



**HAL**  
open science

## Analyzing encrypted traffic using AI models

Louis Poidevin, Françoise Sailhan, Johanne Vincent

► **To cite this version:**

Louis Poidevin, Françoise Sailhan, Johanne Vincent. Analyzing encrypted traffic using AI models. Winter training school: AI for Digital Infrastructure – Digital Infrastructure for AI, Nov 2024, Villeneuve d'Ascq, France. hal-04800387

**HAL Id: hal-04800387**

**<https://hal.science/hal-04800387v1>**

Submitted on 24 Nov 2024

**HAL** is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.



Distributed under a Creative Commons Attribution 4.0 International License

# Analyzing encrypted traffic using AI models

A distributed and in-network approach

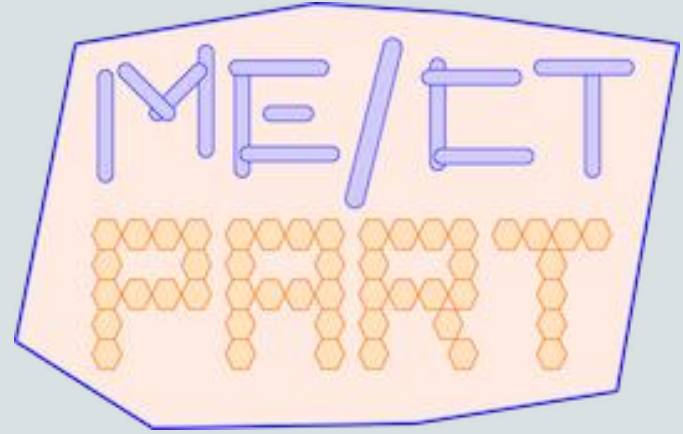
## Affiliation



## Authors

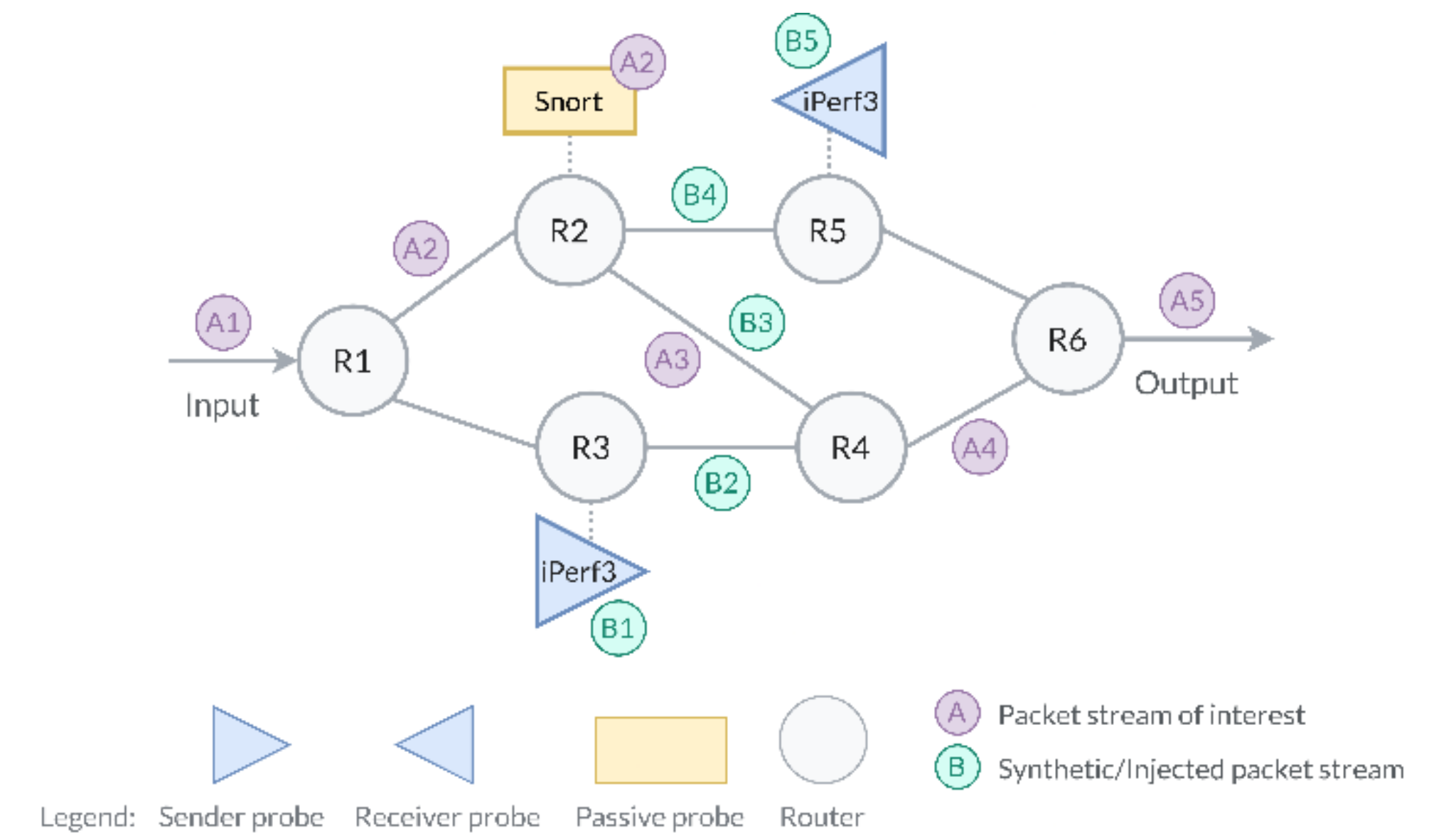
Louis Poidevin  
Francoise Sailhan  
Johanne Vincent

## Funding



## Traffic Analysis

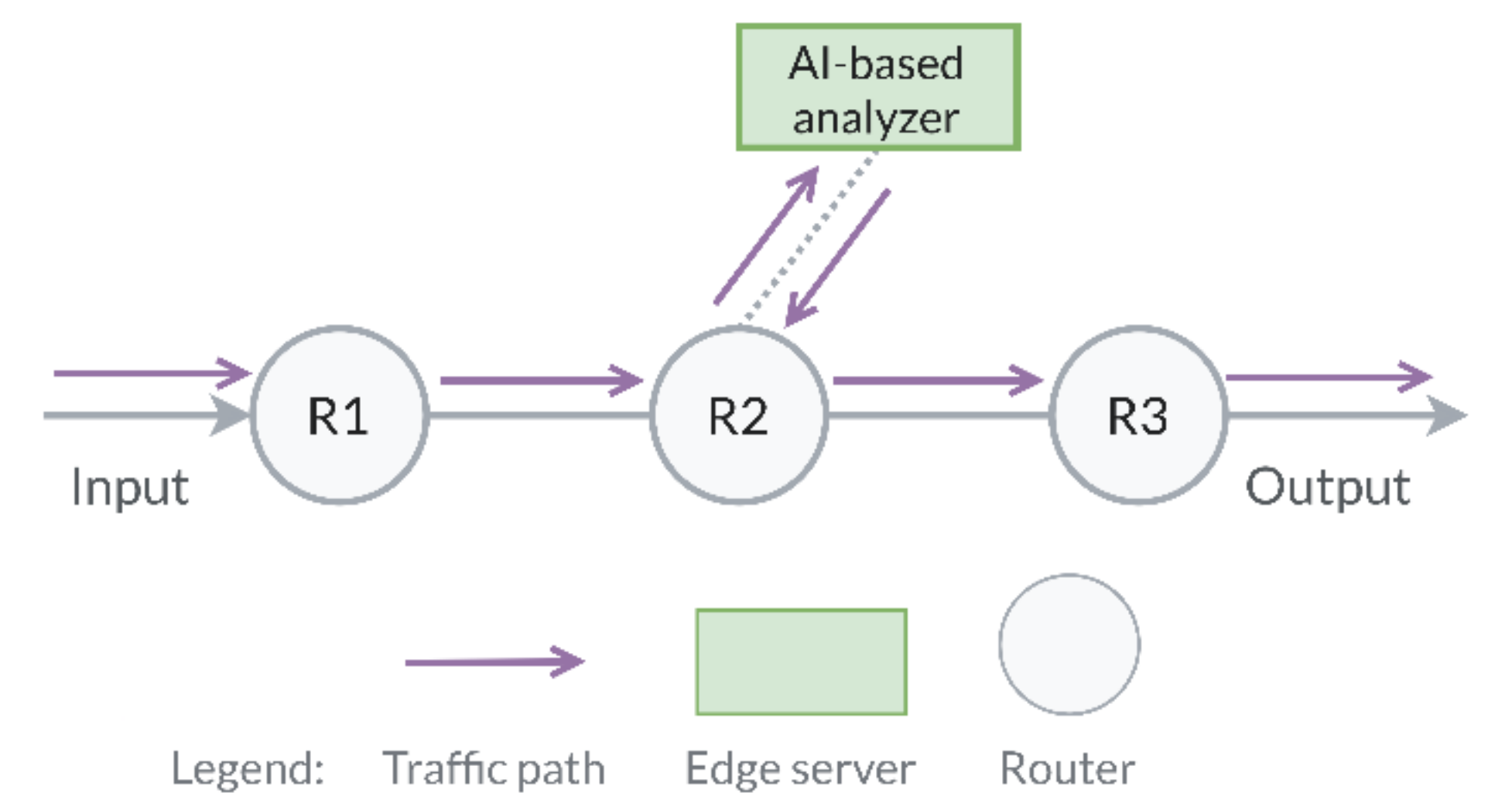
- ▶ Traffic analysis is essential for network operators to enhance **performance**, address **security** issues, manage **bandwidth**, and improve **Quality of Service (QoS)**.
- ▶ Traffic analysis methods include:
  - **Active monitoring**: generating and observing synthetic packet streams.
  - **Passive monitoring**: observing natural traffic streams without alteration.
  - **Hybrid approaches**: combining active and passive techniques for comprehensive insights.



Active vs. Passive Network Monitoring

## Challenges of Encrypted Traffic Analysis

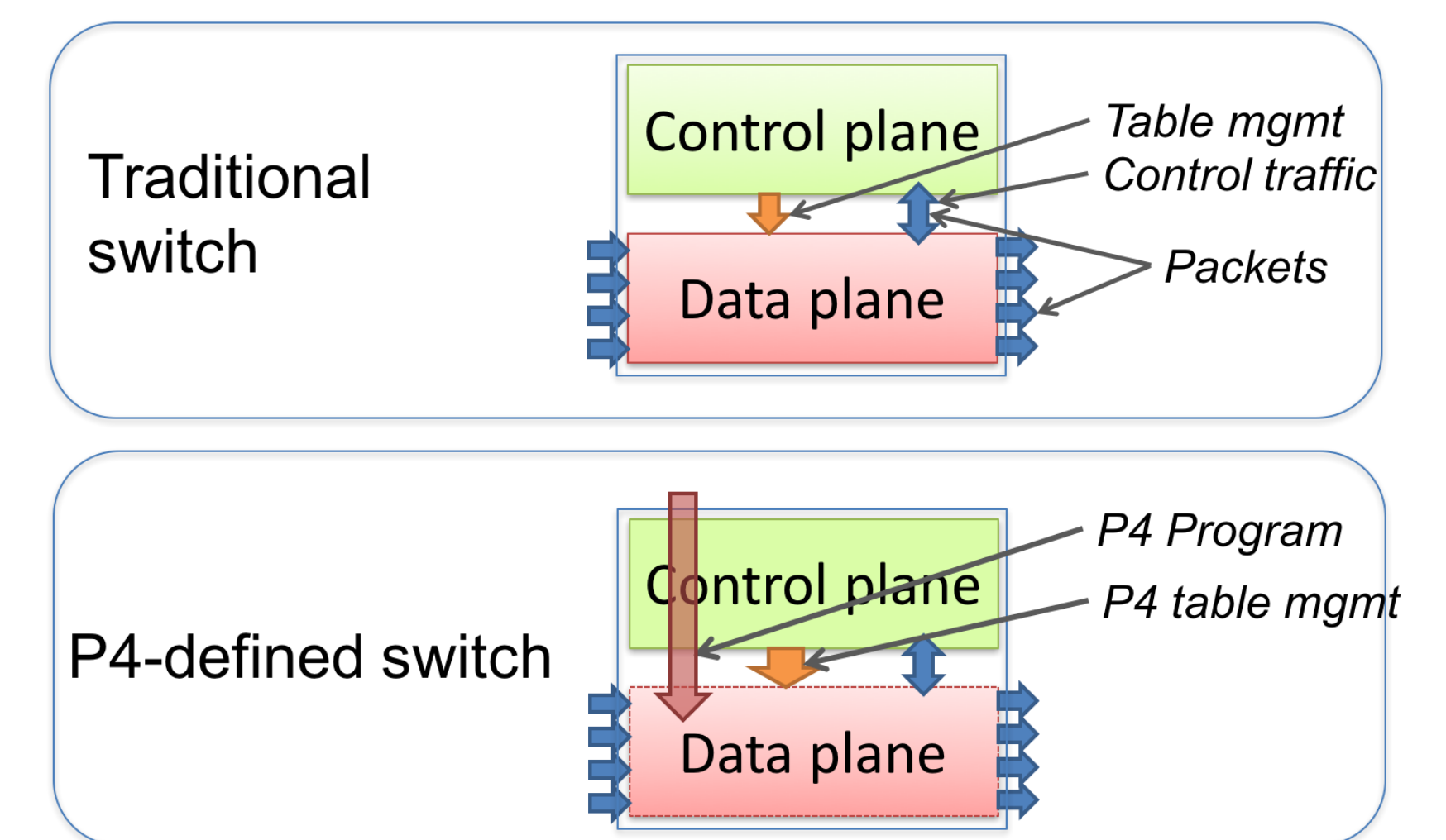
- ▶ The widespread encryption of internet traffic necessitates adaptation of network analysis tools.
- ▶ Traditional packet inspection methods are ineffective on encrypted traffic, requiring alternative approaches.
- ▶ **AI-based analyzers** offer solutions by classifying traffic based on packet statistics and behavioral patterns.
- ▶ However, AI-based analyzers have limitations in **throughput capacity** and **latency** due to their reliance on inference servers.



Traditional AI inference architecture

## In-Network Computing: Pros and Cons

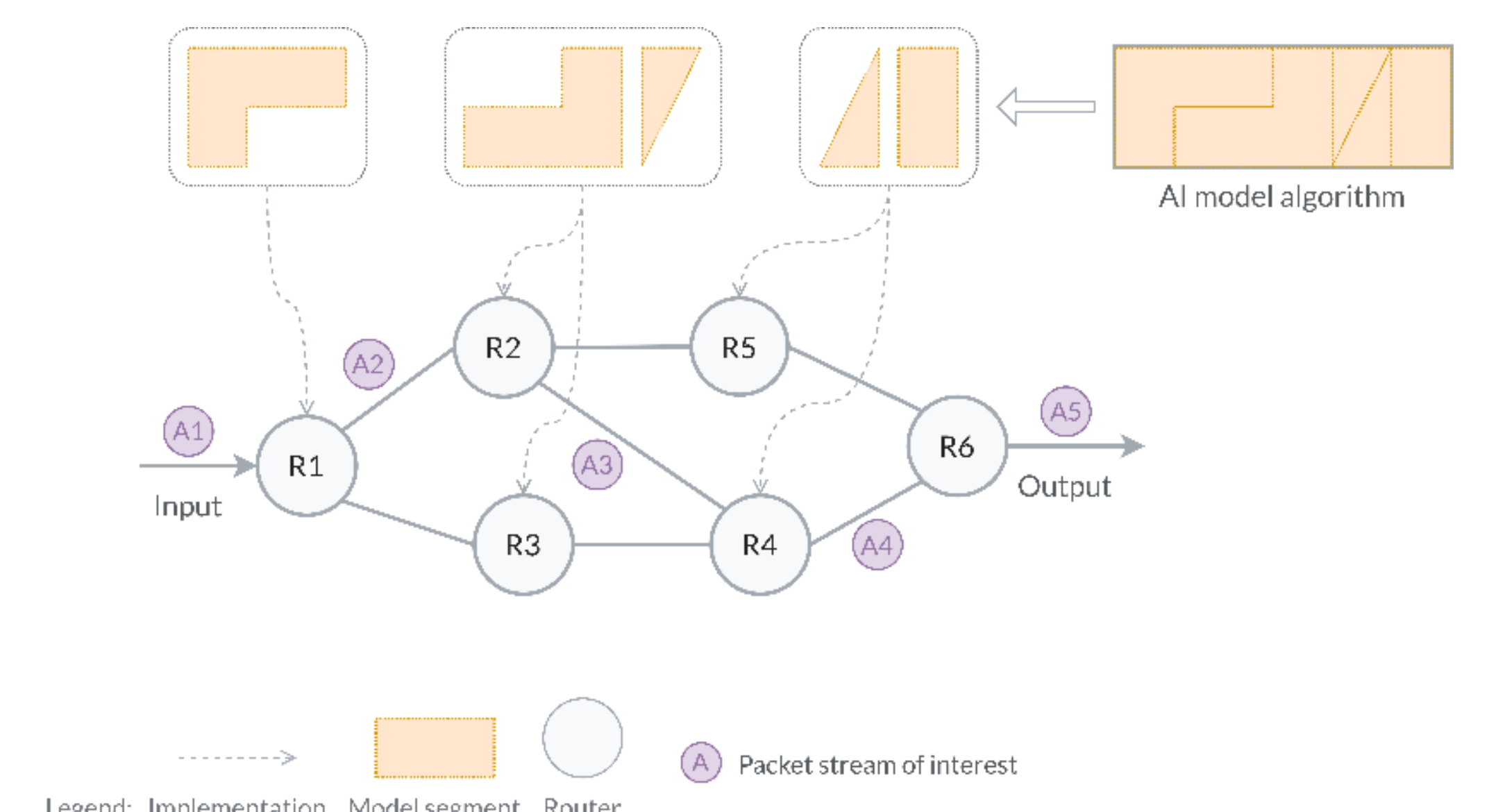
- ▶ To overcome AI model limitations, in-network computing deploys AI models directly on programmable network devices.
- ▶ This approach enables **high-performance**, **real-time processing** by offloading tasks from servers.
- ▶ Despite these advantages, programmable devices face significant constraints:
  - **Memory limitations** and restricted **data type support**.
  - Limited **computational capacity** optimized primarily for high-rate packet processing.
- ▶ Large AI models also present **coexistence challenges** with network operating systems (e.g., RARE).



Traditional vs. programmable switches  
Source: P4<sub>16</sub> Language Specification

## Distributed and In-Network AI Inference for Encrypted Traffic Analysis

- ▶ To address resource constraints, [Zheng+23] propose to **decompose target programs** into segments and **distribute** them across network devices.
- ▶ We intend to apply this approach to our AI-based analyzer, achieving **line-rate traffic analysis** with minimal accuracy degradation.
- ▶ Our study will focus on the **QUIC protocol**, considered as a complex case in encrypted traffic classification.
- ▶ Additional investigations will address unique challenges in **data center** environments, **SDN/multi-tenant** networks, and assess the **energy efficiency** of the analyzer.



Distributed in-network computing paradigm

[Zheng+23] C. Zheng et al. *DINC: Toward Distributed In-Network Computing*. ACM CoNEXT, 2023.