo para cargas de trabalho pesadas, as latências ficam abaixo de 3µs e permanecem gerenciáveis.



Conclusões

- É possível desenvolver **soluções de alto desempenho para equipamentos de rede programáveis.**
- Os exemplos destacam o **impacto da integração entre redes programáveis e IA**, enfatizando o papel inovador da **prototipação** em redes programáveis de alto desempenho.
- As soluções têm explorado a **programabilidade de redes para abordar desafios de segurança** e impulsionado avanços significativos na área.
  - Potencial para habilitar uma nova gama de aplicações complexas de segurança de redes.
  - **Muitas oportunidades de pesquisa e inovação!**

Obrigada!

Cristina Klippel Dominicini

cristina.dominicini@ifes.edu.br

** This work was a recipient of the 2021 Google Research Scholar and the 2022 Intel Connectivity Research Grant (Fast Forward Initiative) Awards, and received funds from CAPES (Finance Code 001), CNPq, FAPESP, FAPES, CTIC, and RNP.*

INSTITUTO FEDERAL
Espírito Santo

UFES