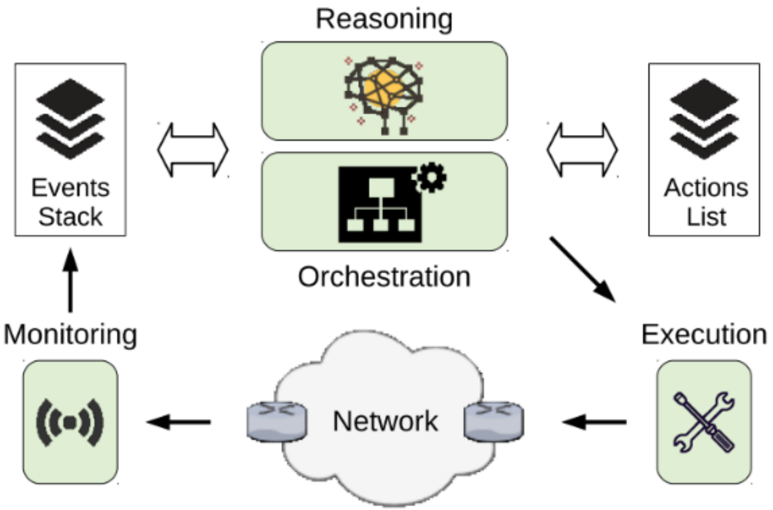
Automated defense system for cybersecurity

Elkin Aguas, Anthony Lambert, Hervé Debar, Grégory Blanc

Orange Labs, Châtillon, France
Télécom SudParis, Institut Polytechnique de Paris,
Evry-Courcouronnes, France

Journée des doctorants IP Paris (Département Informatique, Données et Intelligence Artificielle)
June 2021

An Event-Driven Network Automation Solution



General EDNA architecture: main components are written in bold, while implementation details are in italic.

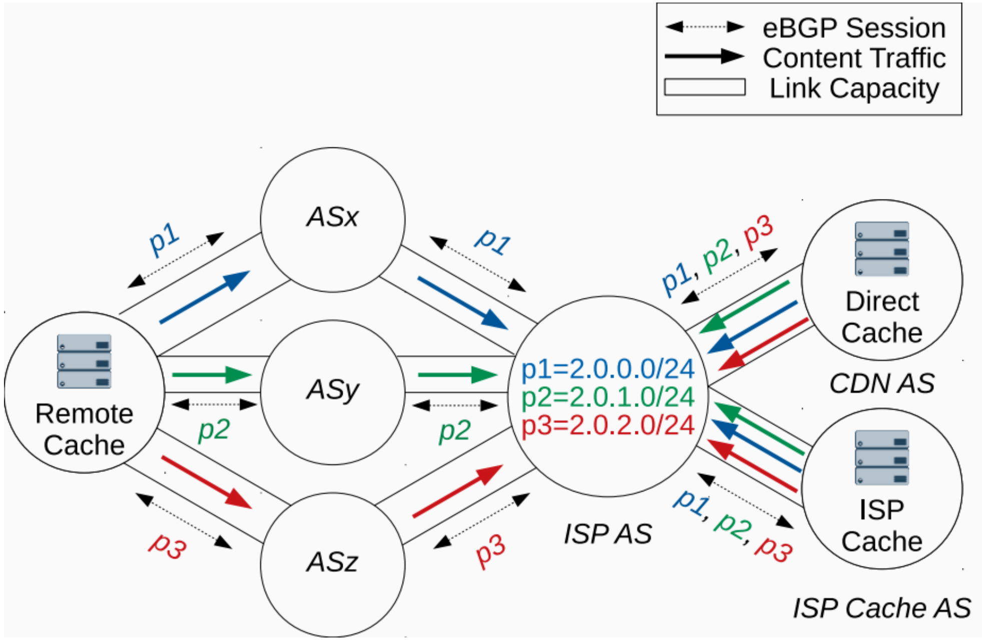
Reasoning block:
- Uses a *Deep Reinforcement Learning* (Deep Q-Learning) Algorithm.

- *Environment*: Max. traffic capacity, number of prefixes and traffic volume on each link.

- *Actions*: move one or more prefixes from one link to another.

CDN and Load Sharing Use Case

Content Delivery Networks' (CDNs) complex and dynamic delivery strategies → Internet Service Providers (ISPs) → "dumb pipes" → This can cause link saturation that lead to different problems

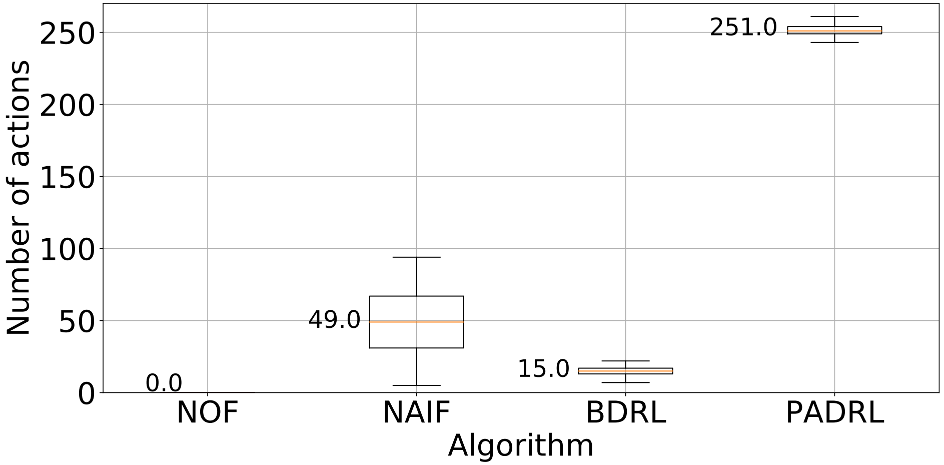


Saturation avoidance through Prefix Load Sharing

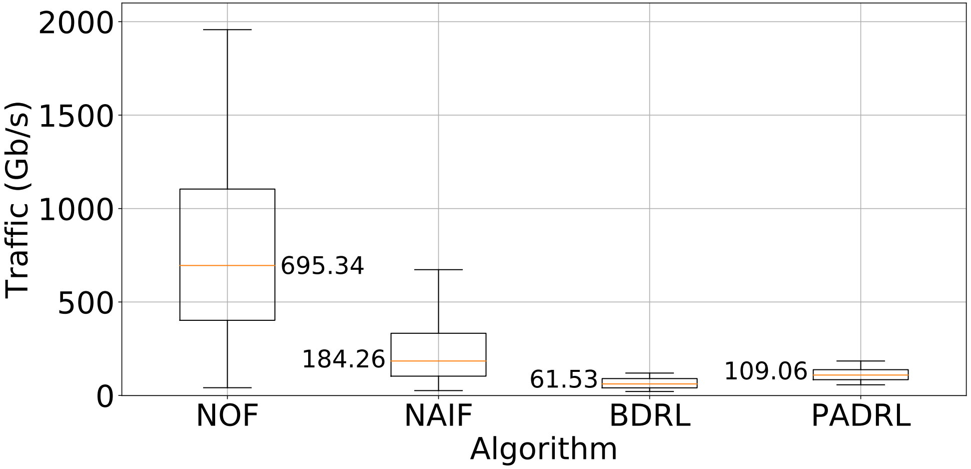
Results

No-function (**NOF**) algorithm
Naive function (**NAIF**) algorithm
Balanced DRL (**BDRL**) algorithm
Priority Aware DRL (**PADRL**) algorithm

Number of actions per algorithm



Traffic loss per algorithm



Please check my poster for more details!